

**Dave Bacon
Miguel Martin-Delgado
Martin Roetteler (Eds.)**

LNCS 6745

Theory of Quantum Computation, Communication, and Cryptography

**6th Conference, TQC 2011
Madrid, Spain, May 24–26, 2011
Revised Selected Papers**



Springer

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

For further volumes:

<http://www.springer.com/series/7407>

Dave Bacon · Miguel Martin-Delgado
Martin Roetteler (Eds.)

Theory of Quantum Computation, Communication, and Cryptography

6th Conference, TQC 2011
Madrid, Spain, May 24–26, 2011
Revised Selected Papers

Editors

Dave Bacon
University of Washington
Seattle, WA
USA

Martin Roetteler
NEC Laboratories America
Princeton, NJ
USA

Miguel Martin-Delgado
Universidad Complutense de Madrid
Madrid
Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-642-54428-6 ISBN 978-3-642-54429-3 (eBook)
DOI 10.1007/978-3-642-54429-3
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014933392

LNCS Sublibrary: SL1 – Theoretical Computer Science

© Springer-Verlag Berlin Heidelberg 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC) is an annual meeting on theoretical aspects of quantum information processing. The goal of the conference is to foster developments in this rapidly growing, interdisciplinary field by providing a forum for the presentation and discussion of original research.

The sixth iteration of TQC was held during May 24–26, 2011, at the Universidad Complutense de Madrid, Spain. It included invited talks, contributed talks, and a poster session. Authors of selected contributed talks were invited to submit a paper to these proceedings.

TQC 2011 would not have been possible without the contributions of numerous individuals and organizations, and we sincerely thank them for their support.

In putting together the scientific program, we were very grateful for the hard work and advice of the Program Committee, listed herein. We also appreciate the help of the following additional reviewers: Abolfazl Bayat, Dan Browne, Bill Coish, Greg Kuperberg, Frédéric Magniez, Iman Marvian, Matthew McKague, Tomoyuki Morimae, Daniel Nagaj, Varun Narasimhachar, Marcin Pawłowski, Jérémie Roland, Pra-deep Sarvepalli, Tommaso Tufarelli, Thomas Vidick, Tsu-Chieh Wei, and Shigeru Yamashita.

The logistics of the conference were expertly managed by the Organizing Committee, also listed herein. Special thanks goes to Inés Escribano and the local organization team from the Quantum Information Technologies in Madrid (QUITEMAD) group for their efforts to make the conference a success.

We would like to thank the invited speakers for their contributions to the program. The six invited talks delivered were on “*Futures of Quantum Communication: Device-Independent QKD, Quantum Networks and Bi-locality*” by Nicolas Gisin, “*Structure of 2D Topological Stabilizer Codes*” by Hector Bombín, “*Quantum Hamiltonian Complexity*” by Umesh Vazirani, “*Globalness of Unitary Operations on Quantum Information*” by Mio Murao, “*Projected Simulation for Artificial Intelligence*” by Hans Briegel and “*The Continuum Limit of a Quantum Circuit: Variational Classes for Quantum Fields*” by Tobias Osborne.

We would like to thank the members of the Conference Series Steering Committee, Wim van Dam, Yasuhito Kawano, Michele Mosca, and Vlatko Vedral, for their important advice.

TQC 2011 was made possible by financial support from the Consejería de Educación (Comunidad de Madrid), the European Union via the European Social Fund, the Universidad Politécnica de Madrid, the Universidad Complutense de Madrid, the Universidad Carlos III de Madrid, Telefónica, the Facultad de Ciencias Físicas, the Fundación General Universidad (both at the Universidad Complutense de Madrid) and

NEC Laboratories America; we thank these organizations for their important contributions.

Finally, we would like to thank Springer for publishing the proceedings of TQC in the *Lecture Notes in Computer Science* series.

December 2013

Dave Bacon
Miguel Martin-Delgado
Martin Roetteler

Organization

Program Committee

Martin Roetteler	NEC Princeton, USA (Chair)
Dave Bacon	University of Washington, USA (Co-chair)
Mohammed Amin	D-Wave Systems, Canada
Dagmar Bruß	Universität Düsseldorf, Germany
Andrew Childs	University of Waterloo, Canada
Richard Cleve	University of Waterloo, Canada
Steve Flammia	Caltech, USA
Markus Grassl	CQT, Singapore
Peter Høyer	University of Calgary, Canada
Kazuo Iwama	Kyoto University, Japan
Elham Kashefi	University of Edinburgh, UK
Debbie Leung	University of Waterloo, Canada
Hoi-Kwong Lo	University of Toronto, Canada
Chiara Macchiavello	Università di Pavia, Italy
Vicente Martin-Ayuso	Universidad Complutense de Madrid, Spain
Miguel Martin-Delgado	Universidad Complutense de Madrid, Spain
Dmitri Maslov	University of Waterloo, Canada and NSF, USA
Michele Mosca	University of Waterloo and Perimeter Institute, Canada
Kae Nemoto	NII Tokyo, Japan
Miklos Santha	Université Paris Sud, France, and CQT Singapore
Pranab Sen	Tata Institute, India
Simone Severini	University College London, UK
Jean-Pierre Tillich	Inria, France
Andreas Winter	Bristol University, UK and CQT, Singapore

Organizing Committee

Alberto Galindo Tixaire	Universidad Complutense de Madrid, Spain
Juan Jose Garcia-Ripoll	CSIC Madrid, Spain
Alberto Ibart	Universidad Carlos III Madrid, Spain (Co-chair)
Juan Leon	CSIC Madrid, Spain
Vicente Martin-Ayuso	Universidad Politecnica de Madrid, Spain
Miguel Martin-Delgado	Universidad Complutense de Madrid, Spain (Chair)
David Perez-Garcia	Universidad Complutense de Madrid, Spain
Diego Porras	Universidad Complutense de Madrid, Spain

Steering Committee

Wim van Dam	UC Santa Barbara, USA
Yasuhito Kawano	NTT Tokyo, Japan
Michele Mosca	University of Waterloo and Perimeter Institute, Canada
Vlatko Vedral	University of Oxford, UK and CQT, Singapore

Contents

Weak Coin Flipping in a Device-Independent Setting	1
<i>Nati Aharon, André Chailloux, Iordanis Kerenidis, Serge Massar, Stefano Pironio, and Jonathan Silman</i>	
Security of Device-Independent Quantum Key Distribution Protocols	13
<i>Chirag Dhara, Lluís Masanes, Stefano Pironio, and Antonio Acín</i>	
The Locking-Decoding Frontier for Generic Dynamics	23
<i>Frédéric Dupuis, Jan Florjanczyk, Patrick Hayden, and Debbie Leung</i>	
Telescopic Relative Entropy	39
<i>Koenraad M.R. Audenaert</i>	
Approximating the Turaev-Viro Invariant of Mapping Tori is Complete for One Clean Qubit	53
<i>Stephen P. Jordan and Gorjan Alagic</i>	
Span-Program-Based Quantum Algorithm for Evaluating Unbalanced Formulas	73
<i>Ben W. Reichardt</i>	
Self-Testing Graph States	104
<i>Matthew McKague</i>	
Unconditionally-Secure and Reusable Public-Key Authentication	121
<i>Lawrence M. Ioannou and Michele Mosca</i>	
Long Distance Quantum Key Distribution with Continuous Variables.	143
<i>Anthony Leverrier and Philippe Grangier</i>	
Multi-query Quantum Sums	153
<i>David A. Meyer and James Pommersheim</i>	
Bitwise Quantum Min-Entropy Sampling and New Lower Bounds for Random Access Codes	164
<i>Jürg Wullschlegel</i>	
Which Graph States are Useful for Quantum Information Processing?	174
<i>Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya, and Peter S. Turner</i>	

Quantum Discord in Quantum Information Theory – From Strong
Subadditivity to the Mother Protocol. 188
Vaibhav Madhok and Animesh Datta

Local Unitary Group Stabilizers and Entanglement for Multiqubit
Symmetric States 198
Curt D. Cenci, David W. Lyons, and Scott N. Walck

Author Index 209

Weak Coin Flipping in a Device-Independent Setting

Nati Aharon¹(✉), André Chailloux^{2,3,4}, Iordanis Kerenidis^{5,6}, Serge Massar⁷, Stefano Pironio⁷, and Jonathan Silman⁷(✉)

¹ School of Physics and Astronomy, Tel-Aviv University, 69978 Tel-Aviv, Israel
nati.aharon@phys.huji.ac.il

² LIAFA, University of Paris 7, 75205 Paris, France

³ University of Paris-Sud, 91405 Orsay, France

⁴ Computer Science Division, UC Berkeley, Berkeley 94720, CA, USA

⁵ LIAFA, University of Paris 7 – CNRS, 75205 Paris, France

⁶ Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore

⁷ Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
jsilman@ulb.ac.be

Abstract. A protocol is said to be device-independent when the level of its performance can be inferred without making any assumptions regarding the inner workings of the apparatus used to implement it. In this paper we introduce a device-independent weak coin flipping protocol based on a single GHZ test. Interestingly, the protocol calls for the exchange of (quantum) systems between participants; a feature which is not trivial to incorporate in a device-independent setting where a system's behavior may depend on the time, location, and its history. Alice's and Bob's maximal cheating probabilities are given by $\simeq 0.974$ and $\cos^2(\frac{\pi}{8}) \simeq 0.854$.

1 Introduction

Cryptographic protocols, whether quantum or classical are always formulated under a certain set of assumptions. In particular, quantum protocols rely on the validity of quantum mechanics, but also on the security of each participant's lab and his having a trusted source of randomness to carry out random choices called for by the protocol. The list, however, usually does not end here. Most protocols, also make, for instance, assumptions as to the Hilbert space dimension of the quantum information carriers, the measurements that are carried out, etc. Such protocols are said to be device-dependent. Clearly, it is desirable to base security

N. Aharon— Racah Institute of Physics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel

A. Chailloux— SECRET Project Team, INRIA Paris-Recquencourt, 78153 Le Chesnay Cedex, France

on a minimum number of assumptions, as this facilitates checking the reliability of the protocol's implementation. The aim of the device-independent approach to quantum cryptography is to do just that by doing away with a maximal number of assumptions regarding the apparatus used to implement the protocol.

More specifically, a quantum protocol is said to be device-independent if the reliability of its implementation can be guaranteed without making any assumptions about the internal workings of the underlying apparatus. Remarkably, this can be achieved by certifying a sufficient amount of nonlocality (quantified by the degree of violation of a suitable Bell inequality) [1]. For example, in quantum key-distribution a high violation of the CHSH inequality guarantees that an eavesdropper will have no information about the (post-processed) key [2–6]. This should be contrasted with the entanglement-based version of the BB84 protocol, where if the source dispenses qubits instead of qubits then security can be utterly compromised [7, 8]. Indeed, recent hacking attacks on quantum key-distribution systems, such as those of [9, 10], exploit device-dependent modes of failure and would not be successful against a device-independent set up.

In addition to quantum key-distribution, device-independent protocols have been suggested for diverse tasks such as random number generation [11, 12], self-testing devices [7, 13, 14], and genuine multipartite entanglement witnesses [15]. However, until most recently we did not know whether the scope of the device-independent approach also covers the class of cryptographic protocols, often referred to as distrustful cryptography, in which the participants do not trust each other and may have conflicting goals. In [16] we showed that (imperfect) bit-commitment and coin flipping admit a device-independent formulation. Whether these result extends to all protocols in the distrustful cryptography class remains an open question.

In contrast to the majority of device-independent protocols, which are CHSH-based, the bit-commitment protocol of [16] is GHZ-based [17, 18]. Moreover, it is single-shot and does not require the generation of statistics to guarantee the presence of nonlocality. The security of the committing party relies on the no-signaling principle, while the security of the other party relies on Tsirelson's bound. The coin flipping protocol is bit-commitment based.

In this paper we introduce a device-independent weak coin flipping protocol. This protocol represents our first successful attempt at tackling the problem of device-independence in the distrustful cryptography model (prior to [16]). The protocol is similar to that of [16] in that it also makes use of a single GHZ state, but is otherwise very different. In particular, it calls for the exchange of boxes (thereby having different parties potentially act on the same box); a feature that has yet to appear in the device-independent literature, but which is part and parcel of device-dependent protocols. Specifically, it is used in Mochon's optimal weak coin flipping protocol [19] and the ensuing optimal strong coin flipping [20] and bit-commitment [21] protocols. In a device-independent setting the box's behavior may depend on the time, location, and its history. Hence, incorporating this feature is far from trivial.

To prove security we make use of tools developed for CHSH-based device-independent protocols, such as dimensional reduction techniques in which the problem is effectively reduced to one of qubits, and help show how these can be adapted to GHZ-based protocols. In the process we gain further insights into the structure of GHZ correlations.

The paper is organized as follows. We begin in Sect. 2 by defining the problem of coin flipping, making explicit exactly what we mean by device-independence, and defining the GHZ paradox, which plays a central role in our protocol. Next, in Sect. 3, we present the protocol, followed by the proofs of Alice’s and Bob’s security in Sects. 4 and 5.

2 Background

2.1 Coin Flipping

Coin flipping is a cryptographic primitive in which a pair of remote distrustful parties wish to agree on a bit. It admits two variants: ‘strong’ coin flipping and ‘weak’ coin flipping. In the former no party is aware of the other’s preference regarding the outcome of the coin, which may be identical to theirs, while in the latter the preferences are known and opposite: If Alice prefers 0 then Bob prefers 1 and vice-versa. Hence, in the weak variant it makes sense to speak of a winner and a loser. The degree of security afforded by a protocol is quantified by the biases $\epsilon_{*i} = P_{*i} - 1/2$ and $\epsilon_{i*} = P_{i*} - 1/2$, where P_{*i} (P_{i*}) is Alice’s (Bob’s) maximal probability of biasing the outcome to i . For strong coin flipping $\epsilon = \max\{\epsilon_{0*}, \epsilon_{*0}, \epsilon_{1*}, \epsilon_{*1}\}$ is usually referred to as the bias of the protocol, while for weak coin flipping, since we are only interested in each party’s maximal probability of winning, $\epsilon = \max\{\epsilon_{*0}, \epsilon_{1*}\}$ (where it is assumed that Alice wins iff she obtains 0).

The problem of coin flipping was first introduced in classical settings by Blum in 1981 [22]. It was subsequently shown that if there are no limitations on their computational power, dishonest parties can always force whatever outcome they desires. In contrast, in quantum settings the problem is not trivial [23]. Two key results are of those Ambainis [24] and Kitaev [25]. The former states that any protocol achieving a bias of ϵ requires at least $\Omega(\log \log \epsilon^{-1})$ rounds of communication, while the latter states that it is impossible to devise a strong coin flipping protocol satisfying $P_{*i}P_{i*} \leq 1/2$ ($i = 0, 1$). Since the appearance of [23] in 1999, the biases of both strong coin flipping and weak coin flipping have been pushed increasingly lower [24, 26–29]. These efforts culminated in Mochon’s proof that weak coin flipping with an arbitrarily small bias is possible [19]. Building upon this result, Chailloux and Kerenidis have recently introduced a strong coin flipping protocol saturating Kitaev’s bound [20]. Finally, we mention that quantum coin flipping has also been extended to multi-party [30] and many-outcome settings [31, 32], as well as simultaneously to both [33, 34].

2.2 Device-Independence

Let us now make precise just what we mean by device-independence. We make the following assumptions regarding the set up:

1. Each party has (‘black’) boxes with knobs to choose (classical) inputs s_i and registers for (classical) outputs r_i . Entering an input always results in an output (i.e. we do not consider losses).
2. The parties, in particular dishonest parties, are restricted by quantum mechanics.
3. The parties can prevent the boxes from communicating with one another.
4. The parties have a trusted source of randomness to make random choices called for by the protocol.
5. No information leaks out of an honest party’s lab.

Assumptions 2, and 3 imply that the probabilities of the outputs given the inputs for an honest party can be expressed as

$$P(r_1, \dots, r_n \mid s_1, \dots, s_n) = \text{Tr}\left(\rho \bigotimes_i \Pi_{s_i}^{r_i}\right), \quad (1)$$

where ρ is some joint quantum state and $\Pi_{s_i}^{r_i}$ is the POVM element corresponding to inputting s_i into box i and obtaining the outcome r_i . Apart from this constraint, we put no limitations on the boxes’ behavior. Specifically, we allow a dishonest party to choose the state ρ and the POVM elements $\Pi_{s_i}^{r_i}$ as best suits him. We also allow the boxes to have internal memories, clocks, gyroscopes, etc. With such internal mechanisms, a dishonest party can program the boxes so that their behavior depends on the trajectories they have followed in space, on the time at which inputs are fed, or any other aspect of their past history.

Note that when we will talk about boxes being sent from one party to the other, we will not mean by this that actual measurement devices have been sent (though it is easier to present and formulate our results in this way). Instead, we will simply mean that quantum states or classical information encoding instructions for the measurement devices are exchanged between the parties, such that in an honest execution the state ρ and the POVM elements $\Pi_{s_i}^{r_i}$ characterizing the behavior, say, of Alice’s box before the transmission of quantum information now characterize the behavior of Bob’s box after receiving the transmission. Of course, if Alice is dishonest then the state and POVM elements after the transmission may be very different, i.e. $\rho \rightarrow \tilde{\rho}$ and $\Pi_{s_i}^{r_i} \rightarrow \tilde{\Pi}_{s_i}^{r_i}$ with $\tilde{\rho}$ and the $\tilde{\Pi}_{s_i}^{r_i}$ chosen at will by Alice.

Finally, we wish to emphasize that spacelike related measurements are not necessary to implement assumption 2. Indeed, spacelike related measurements do not constitute the only way to prevent communication between quantum boxes and one can instead ‘shield’ each box. For a discussion of this point see [3, 12]. This observation is important because (i) in our protocol some pairs of measurements are not spacelike related as the former and the latter measurements are separated by a step involving communication between the parties; (ii) relativistic causality is by itself sufficient for perfect coin flipping [35] (albeit at the cost of assigning each party two remote secure labs).

2.3 The GHZ Paradox

The GHZ paradox [17, 18] is another famous example of the nonlocal nature of quantum mechanics. It is easy to explain in terms of a three-player game [36]. The rules of the game state that before it starts the players may communicate, devise joint strategies and share classical and quantum resources, but that communication must cease once it begins. The game begins with player i receiving an input $s_i \in \{0, 1\}$. The players are guaranteed that the inputs satisfy $s_1 \oplus s_2 \oplus s_3 = 1$ and that each of the four possible combinations of inputs occurs with probability $\frac{1}{4}$. Let $r_i \in \{0, 1\}$ be the output of player i . The game is won if the players output a combination satisfying $r_1 \oplus r_2 \oplus r_3 = s_1 s_2 s_3 \oplus 1$. It is easy to verify that classically the game can be won with probability $\frac{3}{4}$ at most. The ‘paradox’ consists of the fact that using quantum resources the game can always be won. This can be achieved if the players share a GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, measure along σ_y (σ_x) when receiving the input 0 (1), and output the outcome.

3 Weak Coin Flipping in a Device-Independent Setting

The different steps of the protocol take place at fixed times $t_0 < t_1 < t_2 < t_3$, with the interval between succeeding times Δt being sufficient for communication to take place between the parties. Let $c \in \{0, 1, \perp\}$ denote the outcome of the protocol ($c = \perp$ is output if a party aborts). We assume that at the beginning of the protocol Alice has a two-input two-output box, box 1, and Bob has a pair of two-input two-output boxes, 2 and 3. We denote their inputs and outputs by s_i and r_i respectively, where i labels the box. The boxes are supposed to exhibit GHZ correlations (i.e. satisfy the GHZ paradox). The protocol reads as follows (see Fig. 1):

1. At $t = t_0$:
 - Bob flips a (possibly unbalanced) coin to decide whether to test if the boxes fail to exhibit GHZ correlations, such that its outcome is $b = 0$ with probability p . Bob informs Alice of the value of b .
2. At $t = t_1$:
 - I. If $b = 0$ Alice sends Bob her box (continue to step 3.I).
 - II. If $b = 1$ Alice uniformly at random picks an input s_1 and feeds it into her box:
 - (a) If $r_1 = 0$ she announces that she has won and informs Bob of the value of s_1 (continue to step 3.II.a).
 - (b) If $r_1 = 1$ she asks Bob to send her his boxes (continue to step 3.II.b).
3. At $t = t_2$:
 - I. Bob checks the three boxes for failure to satisfy GHZ correlations: He picks uniformly at random, a triplet $s_1 \oplus s_2 \oplus s_3 = 1$ and inputs s_i into box i . He then checks whether the outputs satisfy $r_1 \oplus r_2 \oplus r_3 = s_1 s_2 s_3 \oplus 1$. If they do, then he asks Alice to proceed with the protocol (continue to step 4.I), else he aborts.

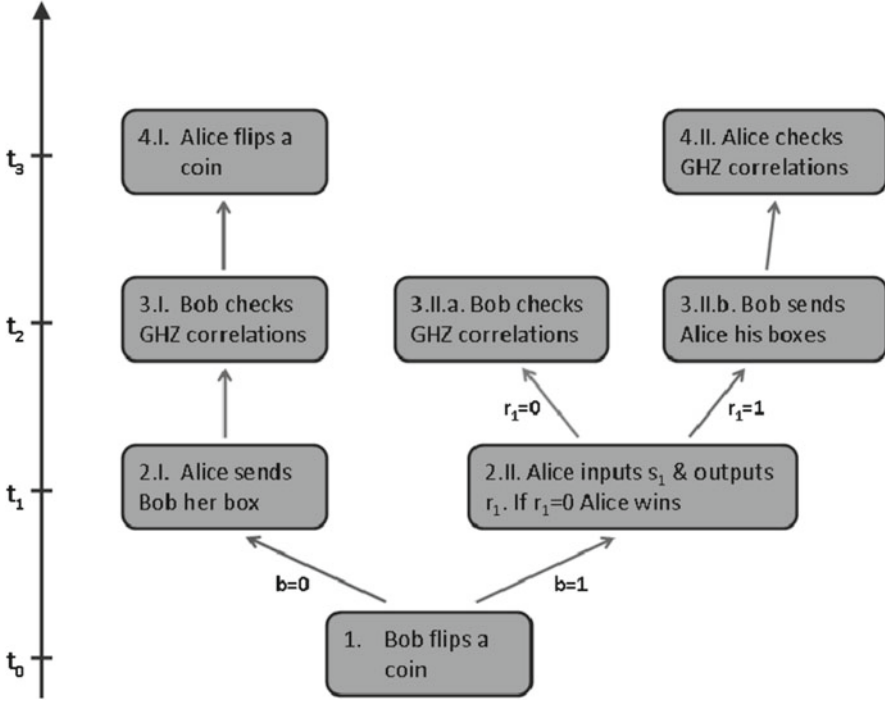


Fig. 1. The protocol. At $t = t_2$ boxes 2 and 3 do not know whether they are tested as part of step 3.I or step 3.II.a.

- II. (a) Bob tests his two boxes to see whether the values of s_1 and $r_1 = 0$ fail to satisfy GHZ correlations: He picks uniformly at random, a pair of inputs s_2 and s_3 satisfying $s_2 \oplus s_3 = 1 \oplus s_1$ and feeds them into boxes 2 and 3. He then checks whether the outputs r_2 and r_3 satisfy $r_2 \oplus r_3 = s_1 s_2 s_3 \oplus 1$. If they do not, then he aborts.
- (b) Bob sends Alice his two boxes (continue to step 4.II).
4. At $t = t_3$:
 - I. Alice flips a balanced coin. If its outcome a equals 0 (1), then she announces that she has won (lost).
 - II. Alice tests the two boxes she received from Bob to see whether the values of s_1 and $r_1 = 1$ fail to satisfy GHZ correlations: She picks uniformly at random, a pair of inputs s_2 and s_3 satisfying $s_2 \oplus s_3 = 1 \oplus s_1$ and feeds them into boxes 2 and 3. She then checks whether the outputs r_2 and r_3 satisfy $r_2 \oplus r_3 = s_1 s_2 s_3$. If they do not, then she aborts. Otherwise, Alice announces that Bob has won.

Note that if the parties are honest (and all devices are perfect) then the protocol does not abort and the coin is balanced, i.e. $P(c = 0) = P(c = 1) = \frac{1}{2}$ and $P(c = \perp) = 0$. For the protocol to be secure, it is crucial that the (mutually

exclusive) tests that Bob performs in step 3.I or 3.II.a be carried out in such a way that it is impossible for boxes 2 and 3 to know whether they are being tested as part of step 3.I or 3.II.a (see Fig. 1). This means that: (i) Each of the tests must be scheduled for the same time, i.e. t_2 . (ii) Each of the tests must take place at the same location i.e. Bob's lab. (iii) At the time of the test the boxes should have the same history (at all times prior the test boxes 2 and 3 are in Bob's lab). On the other hand, boxes 2 and 3 may behave differently in step 4.II, having now a different history (having been sent from Bob to Alice).

4 Alice's Security

4.1 Bob's Maximal Bias

Clearly, dishonest Bob will never ask Alice for her box to test for failure to satisfy GHZ correlations, that is, in step 1 he will announce $b = 1$. Moreover, he will program Alice's box (box 1) such that it always outputs $r_1 = 1$ in step 2.II (otherwise he loses). In order that Alice agree that he has won, and not declare him a cheat, he must pass the test that she carries out on boxes 2 and 3 in step 4.II. To facilitate the analysis, we switch to a notation in which the outputs corresponding to inputting $s_i = 0$ and $s_i = 1$ are labeled by $y_i = (-1)^{r_i}$ and $x_i = (-1)^{r_i}$, respectively. Suppose now that Alice has input $s_1 = 0$, then $y_1 = -1$, and in step 4.II she will feed different inputs into boxes 2 and 3. Therefore, Bob's probability of winning equals $\frac{1}{2} [P(y_2x_3 = 1) + P(x_2y_3 = 1)]$, since she is as likely to input $s_2 = 0$ and $s_3 = 1$ as $s_2 = 1$ and $s_3 = 0$. Similarly, if she has input $s_1 = 1$, then $x_1 = -1$, and in step 4.II she will feed the same inputs into boxes 2 and 3. Bob's probability of winning will then equal to $\frac{1}{2} [P(x_2x_3 = -1) + P(y_2y_3 = 1)]$. Since Alice's choice of s_1 is fully random, it follows that Bob's maximal probability of winning is given by

$$P_{1*} = \frac{1}{4} \max [P(x_2x_3 = -1) + P(y_2y_3 = 1) + P(y_2x_3 = 1) + P(x_2y_3 = 1)], \quad (2)$$

where the maximization is carried out over all possible states and measurements and the dimension of the Hilbert space. This is just the CHSH expression [37] cast in terms of probabilities. The maximum is, therefore, given by Tsirelson's bound [38]. That is, $P_{1*} = \cos^2(\frac{\pi}{8})$.

4.2 Bob's Optimal Cheating Strategy

Dishonest Bob's cheating probability is bounded by Tsirelson's bound. To achieve the bound he simply has to prepare boxes 2 and 3 such that each contains one out of a pair of maximally entangled qubits and such that the measurement settings are optimal, i.e. give rise to a maximal violation of the CHSH inequality.

5 Bob's Security

5.1 Alice's Maximal Bias

To maximize her probability of winning, dishonest Alice must take into account both the possibility that Bob will decide to check that the GHZ correlations are satisfied, i.e. the possibility that he obtains $b = 0$ in step 1, and the possibility that he asks her to proceed with the protocol, i.e. that he obtains $b = 1$. If $b = 0$ and Bob does not find a discrepancy with the GHZ correlations in step 3.I, she announces $c = 0$ in step 4.I and wins. If $b = 1$, then she announces $r_1 = 0$ in step 2.II. It then remains for her to pass Bob's test on boxes 2 and 3 in step 3.II.a, where he checks whether the values of s_1 and $r_1 = 0$ are consistent with GHZ correlations. To this end she carries out a measurement (which we label as m_1) on box 1, whose outcome $q_1 \in \{0, 1\}$ determines what value of the input s_1 she tells Bob that she (supposedly) fed into box 1 in step 2.II. Alice's maximal winning probability is therefore given by

$$\begin{aligned}
 P_{*0} = & \max \left[\frac{p}{4} \sum_{\{s_1, s_2, s_3 | s_1 \oplus s_2 \oplus s_3 = 1\}} \right. \\
 & \times \sum_{\{r_1, r_2, r_3 | r_1 \oplus r_2 \oplus r_3 = s_1 s_2 s_3 \oplus 1\}} P(r_1, r_2, r_3 | s_1, s_2, s_3) \\
 & + \frac{1-p}{2} \sum_{q_1} \sum_{\{s_2, s_3 | q_1 \oplus s_2 \oplus s_3 = 1\}} \\
 & \left. \times \sum_{\{r_2, r_3 | r_2 \oplus r_3 = q_1 s_2 s_3 \oplus 1\}} P(q_1, r_2, r_3 | m_1, s_2, s_3) \right]. \quad (3)
 \end{aligned}$$

To compute P_{*0} we first recall that the space of correlations arising via local measurements is convex. Hence, the maximum will be attained by extremal states, i.e. pure states, and by extremal measurements, i.e. projective measurements. (This is in keeping with the maxims of device-independence, since we do not restrict the dimension of the Hilbert space.) To proceed further, we once again label the outputs corresponding to inputting $s_i = 0$ ($s_i = 1$) by $y_i = (-1)^{r_i}$ ($x_i = (-1)^{r_i}$). Let Y_i and X_i be the corresponding operators, Π and Π_\perp the orthogonal projectors corresponding to obtaining $q_1 = 1$ and $q_1 = 0$, and let \mathcal{H}_i denote the Hilbert space of box i . Since box 2 admits binary inputs and outputs, there exists a basis in which Y_2 and X_2 are block diagonal with blocks of size 2×2 or less [39, 40]. Of course the same holds true for box 3. Hence, it follows from convexity that without loss of generality we can set $\dim \mathcal{H}_2, \dim \mathcal{H}_3 \leq 2$, where $\dim \mathcal{H}_i$ is the dimension of \mathcal{H}_i , and consequently, making use of the Schmidt decomposition theorem, it follows that $\dim \mathcal{H}_1 \leq 4$.

P_{*0} can be re-expressed as

$$\begin{aligned}
P_{*0} = & \frac{1}{2} + \frac{1}{8} \max_{\{X_i, Y_i\}_i, \Pi, |\psi\rangle} \left[p \langle \psi | X_1 \otimes X_2 \otimes X_3 - X_1 \otimes Y_2 \otimes Y_3 \right. \\
& - Y_1 \otimes X_2 \otimes Y_3 - Y_1 \otimes Y_2 \otimes X_3 | \psi \rangle \\
& + 2(1-p) \langle \psi | \Pi \otimes (X_2 \otimes X_3 - Y_2 \otimes Y_3) \\
& \left. - \Pi_{\perp} \otimes (X_2 \otimes Y_3 + Y_2 \otimes X_3) | \psi \rangle \right], \tag{4}
\end{aligned}$$

where $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ is the state of the three boxes. In terms of the operators $D = X_2 \otimes X_3 - Y_2 \otimes Y_3$ and $D' = -X_2 \otimes Y_3 - Y_2 \otimes X_3$, P_{0*} assumes a more compact form

$$\begin{aligned}
P_{0*} = & \frac{1}{2} + \frac{1}{8} \max_{\{X_i, Y_i\}_i, \Pi, |\psi\rangle} \langle \psi | [pX_1 + 2(1-p)\Pi] \otimes D \\
& + [pY_1 + 2(1-p)\Pi_{\perp}] \otimes D' | \psi \rangle \tag{5}
\end{aligned}$$

The freedom that we have in manipulating both the state and operators means that we can always choose the axes such that for boxes 2 and 3 $X_i = \sigma_x$ and $Y_i = \hat{\mathbf{n}}_i \cdot \boldsymbol{\sigma}$, where $\hat{\mathbf{n}}_i$ is some arbitrary unit vector on the xy plane spanning an angle θ_i from the x axis. Now $\hat{\mathbf{n}}_i \cdot \boldsymbol{\sigma} = e^{-i\theta_i \sigma_z} \sigma_x$, so that

$$X_i Y_i = \sigma_x (\cos \theta_i \sigma_x + \sin \theta_i \sigma_y) = \cos \theta_i \mathbb{1} + i \sin \theta_i \sigma_z = e^{i\theta_i \sigma_z}. \tag{6}$$

It is straightforward to verify that in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ D and D' are block diagonal with blocks of size 2×2 , corresponding to the subspaces spanned by $\{|00\rangle, |11\rangle\}$ and $\{|01\rangle, |10\rangle\}$. By noting that we can always flip the coordinate system of one of the qubits about the z axis, we see that it suffices to maximize over states of the form $c_1 |\varphi_1\rangle \otimes |00\rangle + c_2 |\varphi_2\rangle \otimes |11\rangle$. It follows that we can set $\dim \mathcal{H}_1 \leq 2$.

It is easy to show that on the two-dimensional subspace spanned by $|00\rangle$ and $|11\rangle$ D and D' assume the form

$$D = -2 \sin\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \left[-\sin\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \varsigma_x + \cos\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \varsigma_y \right], \tag{7}$$

$$D' = -2 \cos\left(\frac{1}{2}(\theta_2 - \theta_3)\right) \left[\cos\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \varsigma_x + \sin\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \varsigma_y \right], \tag{8}$$

where the ς_i denote Pauli operators on the subspace spanned by $|00\rangle$ and $|11\rangle$. Without loss of generality, we can redefine the x and y axes such that $D = 2 \sin\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \varsigma_y$ and $D' = 2 \cos\left(\frac{1}{2}(\theta_2 - \theta_3)\right) \varsigma_x$. Equation (5) now simplifies to

$$\begin{aligned}
P_{0*} = & \frac{1}{2} + \max_{X_1, Y_1, \Pi, |\psi\rangle} \langle \psi | \sin\left(\frac{1}{2}(\theta_2 + \theta_3)\right) \left(\frac{p}{4} X_1 + \frac{1-p}{2} \Pi \right) \otimes \varsigma_y \\
& + \cos\left(\frac{1}{2}(\theta_2 - \theta_3)\right) \left(\frac{p}{4} Y_1 + \frac{1-p}{2} \Pi_{\perp} \right) \otimes \varsigma_x | \psi \rangle, \tag{9}
\end{aligned}$$

with the maximum obtaining when both terms are positive. This implies that we should set $\theta_2 = \theta_3 = \frac{\pi}{2}$. Equation (9) can then be re-expressed as

$$P_{0*} = \frac{1}{2} + \max_{X_1, Y_1, \Pi, |\psi\rangle} \langle \psi | \left[\left(\frac{p}{4} X_1 + \frac{1-p}{2} \Pi \right) \otimes \mathbb{1} + i \left(\frac{p}{4} Y_1 + \frac{1-p}{2} \Pi_{\perp} \right) \otimes \varsigma_z \right] \mathbb{1} \otimes \varsigma_y | \psi \rangle, \quad (10)$$

and consequently

$$P_{0*} = \frac{1}{2} + \frac{1}{4} \sqrt{\max_{X_1, Y_1, \Pi, |\psi'\rangle} \langle \psi' | A^{\dagger} A | \psi' \rangle}. \quad (11)$$

where $A = (pX_1 + 2(1-p)\Pi) \otimes \mathbb{1} + i(pY_1 + 2(1-p)\Pi_{\perp}) \otimes \varsigma_z$ and $|\psi'\rangle$ is related to $|\psi\rangle$ via $|\psi'\rangle = \mathbb{1} \otimes \varsigma_y |\psi\rangle$

$A^{\dagger}A$ commutes with $\mathbb{1} \otimes \varsigma_z$, therefore, its eigenstates have the form $|u_i\rangle \otimes |0\rangle$ and $|u_i\rangle \otimes |1\rangle$. Suppose now that the maximum obtains for an eigenstate $|u_i\rangle \otimes |0\rangle$ and some specific choice of operators X_1, Y_1 , and Π , and consider now the choice of operators $X'_1 = Y_1, Y'_1 = X_1$, and $\Pi' = \Pi_{\perp}$, then it is straightforward to verify that

$$\langle 0 | \otimes \langle u_i | A^{\dagger} A | u_i \rangle \otimes | 0 \rangle = \langle 1 | \otimes \langle u_i | A'^{\dagger} A' | u_i \rangle \otimes | 1 \rangle, \quad (12)$$

where $A' = (pX'_1 + 2(1-p)\Pi') \otimes \mathbb{1} + i(pY'_1 + 2(1-p)\Pi'_{\perp}) \otimes \varsigma_z$. Clearly, the second choice of operators is just as valid. Hence, without loss of generality we may assume that the maximum obtains for one of the eigenstates $|u_i\rangle \otimes |0\rangle$. The problem then reduces to maximizing over the two-dimensional Hilbert space \mathcal{H}_1 . That is,

$$P_{0*} = \frac{1}{2} + \frac{1}{4} \sqrt{\max_{X_1, Y_1, \Pi, |\xi\rangle} \langle \xi | B^{\dagger} B | \xi \rangle}, \quad (13)$$

where $B = (pX_1 + 2(1-p)\Pi) + i(pY_1 + 2(1-p)\Pi_{\perp})$ and $|\xi\rangle \in \mathcal{H}_1$.

Parameterizing $X_1 = \hat{\mathbf{a}} \cdot \boldsymbol{\sigma}$, $Y_1 = \hat{\mathbf{b}} \cdot \boldsymbol{\sigma}$ and $2\Pi = \mathbb{1} + \hat{\mathbf{c}} \cdot \boldsymbol{\sigma}$, we have

$$\begin{aligned} B^{\dagger}B &= 2 \left[p^2 + 2(1-p)^2 + p(1-p) (\hat{\mathbf{a}} - \hat{\mathbf{b}}) \cdot \hat{\mathbf{c}} \right] \mathbb{1} \\ &\quad + 2p \left[(1-p) (\hat{\mathbf{a}} + \hat{\mathbf{b}}) + (1-p) (\hat{\mathbf{a}} + \hat{\mathbf{b}}) \times \hat{\mathbf{c}} - p\hat{\mathbf{a}} \times \hat{\mathbf{b}} \right] \cdot \boldsymbol{\sigma} \\ &= 2 \left[p^2 + 2(1-p)^2 + 2p(1-p) \sin \mu \hat{\mathbf{t}} \cdot \hat{\mathbf{c}} \right] \mathbb{1} \\ &\quad + 4p \left[(1-p) \cos \mu \hat{\mathbf{s}} + (1-p) \cos \mu \hat{\mathbf{s}} \times \hat{\mathbf{c}} + p \cos \mu \sin \mu \hat{\mathbf{s}} \times \hat{\mathbf{t}} \right] \cdot \boldsymbol{\sigma}, \end{aligned} \quad (14)$$

where in the last line we have reparametrized $\hat{\mathbf{a}} = \cos \mu \hat{\mathbf{s}} + \sin \mu \hat{\mathbf{t}}$ and $\hat{\mathbf{b}} = \cos \mu \hat{\mathbf{s}} - \sin \mu \hat{\mathbf{t}}$ with $\mu \in [0, \frac{\pi}{2}]$. Clearly, the maximum obtains when $\hat{\mathbf{c}} = \hat{\mathbf{t}}$. Setting $\hat{\mathbf{s}} = \hat{\mathbf{z}}$ and $\hat{\mathbf{s}} \times \hat{\mathbf{t}} = \hat{\mathbf{x}}$ we have to find the largest eigenvalue of

$$\begin{aligned} &2 \left[p^2 + 2(1-p)^2 + 2p(1-p) \sin \mu \right] \mathbb{1} + 4p \cos \mu \left[1 - p(1 - \sin \mu) \right] \sigma_x \\ &+ 4p(1-p) \cos \mu \sigma_z. \end{aligned} \quad (15)$$

This is given by

$$\lambda_{\max}(p, q) = 2p^2(3 - 2q) - 4p(2 - q) + 4 \left[1 + p\sqrt{(1 - q^2)(2 - 2p(2 - q) + 2p^2 - p^2(2 - q)q)} \right] \quad (16)$$

with $q = \sin \mu$, and can be analytically maximized for any value of p . For $p = \frac{3}{5}$ we get that $P_{*0} \simeq 0.974$. Numerics indicate that this result is optimal (or at least very close to optimal), i.e. other values of p give rise to a higher winning probability.

5.2 Alice's Optimal Cheating Strategy

Having obtained the optimal values of p and μ , we can use them to explicitly determine the optimal X_1 , Y_1 and Π . The optimal state is then obtained by plugging these back into $A \mathbb{1} \otimes \varsigma_y$, i.e. the operator appearing in Eq. (10), and diagonalizing it. (Note that the eigenstates of $A^\dagger A$ need not correspond to those of $A \mathbb{1} \otimes \varsigma_y$ since $A^\dagger A$ is doubly degenerate.) In this way we find that dishonest Alice optimal cheating strategy consists of preparing the entangled state $|\psi\rangle \simeq 0.43(1 - i)|0\rangle \otimes |00\rangle + 0.60|0\rangle \otimes |11\rangle + 0.26(i - 1)|1\rangle \otimes |00\rangle + 0.37|1\rangle \otimes |11\rangle$, where $|\psi\rangle$ is the eigenvector corresponding to the largest eigenvalue of the operator appearing in Eq. (10). We see that while the optimal measurement settings of boxes 2 and 3 are the same as those of the device-dependent scenario, i.e. measurements along the x and y axes ($X_2 = X_3 = \sigma_x$ and $Y_2 = Y_3 = \sigma_y$), the optimal measurement settings of box 1 are different and given by $X_1 = \hat{\mathbf{a}} \cdot \boldsymbol{\sigma}$, $Y_1 = \hat{\mathbf{b}} \cdot \boldsymbol{\sigma}$ and $\Pi = \frac{1}{2}(\mathbb{1} - \sigma_y)$, where $\hat{\mathbf{a}} = \cos \mu \hat{\mathbf{z}} - \sin \mu \hat{\mathbf{y}}$, $\hat{\mathbf{b}} = \cos \mu \hat{\mathbf{z}} + \sin \mu \hat{\mathbf{y}}$ and $\mu \simeq 0.73$.

Acknowledgements. We acknowledge support from the BSF (grant no. 32/08) (N.A.), the Inter-University Attraction Poles Programme (Belgian Science Policy) under Project IAP-P6/10 (Photonics@be) (S.M., S.P., J.S), a BB2B grant of the Brussels-Capital region (S.P.), the Fonds de la Recherche Scientifique – FNRS (J.S.), the projects ANR-09-JCJC-0067-01, ANR-08-EMER-012 (A.C., I.K.), and the project QCS (grant 255961) of the E.U. (A.C., I.K., S.M., S.P., J.S.).

References

1. Barrett, J., et al.: Phys. Rev. Lett. **95**, 010503 (2005)
2. Acín, A., et al.: Phys. Rev. Lett. **98**, 230501 (2007)
3. Pironio, S., et al.: New J. Phys. **11**, 045021 (2009)
4. McKague, M.: New J. Phys. **11**, 103037 (2009)
5. Masanes, L.L., Pironio, S., Acín, A.: Nat. Commun. **2**, 238 (2011)
6. Hanggi, E., Renner, R.: arXiv:1009.1833
7. Magniez, F., Mayers, D., Mosca, M., Ollivier, H.: Self-testing of quantum circuits. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4051, pp. 72–83. Springer, Heidelberg (2006)

8. Acín, A., Gisin, N., Masanes, Ll.: Phys. Rev. Lett. **97**, 120405 (2006)
9. Xu, F., et al.: New J. Phys. **12**, 113026 (2010) arXiv:1005.2376 [quant-ph]
10. Lydersen, L., et al.: Nat. Photonics **4**, 686 (2010)
11. Colbeck, R., Kent, A.: J. Phys. A: Math. Theor. **44**, 095305 (2011)
12. Pironio, S., et al.: Nature **464**, 1021 (2010)
13. Mayers, D., Yao, A.: Quantum Inform. Comput. **4**, 273 (2004)
14. McKague, M., Mosca, M.: Generalized self-testing and the security of the 6-state protocol. In: van Dam, W., Kendon, V.M., Severini, S. (eds.) TQC 2010. LNCS, vol. 6519, pp. 113–130. Springer, Heidelberg (2011)
15. Bancal, J.-D., et al.: Phys. Rev. Lett. **106**, 250404 (2011) arXiv:1102.0197 [quant-ph]
16. Silman, J., et al.: Phys. Rev. Lett. **106**, 220501 (2011)
17. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Going beyond Bell's theorem. In: Kafatos, M. (ed.) Bell's Theorem, Quantum Theory, and Conceptions of the Universe, p. 74. Kluwer, Dordrecht (1989)
18. Mermin, N.D.: Phys. Today **43**, 9 (1990)
19. Mochon, C.: arXiv:0711.4114 [quant-ph]
20. Chailloux, A., Kerenidis, I.: In: Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, p. 527. CS Press (2009)
21. Chailloux, A., Kerenidis, I.: In: Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science, p. 354. CS Press (2011) arXiv:1102.1678v1 [quant-ph]
22. Blum, M.: In: Gersho, A., Santa Barbara, U.C. (eds.) Advances in Cryptology: a report on CRYPTO 81. Department of Electrical and Computer Engineering, ECE Report No. 82–04, 1982, p. 11
23. Aharonov, D., et al.: In: Proceedings of the 32nd Annual ACM Symposium on the Theory of Computing, p. 705. ACM Press (2000)
24. Ambainis, A.: In: Proceedings of the 33rd Annual ACM Symposium on the Theory of Computing, p. 134. ACM Press (2001)
25. Kitaev, A.: Unpublished. Proof reproduced in [29]
26. Spekkens, R.W., Rudolph, T.: Phys. Rev. A **65**, 012310 (2001)
27. Spekkens, R.W., Rudolph, T.: Phys. Rev. Lett. **89**, 227901 (2002)
28. Mochon, C.: In: Proceedings of the 45th Annual IEEE Symposium on the Foundations of Computer Science, p. 2. CS Press (2004)
29. Mochon, C.: Phys. Rev. A **72**, 022341 (2005)
30. Ambainis, A., et al.: In: Proceedings of the 19th Annual IEEE Conference on Computational Complexity, p. 250. CS Press (2004)
31. Barrett, J., Massar, S.: Phys. Rev. A **69**, 022322 (2004)
32. Barrett, J., Massar, S.: Phys. Rev. A **70**, 052310 (2004)
33. Aharon, N., Silman, J.: New J. Phys. **12**, 033027 (2010)
34. Ganz, M.: arXiv:0910.4952 [quant-ph]
35. Kent, A.: Phys. Rev. Lett. **83**, 5382 (1999)
36. Vaidman, L.: Found. Phys. **29**, 615 (1999)
37. Clauser, J.F., et al.: Phys. Rev. Lett. **23**, 880 (1969)
38. Cirel'son, B.S.: Lett. Math. Phys. **4**, 93 (1980)
39. Tsirelson, B.: Hadronic J. Suppl. **8**, 329 (1993)
40. Masanes, Ll.: Phys. Rev. Lett. **97**, 050503 (2006)

Security of Device-Independent Quantum Key Distribution Protocols

Chirag Dhara¹, Lluís Masanes¹, Stefano Pironio², and Antonio Acín^{1,3}(✉)

¹ ICFO–Institut de Ciències Fotòniques, Castelldefels, 08860 Barcelona, Spain

² Laboratoire d’Infomation Quantique, Université Libre de Bruxelles,
1050 Bruxelles, Belgium

³ ICREA–Institutió Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain
`antonio.acin@icfo.es`

Abstract. Device-independent cryptography represent the strongest form of physical security: it is based on general physical laws and does not require any detailed knowledge or control of the physical devices used in the protocol. We discuss a general security proof valid for a large class of device-independent quantum key distribution protocols. The proof relies on the validity of Quantum Theory and requires that the events generating the raw key are causally disconnected. We then apply the proof to the chained Bell inequalities and compute the corresponding secret-key rates.

1 Introduction

Quantum Key Distribution (QKD), and more generally Quantum Cryptography, implied a change of paradigm in security. Before the conception of QKD in 1984 [1], most cryptographic applications based their security on reasonable assumptions on the eavesdropper’s computational power plus unproven assumptions on the computational complexity of some problems. In QKD, however, security is mainly based on a physically motivated assumption: the honest parties, Alice and Bob, and the eavesdropper, Eve, are constrained by the laws of quantum physics. Still, this is not the only assumption needed for security proofs of QKD. First of all, the honest parties should have a good physical characterization and control of the devices used in the protocol. Moreover, the security proof also requires a pair of minimal assumptions essential to make the cryptographic scenario meaningful: no information leaks Alice and Bob’s laboratories, and the honest parties have a source of trusted randomness and trusted devices to process and store the information generated during the protocol execution.

The main goal of Device-Independent Quantum Key Distribution (DIQKD) [2–4] is to design protocols whose security proof requires no detailed knowledge of the physical devices used for generating correlations. That is, apart from unavoidable assumptions on the security of the honest parties’ locations and the reliability of the devices they use for information processing, which in a way are inherent to the very definition of the cryptographic scenario, only the general validity of quantum theory is needed for security. In this scenario, the only

possible security certificate is the one proposed by Ekert [5], see also [2,6]: the observation of a Bell inequality violation. There are three main motivations to consider the device-independent scenario. First, from a purely theoretical point of view, DIQKD involves fewer assumptions and, thus, implies a stronger security. More generally, identifying the minimal set of physical assumptions needed for secure key distribution is a fundamental problem in cryptography. Second, from an applied point of view, the implementation of DIQKD schemes is more robust to imperfections since their security proof is independent of the devices' details. However, it requires a long-distance detection-loophole-free Bell inequality violation, which at present is an experimental challenge (see however [7]). Finally, DIQKD, as the works on self testing techniques [8,9], opens Quantum Cryptography to the unreliable, yet non-adversarial, provider scenario, as any device compatible with the protocol requirements is secure.

In this work we discuss a general formalism to prove the security of DIQKD protocols [10] (see also [11]). The security proof is completely general and can be applied to any protocol associated to a Bell inequality. The key element in the construction is a bound on the min-entropy of the raw key from the estimated Bell inequality violation. Compared to previous approaches [12], the proof exploits the constraints imposed by quantum theory, which significantly increases the efficiency of the protocols. For instance, when applied to the protocol of Ref. [3], based on the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [13], security can be guaranteed up to a quantum-bit error rate (QBER) of approximately 5%.

The security proof, however, needs a requirement which limits its applicability from a practical point of view: all the events generating the raw-key symbols must be causally disconnected. There are different possibilities to meet this requirement. First, one can relax the device-independent character of the protocol and assume that the measuring apparatuses have no internal memory. Of course, the no-memory assumption is present in any of the security proofs for standard QKD [1]. The requirement can also be fulfilled in a device-independent manner if the honest parties have access to separated devices. For instance, if all raw-key symbols are defined by space-like separated events, special relativity warrants their causal independence. However, space-like separation is not necessarily required for the generation of the raw-key symbols. It is sufficient that the parties are able to shield each of these devices and prevent any unwanted information exchange among them when generating the raw-key symbols. This assumption is similar to the one that the honest parties are capable of preventing information leakage from their laboratories, without which the cryptographic scenario would not make sense.

2 Bell Inequalities and DIQKD Protocols

The class of protocols we consider are variations of Ekert's QKD protocol [5,14]. Alice and Bob share a quantum channel that distributes entangled states and they both have a quantum apparatus to measure their incoming particles. These

apparatuses take an input (the measurement setting) and produce an output (the measurement outcome). We label the inputs and outputs x and a for Alice, and y and b for Bob, and assume that they take a finite set of possible values.

The first step of the protocol consists in measuring the pairs of quantum systems distributed to Alice and Bob. In most of the cases (say N), the inputs are set to fixed values $x_i = x_{\text{raw}}$ and $y_i = y_{\text{raw}}$ and the corresponding outputs $\mathbf{a} = (a_1, \dots, a_N)$ and $\mathbf{b} = (b_1, \dots, b_N)$ constitute the two versions of the raw key. In the remaining systems, which represent a small random subset of all measured pairs (of size say $N_{\text{est}} \approx \sqrt{N}$), the inputs x, y are chosen uniformly at random. From these N_{est} pairs, Alice and Bob determine the relative frequencies $q(ab|xy)$ with which the outputs a and b are obtained when using inputs x and y . These relative frequencies quantify the degree of non-local correlations between Alice and Bob's system through the violation of the Bell inequality associated to the DIQKD protocol. This Bell inequality is defined by a linear function g of the input-output correlations $q(ab|xy)$:

$$g = \sum_{a,b,x,y} g_{abxy} q(ab|xy) \leq g_{\text{loc}}, \quad (1)$$

where g_{abxy} are the coefficients defining the Bell inequality and g_{loc} is its local bound. A particular example of a Bell inequality is the CHSH inequality [13]

$$g_{\text{chsh}} = \sum_{a,b,x,y} (-1)^{a+b+xy} q(ab|xy) \leq 2, \quad (2)$$

where $a, b, x, y \in \{0, 1\}$.

After this initial “measure and estimate” phase, the rest of the protocol is similar to any other QKD protocol. Alice publishes an N_{pub} -bit message about \mathbf{a} , which is used by Bob to correct his errors $\mathbf{b} \rightarrow \mathbf{b}'$, such that $\mathbf{b}' = \mathbf{a}$ with arbitrarily high probability. Alice and Bob then generate their final secret key \mathbf{k} by applying a 2-universal random function to \mathbf{a} and \mathbf{b}' , respectively [15].

3 Generation of the Raw-Key Symbols

In the DIQKD approach, we do not assume that the devices behave according to predetermined specifications. Yet, we must first specify how we model the N pairs of systems used to generate the raw key. These N pairs are eventually all measured using the inputs $x = x_{\text{raw}}$ and $y = y_{\text{raw}}$, but since they were initially selected at random and each of them could have been part of the N_{est} pairs used to estimate the Bell violation, we must also consider what would have happened for any other inputs x and y . Let therefore $P(\mathbf{ab}|\mathbf{xy})$ denote the prior probability to obtain outcomes \mathbf{a} and \mathbf{b} if measurements $\mathbf{x} = (x_1, \dots, x_N)$ and $\mathbf{y} = (y_1, \dots, y_N)$ are made on these N pairs. This unknown probability distribution characterizes the initial system at the beginning of the protocol.

In the theoretical model needed for the security proof of Ref. [10], the N bits of the raw key are viewed as arising from N *commuting* measurements on a joint

quantum system ρ_{AB} . That is, the probabilities $P(\mathbf{ab}|\mathbf{xy})$ can be written as

$$P(\mathbf{ab}|\mathbf{xy}) = \text{tr}[\rho_{AB} \prod_{i=1}^N A_i(a_i|x_i)B_i(b_i|y_i)], \quad (3)$$

where $A_i(a_i|x_i)$ are operators describing the measurements performed by Alice on her i th system if she select input x_i (they thus satisfy $A_i(a_i|x_i) \geq 0$ and $\sum_{a_i} A_i(a_i|x_i) = \mathbb{1}$), where, similarly, $B_i(b_i|y_i)$ are operators describing the measurements by Bob, and where these measurement operators satisfy the commutation relations

$$[A_i(a|x), B_j(b|y)] = 0 \quad (4)$$

and

$$[A_i(a|x), A_j(a'|x')] = [B_i(b|y), B_j(b'|y')] = 0 \quad (5)$$

for all i, j and a, a', b, b', x, x' . Apart from the conditions (4) and (5), the state ρ_{AB} and the operators $A_i(a_i|x_i)$ and $B_i(b_i|y_i)$ are arbitrary and unspecified. The only constraint on them is that they should return measurement probabilities (3) compatible with the statistics of the N_{est} randomly selected pairs, characterized by the observed Bell-inequality violation g .

In quantum theory, measurement operators that commute represent compatible measurements that do not influence each other and which can be performed independently of each other. The commutation relations (4) between the operators $A_i(a_i|x_i)$ describing Alice's measurement devices and the operators $B_i(b_i|y_i)$ describing Bob's measurement devices are thus a necessary part of any DIQDK model; security cannot be guaranteed without them.

The commutation relations (5) between the operators $A_i(a_i|x_i)$ *within* Alice's location, and the commutation relations between the operators $B_i(b_i|y_i)$ *within* Bob's location, represent, on the other hand, additional constraints specific to the model discussed here. As already mentioned these commutation relations are satisfied in an implementation in which the N bits of the raw key are generated by N separate and non-interacting pairs of devices used in parallel. Let's elaborate more on this point.

In the extreme adversarial scenario where the provider of the devices is not trusted (e.g., if the provider is the eavesdropper itself), this independence condition can be guaranteed by shielding the N devices in such a way that no communication between them occurs during the measurement process. One could also consider a setup where the measurements performed by the N devices define space-like separated events. However, even in a space-like separated configuration, the ability to shield the devices is required if the provider of the devices is untrusted, as we cannot guarantee through other means that the devices do not send directly unwanted information to the adversary. But, then, the ability to shield the devices is already sufficient by itself to guarantee (5).

In a more practical implementation where the raw key is generated by repeatedly performing measurements in sequence on a *single* pair of devices, the commutation relation (5) expresses the condition that the functioning of the devices should not depend on any internal memory storing the quantum states and

measurement results obtained in previous rounds. In the most general DIQKD model, the quantum devices could possess a quantum memory such that the state of the system after the i th measurement is passed to the successive round $i + 1$ (this state could also contain classical information about the measurement inputs and outputs of step i). If $\rho_{\mathcal{AB}}^i$ denotes the state of the system before measurement i , the unnormalised state passed to round $i + 1$ in the event that Alice and Bob use inputs x_i and y_i and obtain outputs a_i and b_i would then be $\tilde{A}_i^\dagger(a_i|x_i)\tilde{B}_i^\dagger(b_i|y_i)\rho_{\mathcal{AB}}^i\tilde{A}_i(a_i|x_i)\tilde{B}_i(b_i|y_i)$ where $\tilde{A}_i(a|x)$ and $\tilde{B}_i(b|x_i)$ are generalized measurement operators describing Alice's and Bob's measurements and satisfying $\sum_a \tilde{A}_i(a|x)\tilde{A}_i^\dagger(a|x) = \sum_b \tilde{B}_i(b|y)\tilde{B}_i^\dagger(b|y) = I$. In such a model, the probabilities $P(\mathbf{ab}|\mathbf{xy})$ are then given by

$$P(\mathbf{ab}|\mathbf{xy}) = \text{tr}\left[\prod_{i=N}^1 \tilde{A}_i^\dagger(a_i|x_i)\tilde{B}_i^\dagger(b_i|y_i) \times \rho_{\mathcal{AB}} \prod_{i=1}^N \tilde{A}_i(a_i|x_i)\tilde{B}_i(b_i|y_i)\right], \quad (6)$$

where $\rho_{\mathcal{AB}}$ denotes the initial state at the beginning of the protocol, and the order in the products is relevant. Imposing commutation relations between all operators pertaining to different rounds corresponds to neglect the causal order in (6) due to memory effects. We then recover a model of the form (3) by defining $A_i(a|x) = \tilde{A}_i(a|x)\tilde{A}_i^\dagger(a|x)$ and $B_i(b|y) = \tilde{B}_i(b|y)\tilde{B}_i^\dagger(b|y)$.

4 Security Proof

We are now in position to review the bound on the secret key rate derived in [10]. This bound can be achieved against an unrestricted eavesdropper Eve for any QKD protocol satisfying the description (3), (4) and (5). The information available to Eve can be represented by a quantum system that is correlated with the Alice and Bob's systems. We denote by $\rho_{\mathcal{AB}\mathcal{E}}$ the corresponding $(2N + 1)$ -partite state, with $\text{tr}_{\mathcal{E}} \rho_{\mathcal{AB}\mathcal{E}} = \rho_{\mathcal{AB}}$. This state describes the $2N + 1$ systems at the beginning of the protocol. After the N systems of Alice have been measured, the joint state of Alice and Eve is described by the classical-quantum state

$$\rho_{\mathcal{AE}} = \sum_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\text{raw}})|\mathbf{a}\rangle\langle\mathbf{a}| \otimes \rho_{\mathcal{E}|\mathbf{a}}, \quad (7)$$

where $\rho_{\mathcal{E}|\mathbf{a}}$ is the reduced state of Eve conditioned on Alice having observed the outcomes \mathbf{a} .

The length of the secret key \mathbf{k} obtained by processing the raw key \mathbf{a} with an error correcting protocol and a 2-universal random function is, up to terms of order \sqrt{N} , lower bounded by $H_{\min}(\mathbf{a}|\mathcal{E}) - N_{\text{pub}}$, where $H_{\min}(\mathbf{a}|\mathcal{E})$ is the min-entropy of \mathbf{a} conditioned on Eve's information for the state (7) and N_{pub} is the length of the message published by Alice in the error-correcting phase. It is shown in [16] that the length of the public message necessary for correcting Bob's errors is $N_{\text{pub}} = NH(a|b)$, up to terms of order \sqrt{N} . The quantity $H(a|b)$ is the conditional Shannon entropy [16], defined by

$$H(a|b) = \sum_{a,b} -P(a,b) \log_2 P(a|b), \quad (8)$$

where $P(a, b) = 1/N \sum_{i=1}^N \sum_{a_i, b_i} P(a_i = a, b_i = b)$ is the average probability with which the pair of outcomes a and b are observed. Computing the key rate of the DIQKD protocol, thus essentially amounts to determine the min-entropy $H_{\min}(\mathbf{a}|E)$. A bound on this quantity can be derived as a function of the estimated Bell violation g .

Consider first the simpler case of one pair of systems ($N = 1$) uncorrelated to the adversary and characterized by the joint probabilities

$$P(ab|xy) = \text{tr}[\rho A(a|x)B(b|y)]. \quad (9)$$

If $P(a|x_{\text{raw}}) < 1$ for all a , then the outcome of the measurement x_{raw} cannot be perfectly predicted. The degree of unpredictability of a can be quantified by the probability to correctly guess a [17]. This guessing probability is equal to

$$P_{\text{guess}}(a) = \max_a P(a|x_{\text{raw}}), \quad (10)$$

since the best guess that one can make about a is to output the most probable outcome. If $P_{\text{guess}}(a) = 1$ then the outcome of the measurement x_{raw} can be predicted with certainty, while lower values for $P_{\text{guess}}(a)$ imply less predictability.

Let $g_{\text{exp}} = \sum_{abxy} g_{abxy} P(ab|xy) = \text{tr}[\rho G]$ denote the expected quantum violation of the Bell inequality (1) for the pair of systems described by (9), where

$$G = \sum_{a,b,x,y} g_{abxy} A(a|x)B(b|y), \quad (11)$$

is the Bell operator associated to the inequality g and to the measurements $A(a|x)$ and $B(b|y)$. Independently of the precise form of the state ρ and of the measurement operators $A(a|x)$ and $B(b|y)$, the value of the Bell expectation g_{exp} imposes a constraint on the guessing probability (10). Formally, this constraint can be expressed as a bound of the form

$$P_{\text{guess}}(a) \leq f(g_{\text{exp}}), \quad (12)$$

satisfied by all quantum distributions (9). The optimal point-wise values $f(g_0)$ (for any g_0) correspond to the solution of the following maximization problem

$$\begin{aligned} & \max_{\rho, A, B} \quad \text{tr}[\rho A(a|x_{\text{raw}})] \\ & \text{subject to } \text{tr}[\rho G] = g_0, \end{aligned} \quad (13)$$

which can be solved (or upper-bounded) using the semidefinite programming (SDP) relaxations introduced in [18]. The resulting functions f (and in particular the optimal one) are then always concave and monotonically decreasing, as follows from the convex nature of the problem (13) and of its associated SDP relaxations. In the case of the CHSH inequality, the optimal function f is [10, 19]

$$f_{\text{chsh}}(g) = \frac{1}{2} + \frac{1}{2} \sqrt{2 - \frac{g^2}{4}}, \quad (14)$$

for any of the two possible values $x_{\text{raw}} = 0$ or 1 entering in the CHSH definition (2).

As the function f is concave, it can be upper-bounded by its linearization around any point g_0

$$f(g) \leq \mu(g_0) + \nu(g_0)g, \quad (15)$$

where $\mu(g_0) = f(g_0) - f'(g_0)g_0$, $\nu(g_0) = f'(g_0)$. From concavity, it also follows that

$$f(g) = \min_{g_0} [\mu(g_0) + \nu(g_0)g]. \quad (16)$$

The bound (12) is thus equivalent to the family of inequalities $P(a|x_{\text{raw}}) \leq \mu(g_0) + \nu(g_0)g_{\text{exp}}$ for all a and g_0 . Since these inequalities are satisfied by any quantum distribution (9), and thus in particular by any state ρ , they are equivalent to the operator inequalities

$$A(a|x_{\text{raw}}) \leq \mu(g_0)\mathbb{1} + \nu(g_0)G, \quad (17)$$

valid for all a , g_0 , and any set of measurements $A(a|x)$ and $B(b|y)$.

Moving to the case of N pairs of systems described by (3) and (7), the probability with which Eve can correctly guess the raw key \mathbf{a} by measuring her side information \mathcal{E} can be computed as follows. Suppose thus that Eve performs some measurement z on her system \mathcal{E} and obtains an outcome e . Let $P(\mathbf{a}|\mathbf{x}_{\text{raw}}, ez)$ denote the probability distribution of \mathbf{a} conditioned on Eve's information. On average, her probability to correctly guess \mathbf{a} is given by $\sum_e P(e|z) \max_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\text{raw}}, ez)$, and her optimal correct-guessing probability (optimized over all measurements z) is [17]:

$$P_{\text{guess}}(\mathbf{a}|\mathcal{E}) = \max_z \sum_e P(e|z) \max_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\text{raw}}, ez). \quad (18)$$

Denote by $\rho_{AB|ez}$ the $2N$ -partite state prepared when Eve measures z and obtains the outcome e (with $\rho_{AB} = \sum_e P(e|z)\rho_{AB|ez}$), and write $\mathbf{A}(\mathbf{a}|\mathbf{x}_{\text{raw}}) = \prod_{i=1}^N A_i(a_i|x_{\text{raw}})$, so that

$$P(\mathbf{a}|\mathbf{x}_{\text{raw}}, ez) = \text{tr} [\rho_{AB|ez} \mathbf{A}(\mathbf{a}|\mathbf{x}_{\text{raw}})]. \quad (19)$$

Consider the following N -partite Bell operator

$$\mathbf{G}(g_0) = \prod_{i=1}^N [\mu(g_0)\mathbb{1} + \nu(g_0)G_i], \quad (20)$$

where $G_i = \sum_{a,b,x,y} g_{abxy} A_i(a_i|x_i) B_i(b_i|y_i)$. The single-copy operator inequality (17) implies that for all \mathbf{a} and g_0

$$\mathbf{A}(\mathbf{a}|\mathbf{x}_{\text{raw}}) \leq \mathbf{G}(g_0). \quad (21)$$

To show this, write $A'_i = A_i(a_i|x_{\text{raw}})$ and $G'_i = \mu(g_0)\mathbb{1} + \nu(g_0)G_i$. We thus want to establish that $\prod_{i=1}^N G'_i - \prod_{i=1}^N A'_i \geq 0$. Inequality (17) implies that for all i ,

$0 \leq A'_i \leq G'_i$. Defining $Z_i = G'_i - A'_i \geq 0$, note then that $\prod_{i=1}^N G'_i - \prod_{i=1}^N A'_i = \prod_{i=1}^N (Z_i + A'_i) - \prod_{i=1}^N A'_i = \prod_{i=1}^N Z_i + Z_1 \prod_{i=2}^N A'_i + \dots + \prod_{i=1}^{N-1} A'_i Z_N$. Inequality (21) then follows from the fact that each term in this sum is positive since it is the product of operators that are positive and, according to (5), commuting.

Using inequality (21) in (18), we find

$$\begin{aligned} P_{\text{guess}}(\mathbf{a}|\mathcal{E}) &= \max_z \sum_e P(e|z) \max_{\mathbf{a}} \text{tr} [\rho_{\mathcal{AB}|ez} A(\mathbf{a}|\mathbf{x}_{\text{raw}})] \\ &\leq \max_z \sum_e P(e|z) \min_{g_0} \text{tr} [\rho_{\mathcal{AB}|ez} \mathbf{G}(g_0)], \\ &\leq \min_{g_0} \text{tr} [\rho_{\mathcal{AB}} \mathbf{G}(g_0)] \end{aligned} \quad (22)$$

where to deduce the first inequality we used, in addition to (21), the positivity of $\rho_{\mathcal{AB}|ez}$.

Note now that the quantity $\text{tr} [\rho_{\mathcal{AB}}, \mathbf{G}(g_0)]$ is a function of the marginal distributions $P(\mathbf{a}\mathbf{b}|\mathbf{xy})$ of Alice and Bob only and does not involve directly the system of Eve. It is shown in [17], that Alice and Bob can estimate (with high probability) this quantity from the Bell violation g observed on the randomly-chosen N_{est} pairs. More precisely, Lemma 5 from reference [17] implies that the inequality

$$\text{tr} [\rho_{\mathcal{AB}}, \mathbf{G}(g_0)] \leq \left[\mu(g_0) + \nu(g_0)g_{\text{est}} + N_{\text{est}}^{-1/4} \right]^N \quad (23)$$

holds except with probability exponentially small in N_{est} . This, (22), and (16) imply that

$$P_{\text{guess}}(\mathbf{a}|\mathcal{E}) \leq \left[f(g^{\text{est}}) + N_{\text{est}}^{-1/4} \right]^N. \quad (24)$$

Finally, it is shown in [17] that the (quantum) min-entropy $H_{\min}(\mathbf{a}|\mathcal{E})$ of a state of the form (7) is given by

$$H_{\min}(\mathbf{a}|\mathcal{E}) = -\log_2 P_{\text{guess}}(\mathbf{a}|\mathcal{E}), \quad (25)$$

which implies the asymptotic secret key rate

$$R \geq -\log_2 f(g_{\text{est}}) - H(a|b). \quad (26)$$

As announced, the bound applies to any Bell inequality and the corresponding DIQKD protocol.

5 Key Rates for the Chained Bell Inequality

As an illustration of the formalism, we explicitly compute the secret-key rates for the chained Bell inequalities of Ref. [20]. These inequalities were initially introduced in the scenario in which Alice and Bob perform M measurements of two outcomes. Later, they were generalized to an arbitrary number of outcomes [21], but we don't consider this generalization here.

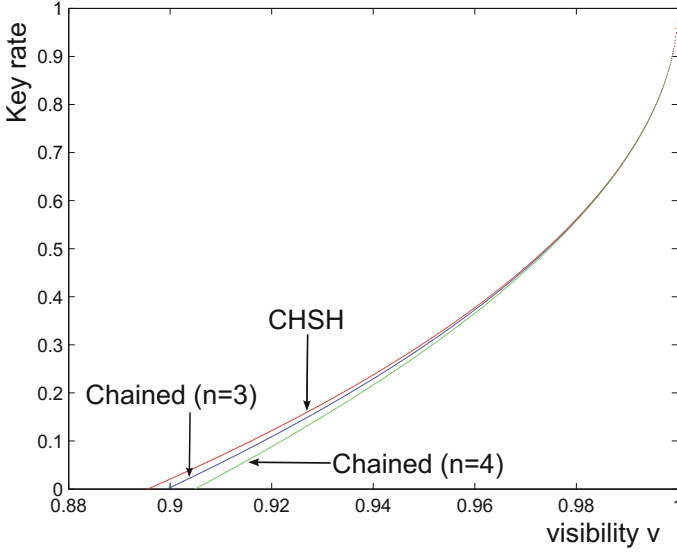


Fig. 1. Key rates for the chained Bell inequalities for 2, 3 and 4 measurements. The critical visibility such that the lower bound on the key rate is zero is approximately of 0.9. Increasing the number of settings up to 4 worsens this critical visibility.

The chained inequalities for two measurement outcomes read as follows. The two outcomes of each measurement by Alice (Bob) are labeled by $A_i = \pm 1$ ($B_i = \pm 1$), with $i = 1, \dots, M$. Then, for any local model one has

$$\sum_{i=1}^M \langle A_i B_i \rangle + \sum_{i=1}^{M-1} \langle B_i A_{i+1} \rangle - \langle B_M A_1 \rangle \leq 2(M-1), \quad (27)$$

where $\langle X \rangle$ stands for the expectation value of the random variable X . The case $M = 2$ corresponds to the standard CHSH inequality.

In Fig. 2 we depict the lower bound on the secret-key rates (26) for DIQKD protocols based on the chained inequalities for $M = 2, 3, 4$. These rates have been computed for the probability distribution resulting from applying the optimal measurements for the maximal quantum violation of the chained inequality on a mixture of a two-qubit maximally entangled state $|\Phi^+\rangle$ and white noise, that is,

$$\rho_{AB} = v|\Phi^+\rangle\langle\Phi^+| + (1-v)\mathbb{1}/4, \quad (28)$$

where v is often known as the visibility. It is important to recall that, while the rate is computed for a concrete set of states and measurements, the security analysis is fully device independent (up to the requirement that measurement outcomes are causally disconnected). Each value of the visibility defines a value for the error rate between Alice and Bob, $\epsilon_{AB} = (1+v)/2$, which specifies the amount of bits needed for error correction. The violation of the chained Bell

inequality is just the maximal quantum violation multiplied by the visibility v . Putting the two things together, one derives the rates given in Fig. 1. The obtained critical values of the visibility such that the key rate is provably strictly positive, are of approximately 0.9. They are then comparable to those of standard QKD, which are around 0.78.

Acknowledgements. This work is supported by the Spanish MINCIN through projects FIS2007-60182 and FIS2010-14830, CHIST-ERA DIQIP, EU Project QCS and an ERC Starting Grant PERCENT, CatalunyaCaixa.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, p. 175 (1984)
2. Acín, A., Gisin, N.: Ll. Masanes. Phys. Rev. Lett. **97**, 120405 (2006)
3. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Phys. Rev. Lett. **98**, 230501 (2007)
4. Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., Scarani, V.: New J. Phys. **11**, 045021 (2009)
5. Ekert, A.: Phys. Rev. Lett. **67**, 661 (1991)
6. Barrett, J., Hardy, L., Kent, A.: Phys. Rev. Lett. **95**, 010503 (2005)
7. Gisin, N., Pironio, S., Sangouard, N.: Phys. Rev. Lett. **105**, 070501 (2010)
8. Mayers, D., Yao, A.: Quantum Inf. Comput. **4**, 273 (2004)
9. Magniez, F., Mayers, D., Mosca, M., Ollivier, H.: Self-testing of quantum circuits. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4051, pp. 72–83. Springer, Heidelberg (2006)
10. Masanes, L., Pironio, S., Acín, A.: Nat. Comm. **2**, 238 (2011)
11. Hanggi, E., Renner, R.: arXiv:1009.1833
12. Ll. Masanes, Phys. Rev. Lett. **102**, 140501 (2009)
13. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Phys. Rev. Lett. **23**, 880 (1969)
14. Acín, A., Massar, S., Pironio, S.: New J. Phys. **8**, 126 (2006)
15. Carter, J.L., Wegman, M.N.: J. Comput. Syst. Sci. **18**, 143–154 (1979)
16. Csiszár, I., Kröner, J.: IEEE Trans. Inf. Theor. **24**, 339 (1978)
17. Koenig, R., Renner, R., Schaffner, C.: IEEE Trans. Inf. Theor. **55**, 9 (2009)
18. Navascues, M., Pironio, S., Acín, A.: Phys. Rev. Lett. **98**, 010401 (2007)
19. Pironio, S., Acín, A., Massar, S., Maunz, A., Olmschenk, S., Hayes, D., Luo, L., Manning, T.A., Monroe, C.: arXiv:0911.3427
20. Braunstein, S.L., Caves, C.M.: Ann. Phys. **202**, 22 (1990)
21. Barret, J., Kent, A., Pironio, S.: Phys. Rev. Lett. **97**, 170409 (2006)

The Locking-Decoding Frontier for Generic Dynamics

Frédéric Dupuis¹, Jan Florjanczyk^{2(✉)}, Patrick Hayden^{2,4},
and Debbie Leung^{3,4}

¹ Institute for Theoretical Physics, ETH Zurich, Zurich, Switzerland

² School of Computer Science, McGill University, Montreal, Canada
jan.orjanczyk@gmail.com

³ Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

⁴ Perimeter Institute for Theoretical Physics, Waterloo, Canada

Abstract. It is known that the maximum classical mutual information that can be achieved between measurements on a pair of quantum systems can drastically underestimate the quantum mutual information between those systems. In this article, we quantify this distinction between classical and quantum information by demonstrating that after removing a logarithmic-sized quantum system from one half of a pair of perfectly correlated bitstrings, even the most sensitive pair of measurements might only yield outcomes essentially independent of each other. This effect is a form of information locking but the definition we use is strictly stronger than those used previously. Moreover, we find that this property is generic, in the sense that it occurs when removing a random subsystem. As such, the effect might be relevant to statistical mechanics or black hole physics. Previous work on information locking had always assumed a uniform message. In this article, we assume only a min-entropy bound on the message and also explore the effect of entanglement. We find that classical information is strongly locked almost until it can be completely decoded. As a cryptographic application of these results, we exhibit a quantum key distribution protocol that is “secure” if the eavesdropper’s information about the secret key is measured using the accessible information but in which leakage of even a logarithmic number of key bits compromises the secrecy of all the others.

Keywords: Information locking · Quantum information · Encryption · Discord · Measure concentration · Black holes

1 Introduction

One of the most basic and intuitive properties of most information measures is that the amount of information carried by a physical system must be bounded by its size. For example, if one receives ten physical bits, then one’s information, regardless of what that information is “about”, should not increase by more than ten bits. While this is true for most information measures, in quantum mechanics

there exist natural ways of measuring information that violate this principle by a wide margin. In particular, this violation occurs when one defines the information contained in a quantum system as the amount of classical information that can be extracted by the best possible measurement. To construct examples of this effect, we take a classical message and encode it into a two-part quantum message: a *cyphertext*, which is roughly as large as the message, and a much smaller *key*. Given both the cyphertext and the key, the message can be perfectly retrieved. We can then look at the amount of information that can be extracted about the message by a measurement given only access to the cyphertext. Locking occurs if this amount of information is less than the amount of information in the message minus the size of the key.

In previous work on locking [DHL+04, HLSW04], this amount of information was taken to be the accessible information, the maximum (classical) mutual information between the message and the result of a measurement. In [DHL+04], the authors constructed the first example of locking as follows: the cyphertext consists of the uniformly random message, encoded in one of two mutually unbiased bases, and the (one-bit) key reveals the basis in which the encoding was done. In this example, given only the cyphertext, the classical mutual information is only $\frac{n}{2}$ for an n -bit message. Hence, the one-bit key can increase the classical mutual information by another $\frac{n}{2}$ bits. In [HLSW04], the authors considered a protocol in which one encodes a classical message using a fixed basis, and then applies one of k fixed unitaries (where $k = O(\text{polylog } n + \log \frac{1}{\varepsilon})$); the classical key reveals which unitary was applied. If the unitaries are chosen according to the Haar measure, then with high probability, the accessible information was shown to be at most εn when one only has the cyphertext.

In this paper, we present stronger and more general locking results, and show that this effect is generic. Our results will be stronger in the sense that instead of using the accessible information, we will define locking in terms of the trace distance between measurement results on the real state and measurement results on a state completely independent of the message (see Definition 4). Unlike the accessible information, this has a very natural operational interpretation: it bounds the largest probability with which we can guess, given a message m and the result x of a measurement done on a cyphertext, whether x comes from a valid cyphertext for m or from a cyphertext generated independently of m . In other words, one could almost perfectly reproduce any measurement results made on a valid cyphertext without having access to the cyphertext at all. Moreover, we recover a strengthened version the earlier statements about the accessible information. Whereas previously the accessible information was shown to be at most 3 bits, our techniques show that the accessible information can be made arbitrarily small. (A follow-up paper further strengthens the definition and explores connections to low-distortion embeddings [FHS10].)

Despite this stronger definition, we will be able to show that the locking phenomenon is generic. Instead of having a classical key reveal the basis in which the information is encoded, as in [DHL+04, HLSW04], we consider the case where there is a single unitary, and the key is simply a small part of the quantum system

after the unitary is applied. This means that we can make not only cryptographic statements, but also statements about the dynamics of physical systems, where the unitary represents the evolution of the system. In particular, we will be able to show that locking occurs with high probability in physical systems whose internal dynamics are sufficiently generic to be adequately modelled by a Haar-distributed unitary. This can therefore give interesting results in the context of thermodynamics, or of the black hole information problem.

In that vein, we will also allow the measuring device to share entanglement with the cyphertext-key compound system. While this may not correspond to a very meaningful cryptographic scenario, it allows us to study the behavior of entanglement in physical systems, and to study the extent to which the presence of entanglement interferes with this locking effect.

Finally, in contrast to previous studies, we will not limit the message (or the entanglement) to be uniform; the size of the key will instead depend on the min-entropy of the message. This assumption is easier to justify in cryptographic applications. Indeed, while the locking results we present here can be interpreted as demonstrating the possibility of encrypting classical messages in quantum systems using only very small keys, care must be taken when composing such encryption with other protocols. We use our results to exhibit a quantum key distribution protocol, for example, that appears to be secure if the eavesdropper’s information about the secret key is measured using the accessible information, but in which leakage of a logarithmic amount of key causes the entire key to be compromised.

1.1 Transmitting Information Through a Generic Unitary

To end the introduction, we introduce the physical scenario that will occupy us throughout the article. The situation is depicted in Fig. 1.

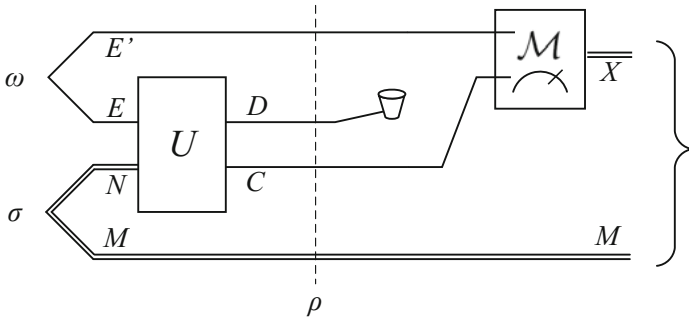


Fig. 1. A quantum circuit depicting the physical scenario. The classical message M gets encoded in N , and the unitary then mixes it with the E part of the shared entanglement. If the information is locked, any joint measurement \mathcal{M} on C and E' will yield a result X that is almost independent of the message. On the other hand, if C is large enough, there will be a joint measurement \mathcal{M} reliably decoding M .

Now, let $\{|\psi_m\rangle : 1 \leq m \leq |M|\}$ be any orthonormal basis for N . The analysis will focus on the properties of the states

$$\sigma^{MN} := \sum_{m=1}^{|M|} p_m |m\rangle\langle m|^M \otimes |\psi_m\rangle\langle\psi_m|^N \quad \text{and} \quad (1)$$

$$\rho^{MCDE'} := \left(\mathbb{I}^{ME'} \otimes U^{NE \rightarrow CD} \right) \left(\sigma^{MN} \otimes \omega^{EE'} \right) \left(\mathbb{I}^{ME'} \otimes U^{NE \rightarrow CD} \right)^\dagger \quad (2)$$

Our objective is to demonstrate that until C is large enough that there exists a measurement on CE' capable of revealing *all* the information about the message M , no measurement will reveal *any* information about the message. This can't quite be true, of course, so what we will demonstrate is that the jump from no information to complete information involves enlarging C by a number of qubits logarithmic in the size of the message M and the amount of entanglement E .

Assume for simplicity both that M is uniformly distributed and that the state $\omega^{EE'}$ is maximally entangled. As a first step, it is necessary to determine how large C needs to be in order for there to exist a measurement on CE' that will reveal the message M . Begin by purifying the state σ to

$$|\sigma\rangle^{RMN} = \frac{1}{\sqrt{|M|}} \sum_{m=1}^{|M|} |m\rangle^R \otimes |m\rangle^M \otimes |\psi_m\rangle^N. \quad (3)$$

Even more demanding than performing a measurement to reveal m is the task of transmitting the quantum information about RM through U , allowing the decoder, who has access only to CE' , to recover a high fidelity copy of the state $|\sigma\rangle^{RMN}$. If U is selected according to the Haar measure, then Theorem IV.1 of [ADHW09] implies that there is a quantum operation $\mathcal{D}^{CE' \rightarrow N}$ acting only on CE' such that

$$\left\| \mathcal{D} \left(\text{Tr}_D \left[U^{NE \rightarrow CD} \cdot (\sigma^{RMN} \otimes \omega^{EE'}) \right] \right) - \sigma^{RMN} \right\|_1 \leq 2\sqrt{\frac{M}{C}}. \quad (4)$$

Because the trace distance is monotonic under quantum operations, it will not increase by taking the partial trace over R and measuring in the basis $\{|\psi_m\rangle\}$ [NC00]. If we let $p(m'|m)$ be the probability of getting an outcome $|\psi_{m'}\rangle$ when the message was in fact m , Eq. (4) therefore implies that

$$\frac{1}{M} \sum_m \sum_{m' \neq m} p(m'|m) \leq \sqrt{\frac{M}{C}}. \quad (5)$$

In words, the probability of the measurement yielding the incorrect outcome, averaged over all messages, is at most $\sqrt{M/C}$, so as soon as C is significantly larger than M , a measurement on CE' can be found that will reveal the message. Our goal in this article will be to demonstrate that until this condition is met, no measurement will reveal any significant information about the message.

1.2 Structure and Notation

In Sect. 2 we define ε -locking schemes in terms of (s, η) -quasi-measurements, a new tool which we use later to extend our results to general POVMs. In Sect. 3 we present the main technical theorem (Theorem 5) for the existence of ε -locking schemes. The concentration of measure and union bound arguments which constitute the proof of the theorem, as well as the proofs of all of the remaining lemmas, corollaries, and theorems, can be found in [DFHL10]. In Sect. 4, we calculate the minimum key size to securely lock against projective measurement and in Sect. 5 we extend these results for POVMs. Finally, in Sects. 6–8 we show the necessary argument for decoding, applications to the security of quantum key distribution, and review the results.

All logarithms are taken base 2. $|A|$ will denote the dimension of Hilbert space A . However, we will often drop the $|\cdot|$. For example, the dimension of the composite system MCK is denoted by MCK (a scalar value). $A^{\otimes 2}$ will denote two identical copies of A the second of which is denoted by \bar{A} . π^A is the maximally mixed state $\frac{\mathbb{I}^A}{|A|}$. $\mathcal{U}(A)$ is the unitary group on A . $\text{Pos}(A)$ is the subset of Hermitian operators from A to A consisting of positive semidefinite matrices. $\mathcal{L}(s, \eta)$ will denote the set of all (s, η) -quasi-measurements, see Definition 3. We will use $M \cdot N$ to denote MNM^\dagger . The following three norms are defined: $\|M^{A \rightarrow B}\|_1 = \text{Tr} \sqrt{M^\dagger M}$, $\|\psi\|_2 = \sqrt{|\langle \psi | \psi \rangle|}$, and $\|M^{A \rightarrow B}\|_2 = \sqrt{\text{Tr}[M^\dagger M]}$. We will denote by $\|M^{A \rightarrow B}\|_\infty$ the largest singular value of M . $H_2(A)_\rho$ will be the Renyi 2-entropy of A , defined as $-\log \text{Tr}[\rho^2]$. $H_{\min}(A)_\rho$ will be the quantum min-entropy of A , defined as $-\log \min_{\lambda \in \mathbb{R}} \{\lambda : \rho^A \leq \lambda \mathbb{I}^A\}$. $H_{\max}(A)_\rho$ will be the quantum max-entropy of A , defined as $2 \log \text{Tr} \sqrt{\rho^A}$. We will denote by $I(A; B)_\rho$ the mutual information of A and B , defined as $H(A)_\rho + H(B)_\rho - H(AB)_\rho$.

2 Definitions

This section will present the basic definitions needed to state our results. First, it will be very convenient for us to represent measurements via superoperators in the following manner:

Definition 1 (Measurement superoperator). *We call a completely positive, trace-preserving (CPTP) map $\mathcal{M} : \mathcal{B}(A) \rightarrow \mathcal{B}(X)$ a measurement superoperator if it is of the form $\mathcal{M}(\rho) = \sum_{i=1}^N |i\rangle\langle i|^X \text{Tr}[M_i^A \rho]$, where $\{|i\rangle^A : i \in \{1, \dots, N\}\}$ is an orthonormal basis for X , each M_i^A is positive semidefinite, and $\sum_{i=1}^N M_i^A = \mathbb{I}^A$.*

These play a central role in the definition of accessible information.

Definition 2 (Accessible information [Fuc96]). *Let ρ^{AB} be a quantum state. Then, the accessible information $I_{\text{acc}}(A; B)$ is defined as*

$$I_{\text{acc}}(A; B)_\rho := \sup_{A, B} I(X; Y)_{(A \otimes B)(\rho)},$$

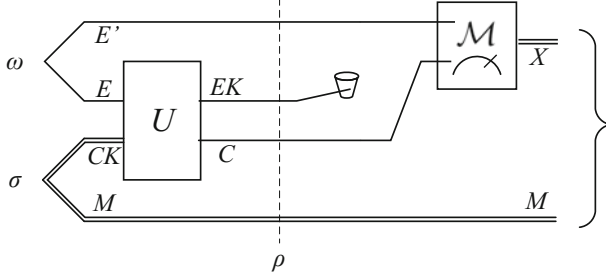


Fig. 2. A quantum circuit depicting the physical scenario with the locking-specific identifications $N \cong C \otimes K$ and $D \cong E \otimes K$ made.

where $\mathcal{A}^{A \rightarrow X}$ and $\mathcal{B}^{B \rightarrow Y}$ are measurement superoperators, and the supremum is taken over all possible superoperators.

We also need to introduce the concept of *quasi-measurements* for our analysis. They are, as their name indicates, almost measurements, but differ in three ways: they only contain rank-one elements of equal weight, they have exactly n outcomes, and the sum of all the elements does not necessarily equal the identity, but is instead bounded by $k\mathbb{I}$:

Definition 3 (Quasi-measurement). We call a superoperator $\mathcal{M}^{A \rightarrow B}$ an (s, η) -quasi-measurement if it is of the form

$$\mathcal{M}(\rho) = \frac{|A|}{s} \sum_{i=1}^s |i\rangle \langle \chi_i | \rho | \chi_i \rangle \langle i|$$

where the $|i\rangle$ index an orthonormal basis for B , and $\frac{|A|}{s} \sum_{i=1}^s |\chi_i\rangle \langle \chi_i| \leq \eta \mathbb{I}^A$. We call the set of all (s, η) -quasi-measurements on a given system, $\mathcal{L}(s, \eta)$.

The reason for introducing these, as will soon become apparent, is that they are almost equivalent to POVMs for our purposes while being much easier to handle mathematically. By definition projective measurements are simply $(A, 1)$ -quasi-measurements.

We now give the formal, strengthened definition of locking. The states in question were introduced in Sect. 1.1. However, because the cyphertext will always be smaller than or equal to the message when locking occurs, certain identifications become possible. In particular, we can assume without loss of generality that $N \cong C \otimes K$ and $D \cong E \otimes K$. Since the analysis will be performed using only C , K and E , we reproduce the illustration of the physical scenario with the identifications made in Fig. 2.

Definition 4 (ε -locking scheme). Let M, C, K, E and E' be quantum systems. Let $\rho^{MCKEE'}$ be a quantum state of the form

$$\rho^{MCKEE'} = \sum_m p_m U^{CKE} \left(|m\rangle \langle m|^M \otimes |\psi_m\rangle \langle \psi_m|^{CK} \otimes |\omega\rangle \langle \omega|^{EE'} \right) U^{CKE^\dagger}, \quad (6)$$

where the $|\psi_m\rangle$ are orthogonal and U^{CKE} is unitary. Then we call ρ an ε -locking scheme if for any measurement superoperator $\mathcal{M}^{CE' \rightarrow X}$, we have that

$$\left\| \mathcal{M} \left(\rho^{MCE'} \right) - \mathcal{M} \left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 \leq \varepsilon.$$

Note that this definition of locking is rather different from that used in previous work in the area [DHL+04, HLSW04]. Their definition involved the *accessible information* between the cyphertext and the message. Our definition implies the older one via a direct application of the Alicki-Fannes inequality [AF04].

Four quantities will be particularly useful for quantifying variations from uniform messages and maximal entanglement,

$$\Delta_{M,\infty} := 2^{\log M - H_{\min}(M)_\sigma}, \quad (7)$$

$$\Delta_{M,2} := 2^{\log M - H_2(M)_\sigma}, \quad (8)$$

$$\Delta_{E,\infty} := 2^{\log E - H_{\min}(E)_\omega}, \quad (9)$$

$$\Delta_{E,2} := 2^{\log E - H_2(E)_\omega}. \quad (10)$$

The Δ terms are used in the calculations to provide more general statements relating the entropy of the message and entanglement to the key size.

3 Concentration of the Distinguishability from Independence

The full proof of the following theorem is found in [DFHL10].

Theorem 5. *Given the quantum state $\rho^{MCKEE'} = U^{CKE} \cdot (\sigma^{MCK} \otimes \omega^{EE'})$ where U is a random unitary operator chosen according to the Haar measure, σ is as defined in Eq. (1), $E' \cong E$, and $\omega^{EE'}$ is a bipartite pure state, the following bound holds*

$$\Pr_U \left\{ \sup_{\mathcal{M} \in \mathcal{L}(s,\eta)} \left\| \mathcal{M} \left(\rho^{MCE'} \right) - \mathcal{M} \left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 > \varepsilon \right\} \leq \exp \left(2sCE \ln \left(\frac{40\sqrt{CE}}{\varepsilon} \sqrt{\Delta_{M,2}\Delta_{E,2}} \right) - \frac{(CKE)^2}{2^8 \eta^2 \Delta_{M,\infty} \Delta_{E,\infty}} \left(\varepsilon - \frac{4\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \right).$$

In the above, $\Delta_{M,\infty}$, $\Delta_{M,2}$, $\Delta_{E,2}$ and $\Delta_{E,\infty}$ are as defined in Eqs. (7), (8), (10) and (9).

4 Locking Against Projective Measurements

In this section we will only consider projective measurements, in other words $(s, \eta) = (CE', 1)$. We will also state all of the subsequent theorems in terms of qubits. For this reason we will identify $C = 2^c$, $K = 2^k$ and $E = E' = 2^e$.

Corollary 6. *Consider the locking scheme described in Definition 4 for a uniform message with maximal entanglement available at the measurement. Choose p and ϵ such that $\epsilon > 8\sqrt{1/KE}$ and $p > 2^{-2(CE)^2}$. Then the scheme will be an ϵ -locking locking scheme except with probability p so long as the measurement superoperators are restricted to projective measurements and*

$$k > 9 + 2 \log \frac{1}{\epsilon} + \frac{1}{2} \log(c + e).$$

Corollary 6, and its extension to arbitrary POVM measurements in Corollary 9 is a mathematical expression that “generically, information is locked until it can be completely decoded.” To arrive at this interpretation, recall from Eq. (4) that to achieve a decoding error of ϵ , the measurement must be supplied with the entanglement through system E' as well as a system C satisfying $c - n > 2 \log(1/\epsilon)$. Of course, this condition could never be met if the constraint $n = c + k$ is assumed, but the constraint was only made for convenience to prove the locking results. Using it to re-express Corollary 6, though, we find that the information about the message is ϵ -locked provided $c = n - k < n - 9 - 2 \log(1/\epsilon) - 1/2 \cdot \log(c + e)$. Therefore, regardless of the size of the message or the amount of entanglement, the message goes from being ϵ -locked to being decodable with average probability of error at most ϵ with the transfer of $9 + 4 \log(1/\epsilon) + 1/2 \cdot \log(c + e)$ qubits.

We also present the dependence of the minimum key size k on the various entropies of the message M and the entanglement E .

Corollary 7. *Consider the locking scheme described in Definition 4 for a message of bounded entropy with entanglement of a bounded fidelity available at the measurement. Choose ϵ and p satisfying $\epsilon > 8\Delta_{E,\infty}/\sqrt{KE}$ and $p > 2^{-2(CE)^2}$. Then the scheme will be an ϵ -locking locking scheme except with probability p so long as the measurement superoperators are restricted to projective measurements and*

$$k' + \frac{1}{2} \left(n - H_{\min}(M)_{\sigma} \right) + \frac{1}{2} \left(e - H_{\min}(E)_{\omega} \right) < k, \quad (11)$$

where we've defined k' as the lower bound given in Corollary 6, i.e.: $k' = 9 + 2 \log(1/\epsilon) + 1/2 \cdot \log(c + e)$.

5 Locking Against Generalized Measurements

We show that the results of the previous section hold not only for projective measurements, but also for general POVMs, up to very minor changes in the various constants. The main difficulty at this point is that we cannot use Theorem 5 directly, since it only gives bounds for (s, η) -quasi-measurements. We must therefore show that a general POVM behaves essentially like an (s, η) -quasi-measurement for the purposes of the theorem. Our strategy for the proof (see [DFHL10]) is probabilistic in nature: we show that doing a general POVM \mathcal{M} is mathematically equivalent to randomly selecting a measurement constructed from possible sequences of

s measurement results obtained from \mathcal{M} . With overwhelming probability, the sequence chosen is an (s, η) -quasi-measurement, and Theorem 5 then applies in this case.

Theorem 8. *Given the quantum state $\rho^{MCKEE'} = U^{CKE} \cdot (\sigma^{MCK} \otimes \omega^{EE'})$ where U is a random unitary operator chosen according to the Haar measure, σ is as defined in Eq. (1) and $\omega^{EE'}$ a bipartite pure state, then*

$$\Pr_U \left\{ \sup_{\mathcal{M}} \left\| \mathcal{M}(\rho^{MCE'}) - \mathcal{M}(\rho^M \otimes \rho^{CE'}) \right\|_1 > \varepsilon \right\} \leq \exp \left(9(CE)^2 \ln(CE) \ln \left(\frac{40\sqrt{CE}}{\varepsilon} \sqrt{\Delta_{M,2}\Delta_{E,2}} \right) - \frac{(CKE)^2}{2^{10}\Delta_{M,\infty}\Delta_{E,\infty}} \left(\varepsilon - \frac{8\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \right).$$

In the above, $\Delta_{M,\infty}$, $\Delta_{M,2}$, $\Delta_{E,2}$ and $\Delta_{E,\infty}$ are as defined in Eqs. (7), (8), (10) and (9).

A minimum key size can then be extracted in similar fashion to the previous section.

Corollary 9. *Consider the locking scheme described in Definition 4 for a uniform message and maximal entanglement available at the measurement. Choose p and ε such that $\varepsilon > 16\sqrt{1/KE}$ and $p > 2^{-9(CE)^2}$. Then the scheme will be an ε -locking locking scheme except with probability p so long as*

$$11 + 2 \log \frac{1}{\varepsilon} + \log(c + e) < k.$$

Corollary 10. *Consider the locking scheme described in Definition 4 for a message of bounded entropy with entanglement of a bounded fidelity available at the measurement. Choose p and ε such that $\varepsilon > 16\Delta_{E,\infty}/\sqrt{KE}$ and $p > 2^{-9(CE)^2}$. Then the scheme will be an ε -locking locking scheme except with probability p so long as*

$$k' + \frac{1}{2} \left(n - H_{\min}(M)_\sigma \right) + \frac{1}{2} \left(e - H_{\min}(E)_\omega \right) < k, \quad (12)$$

where we've defined k' as the lower bound given in Corollary 9, i.e.: $k' = 11 + 2 \log(1/\varepsilon) + \log(c + e)$.

6 Locking Versus Decodability

The previous sections have shown that, under certain conditions, no classical information is recoverable by the receiver. Here we aim to show that, in many regimes, these results are essentially optimal. We do this by showing that if we make the key only very slightly smaller, then with overwhelming probability,

the classical message will be decodable with a negligible error probability. In fact we prove even more: in this regime where the information is decodable, the decoder can even decode a *purification* of the classical message. In other words, in this generic scenario where U is chosen with no preferred basis, either all *classical* information is locked away, or we can decode *quantum* information. This is formalized in the next theorem.

In order to study decodability, we must discard the identifications made in Fig. 2 to study locking and return to the original scenario described by Fig. 1. Whereas k was previously the number of qubits in system K , there is no system K in Fig. 2. Instead, we define $k = n - c$, which is consistent with its earlier definition. Now, however, it might be the case that k is negative since decoding could require the ciphertext to be longer than the message.

The following theorem generalizes the discussion of Sect. 1.1 to nonuniform messages and imperfect entanglement.

Theorem 11. *If U is chosen according to the Haar measure, then the information in the scheme described in Fig. 1 is such that there exists a decoding CPTP map $\mathcal{D}^{CE' \rightarrow N}$ such that*

$$\left\| \mathcal{D} \left(\text{Tr}_D \left[U^{NE \rightarrow CD} \left(\sigma^{RMN} \otimes \omega^{E'E} \right) (U^{NE \rightarrow CD})^\dagger \right] \right) - \sigma^{RMN} \right\|_1 \leq \varepsilon$$

asymptotically almost surely, where σ^{RMN} is a purification of σ^{MN} , as long as

$$k \leq \frac{1}{2} \left(n - H_{\max}(M)_\sigma \right) - \frac{1}{2} \left(e - H_2(E)_\omega \right) - 2 \log(1/\varepsilon) - 4$$

7 Implications for the Security of Quantum Protocols Against Quantum Adversaries

When designing quantum cryptographic protocols, it is often necessary to show that a quantum adversary (“Eve”) is left with only a negligible amount of information on some secret string. An initial attempt at formalizing this idea is to say that, at the end of the protocol, regardless of what measurement Eve makes on her quantum system, the mutual information between her measurement result and the secret string is at most ε (in other words, her accessible information about the message is at most ε). This was often taken as the security definition for quantum key distribution, usually implicitly by simply not considering that the adversary might keep quantum data at the end of the protocol [LC99, SP00, NC00, GL03, LCA05] (see also discussion in [BOHL+05, RK05, KRBM07]). In [KRBM07], it is shown that this definition of security is inadequate, precisely because of possible locking effects. Indeed, this security definition does not exclude the possibility that Eve, upon gaining partial knowledge of S after the end of the protocol, could then gain more by making a measurement on her quantum register that depends on the partial information that she has learned. In [KRBM07], the authors exhibit an admittedly contrived quantum key distribution protocol which generates a secret n -bit key such that, if Eve learns

the first $n - 1$ bits, she can then learn the remaining bit by measuring her own quantum register.

The locking scheme presented above allows us to demonstrate a much more spectacular failure of this security definition. We will show that there exists a quantum key distribution protocol that ensures that an adversary has negligible accessible information about the final key, but with which an adversary can recover the entire key upon learning only a very small fraction of it.

7.1 Description of the Protocol

We will derive this faulty protocol by starting with a protocol that is truly secure, and then making Alice send a locked version of the secret string directly to Eve. We will be able to prove that regardless of what measurement Eve makes on her state, she will learn essentially no information on the string, but of course, she only needs to learn a tiny amount of information to unlock what Alice sent her. More precisely, let P be a quantum key distribution protocol such that, at the end of its execution, Alice and Bob share an n -bit string, and Eve has a quantum state representing everything that she has managed to learn about the string. We will also assume that P is a truly secure protocol: the string together with Eve's quantum state can be represented as a quantum state σ^{SE} such that $\|\sigma^{SE} - \pi^S \otimes \sigma^E\|_1 \leq \varepsilon$, where S is a quantum register holding the secret string, and E is Eve's quantum register. Now, we will define the protocol P' to be the following quantum key distribution protocol: Alice and Bob first run P to generate a string s of length n , and then Alice splits s into two parts: the first part s_k is of size $O(\log n)$, and the second part s_c contains the rest of the key. Alice then uses the classical key s_k to create a quantum state in register C that contains a locked version of s_c and sends the system C to Eve.

How secure is P' ? It is clearly very insecure, since, if Eve ever ends up learning s_k (via a known plaintext attack, for instance), she can then completely recover s_c . However, the next theorem shows that, right after the execution of P' , Eve cannot make any measurement that will reveal information about the key. In particular, P' satisfies the requirement that Eve's accessible information on the key be very low.

Theorem 12. *Let P and P' be quantum key distribution protocols as defined as above, and let ρ^{CES} be the state at the end of the execution of P' : S contains the n -bit string s , E is Eve's quantum register after the execution of P , and C contains the locked version of s_c that Alice sent to Eve. Then, for any measurement superoperator $\mathcal{M}^{CE \rightarrow X}$, there exists a state ξ^X such that*

$$\|\mathcal{M}(\rho^{CES}) - \xi^X \otimes \pi^S\|_1 \leq 2\varepsilon.$$

This also entails that

$$I_{\text{acc}}(S; CE) \leq 8\varepsilon n + 2\eta(1 - 2\varepsilon) + 2\eta(2\varepsilon)$$

via the Alicki-Fannes inequality.

Hence, we have shown that requiring that Eve’s accessible information on the generated key be low is not an adequate definition of security for quantum key distribution. We have exhibited a protocol P' which guarantees low accessible information and yet is clearly insecure due to locking effects.

8 Discussion

It is natural in physics to measure the “correlation” between two quantum physical systems using the correlation between the outcomes of measurements on those two systems. Two-point correlation functions are but the most ubiquitous examples. The results in this article demonstrate that this practice can sometimes be very misleading. The ϵ -locking quantum states exhibited in this article would reveal no correlations using any type of measurement, but enlarging one of the two systems by a small number of qubits would expose near-perfect correlation between the two systems. This is an important and counterintuitive property of information in quantum mechanical systems: measurements can be distressingly bad ways to detect correlation.

The extensive literature on quantum discord is essentially devoted to exploring the relationship between accessible, or classical, and quantum mutual information [OZ01, HV01, BKZ06]. Since the discord is defined as the gap between the quantum and classical mutual informations, locking can be viewed as the extreme case where classical mutual information doesn’t detect any of the very abundant quantum mutual information. Previous work had demonstrated that transmitting a constant number of physical qubits can cause the classical mutual information to increase from a fixed small constant to an arbitrarily large value. In this article, we have strengthened the definition of locking, replacing the mutual information by the trace distance to a product distribution. Moreover, we have shown that the locking effect still exists even when the trace distance (or the classical mutual information) is made arbitrarily small. In light of these results, claims that the discord is a robust measure of quantum correlation [WSFB09] should be treated with skepticism. While discord is certainly a signature of quantumness, its susceptibility to locking means that it is in this important respect not robust.

Previous studies of information locking had also always focused on the example of sending classical information in one of a small number of different bases unknown to the receiver. The intuition was that a receiver ignorant of the basis could not do much better than guessing the basis and then measuring. Most of the time, he would guess incorrectly and his measurement would then destroy the information. Moving away from that paradigm, in this article we consider classical information encoded using a single generic unitary transformation mixing the input information with half of an entangled state shared with the receiver. The “key” then becomes a quantum system. While the original paradigm can be recovered by eliminating the entanglement and encrypting the key quantum system with a private quantum channel, the setting considered here is strictly more general.

Indeed, we find that, for an n -bit uniform message and maximal entanglement, the information is generically ϵ -locked until the receiver is within $O(\log n/\epsilon)$ qubits of being able to completely decode the message. Our definition of locking is stronger than those previously studied and our results imply, for the first time, that the classical mutual information can be made arbitrarily small. Our method of proof in the case of projective measurements was a fairly standard discretization argument but the extension to POVM measurements required a new strategy exploiting the operator Chernoff bound. In contrast to previous studies of locking, we do not require the message to be uniformly distributed, working instead with a min-entropy bound on the distribution of messages. In that case, we found that the key size was at most the gap between the max- and min-entropies of the message, modulo the logarithmic terms that dominate in the uniform situation.

For information theorists, this may appear reminiscent of a strong converse to a channel capacity problem. Roughly, a strong converse theorem states that any attempt to transmit above the channel capacity will result in the decoding error probability approaching one. In our setting, the analog of the strong converse would be a matching lower bound to Eq. (5) of the form

$$1 - \epsilon < \frac{1}{M} \sum_m \sum_{m' \neq m} p(m'|m) \quad (13)$$

whenever $C < M$, indicating that the probability of incorrectly decoding the message is at least $1 - \epsilon$. What we prove here is much stronger. Equation (13) doesn't rule out the possibility of being able to pin the message down to some relatively small set. More generally, it doesn't imply a small mutual information between the message and the measurement outcome. Information locking does imply these stronger statements.

As such, information locking has a natural cryptographic interpretation even if we haven't emphasized it in this article. The special case of our scenario mentioned above, with no entanglement and a quantum key encrypted using a private quantum channel, leads to a method for encrypting classical messages using a secret key of size independent of the length of the message. Similarly, information locking schemes can be used to construct string commitment protocols with surprisingly good parameters [BCH+06, BCH+08]. These cryptographic applications are emphasized in the companion article [FHS10].

To the extent that random unitary transformations provide good models of black hole evaporation, our results might also have implications for that process. Oppenheim and Smolin had previously suggested that information locking could rescue the long-lived remnant hypothesis [SO06]. In essence, their idea was that a remnant with a small number of states could lock all the information of a large black hole, thereby evading the inconsistencies with low energy physics that arise from having large numbers of remnant species [ACN87, CW87]. Their proposal, however, relied on previously studied locking states that treated the encoded message and the key very differently. Consequently, the proposal required that the black hole keep hold of the key until the very last moments of its evaporation,

implying some ad hoc dynamical distinction between encoded message and key in the evaporation process. Our results imply that *if* the dynamics are well-modeled by a Haar random unitary transformation, then any small portion of the output system can be used as the key. No ad hoc distinction is necessary.

Ironically, the information locking effect is also perfectly compatible with the rapid release of information from a black hole predicted in [HP07], assuming a unitary evaporation process. That article observed that if a black hole is already highly entangled with Hawking radiation from an earlier time, then messages would be released from the black hole in the Hawking radiation once the black hole dynamics had sufficiently “scrambled” the message with internal black hole degrees of freedom. By virtue of the fact that we treat generic unitary transformations acting on a message and half of an entangled state, our results apply to the setting of that paper and the followup [SS08]. Specifically, our results imply that in the case of a larger message, *no* information about the message could be obtained from the Hawking radiation until moments before it could *all* be obtained. The conclusion depends, of course, on whether the random unitary transformation is a good model of the evaporation process. While the generic unitary transformations considered here would take exponential time to implement on a quantum computer, the follow-up article [FHS10] shows, at least, that locking can be achieved with a quantum circuit of depth only slightly superlinear in the number of qubits in the system. Other attempts to apply random unitary transformations to the black hole information problem, such as [Llo06,BSZ09], will be affected similarly by information locking.

To summarize, this article defined information locking more stringently than previously and nonetheless found that this stronger form of locking is generic: if information is encoded using a random unitary transformation, then it will either be decodable or locked. Almost no middle ground occurs. This observation has implications for cryptography and, potentially, for black hole physics.

Acknowledgments. Andreas Winter has independently established some locking results for generic unitary transformations. We would like to thank Jonathan Oppenheim for helpful discussions and the Mittag-Leffler Institute for its kind hospitality. This research was supported by the Canada Research Chairs program, the Perimeter Institute, CIFAR, CFI, FQRNT’s INTRIQ, MITACS, NSERC, ORF, ONR through grant N000140811249, QuantumWorks, and the Swiss National Science Foundation through grant no. 200021-119868.

References

- ACN87. Aharonov, Y., Casher, A., Nussinov, S.: The unitarity puzzle and Planck mass stable particles. *Phys. Lett. B* **191**, 51–55 (1987)
- ADHW09. Abeyesinghe, A., Devetak, I., Hayden, P., Winter, A.: The mother of all protocols: Restructuring quantum information’s family tree. In: *Proceedings of the Royal Society A*, vol. 465, pp. 2537–2563 (2009). [quant-ph/0606225](#)
- AF04. Alicki, R., Fannes, M.: Continuity of quantum mutual information. *J. Phys. A. Math. Gen.* **37**(5), L55–L57 (2004). [quant-ph/0312081](#)

- BCH+06. Buhrman, H., Christandl, M., Hayden, P., Lo, H.-K., Wehner, S.: Security of quantum bit string commitment depends on the information measure. *Phys. Rev. Lett.* **97**, 250501 (2006). arXiv:quant-ph/0609237
- BCH+08. Buhrman, H., Christandl, M., Hayden, P., Lo, H.-K., Wehner, S.: Possibility, impossibility, and cheat-sensitivity of quantum bit string commitment. *Phys. Rev. A* **78**, 022316 (2008). arXiv:quant-ph/0504078
- BKZ06. Blume-Kohout, R., Zurek, W.H.: Quantum Darwinism: entanglement, branches, and the emergence of classicality of redundantly stored quantum information. *Phys. Rev. A* **73**, 062310 (2006)
- BOHL+05. Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 386–406. Springer, Heidelberg (2005)
- BSZ09. Braunstein, S.L., Sommers, H.J., Zyczkowski, K.: Entangled black holes as ciphers of hidden information (2009). arXiv:0907.0739
- CW87. Carlitz, R.D., Willey, R.S.: Lifetime of a black hole. *Phys. Rev. D* **36**, 2336–2341 (1987)
- DFHL10. Dupuis, F., Florjanczyk, J., Hayden, P., Leung, D.: Locking classical information (2010). arXiv:1011.1612
- DHL+04. DiVincenzo, D.P., Horodecki, M., Leung, D.W., Smolin, J.A., Terhal, B.M.: Locking classical correlation in quantum state. *Phys. Rev. Lett.* **92**, 067902 (2004). quant-ph/0303088
- FHS10. Fawzi, O., Hayden, P., Sen, P.: From low-distortion embeddings to metric uncertainty relations and information locking (2010). arxiv:1010.3007v3
- Fuc96. Fuchs, C.A.: Distinguishability and accessible information in quantum theory. Ph.D. thesis, University of New Mexico (1996). quant-ph/9601020
- GL03. Gottesman, D., Lo, H.-K.: Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theor.* **49**(2), 457–475 (2003). quant-ph/0105121
- HLSW04. Hayden, P., Leung, D.W., Shor, P., Winter, A.: Randomizing quantum states: constructions and applications. *Comm. Math. Phys.* **250**(2), 371–391 (2004). quant-ph/0307104
- HP07. Hayden, P., Preskill, J.: Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.* **07**(09), 120 (2007)
- HV01. Henderson, L., Vedral, V.: Classical, quantum and total correlations. *J. Phys. A Math. Gen.* **34**(35), 6899 (2001)
- KRBM07. König, R., Renner, R., Bariska, A., Maurer, U.: Locking of accessible information and implications for the security of quantum cryptography. *Phys. Rev. Lett.* **98**, 140502 (2007). quant-ph/0512021
- LC99. Lo, H.-K., Chau, H.-F.: Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**(5410), 2050–2056 (1999). quant-ph/9803006
- LCA05. Lo, H.-K., Chau, H.-F., Ardehali, M.: Efficient quantum key distribution scheme and proof of its unconditional security. *J. Cryptol.* **18**, 133 (2005). quant-ph/0011056
- Llo06. Lloyd, S.: Almost certain escape from black holes in final state projection models. *Phys. Rev. Lett.* **96**, 061302 (2006)
- NC00. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, New York (2000)
- OZ01. Ollivier, H., Zurek, W.H.: Quantum discord: a measure of the quantumness of correlations. *Phys. Rev. Lett.* **88**, 017901 (2001)

- RK05. Renner, R., König, R.: Universally composable privacy amplification against quantum adversaries. In: Second Theory of Cryptography Conference (TCC 2005), vol. 3378, pp. 407–425 (2005). [quant-ph/0403133](#)
- SO06. Smolin, J., Oppenheim, J.: Locking information in black holes. *Phys. Rev. Lett.* **96**(8), 081302 (2006)
- SP00. Shor, P., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 1 (2000). [quant-ph/0003004](#)
- SS08. Sekino, Y., Susskind, L.: Fast scramblers. *J. High Energy Phys.* **10**, 65 (2008). [arXiv:0808.2096](#)
- WSFB09. Werlang, T., Souza, S., Fanchini, F.F., Villas Boas, C.J.: Robustness of quantum discord to sudden death. *Phys. Rev. A* **80**, 024103 (2009)

Telescopic Relative Entropy

Koenraad M.R. Audenaert^(✉)

Department of Mathematics, Royal Holloway, University of London,
Egham TW20 0EX, UK
koenraad.audenaert@rhul.ac.uk

Abstract. We introduce the telescopic relative entropy (TRE), which is a new regularisation of the relative entropy related to smoothing, to overcome the problem that the relative entropy between pure states is either zero or infinity and therefore useless as a distance measure in this case. We study basic properties of this quantity, and find interesting relationships between the TRE and the trace norm distance. We then exploit the same techniques to obtain a new and shorter proof of an upper bound on the relative Tsallis entropies in terms of the trace norm distance, $1 - \text{Tr} \rho^{1-p} \sigma^p \leq \|\rho - \sigma\|_1 / 2$.

1 Introduction

The quantum relative entropy between two quantum states ρ and σ , $S(\rho || \sigma) = \text{Tr} \rho(\log \rho - \log \sigma)$, is a non-commutative generalisation of the Kullback-Leibler distance between probability distributions. Because of its strong mathematical connections with von Neumann entropy, and its interpretation as an optimal asymptotic error rate in quantum hypothesis testing (in the context of Stein's lemma) relative entropy is widely used as a (non-symmetric) distance measure between states [7].

One of its drawbacks, however, is that for non-faithful (rank-deficient) states the relative entropy can be infinite. More precisely, the relative entropy is infinite when there exists a pure state ψ such that $\langle \psi | \sigma | \psi \rangle$ is zero while $\langle \psi | \rho | \psi \rangle$ is not. In particular, relative entropy is useless as a distance measure between pure states, since it is infinite for pure ρ and σ , unless ρ and σ are exactly equal (in which case it always gives 0).

There are various possibilities to overcome this deficiency. In [5], Lendi, Farhadmotamed and van Wonderen proposed a *regularised relative entropy* as

$$R(\rho || \sigma) = c_d S \left(\frac{\rho + \mathbb{1}_d}{1 + d} \left\| \frac{\sigma + \mathbb{1}_d}{1 + d} \right. \right),$$

where d is the dimension, and c_d is a normalisation constant. This only works for finite-dimensional states.

Another possibility, also useful for infinite dimensional states, is to apply a smoothing process. One can define the *smooth relative entropy* between states

ρ and τ as the infimum of the ordinary relative entropy between ρ and another state τ , where τ is constrained to be ϵ -close to σ in trace norm distance:

$$S_\epsilon(\rho \parallel \sigma) = \inf_{\tau} \{S(\rho \parallel \tau) : \tau \geq 0, \text{Tr } \tau \leq 1, \|\tau - \sigma\|_1 \leq \epsilon\}.$$

This form of smoothing has already been applied to Renyi entropies and max-relative entropy [3, 9], giving rise to a quantity with an operational interpretation, but it could equally well be applied to ordinary relative entropy.

In the case of the ordinary relative entropy there is a simple canonical choice for σ that achieves the same purpose of regularisation but without having to find the exact minimiser. Namely, we can take that τ that is collinear with ρ and σ ; i.e. $\tau = a\rho + (1 - a)\sigma$ (with $a = \epsilon / \|\rho - \sigma\|_1$).

By operator monotonicity of the logarithm, we have

$$\log(\tau) = \log(a\rho + (1 - a)\sigma) \geq \log(a\rho),$$

and, therefore,

$$\begin{aligned} S(\rho \parallel \tau) &= \text{Tr } \rho(\log \rho - \log \tau) \\ &\leq \text{Tr } \rho(\log \rho - \log(a\rho)) \\ &= -\log a. \end{aligned}$$

Thus, $S(\rho \parallel \tau)$ is bounded above by $-\log a$, which is finite for $0 < a < 1$. It therefore makes perfect sense to normalise $S(\rho \parallel \tau)$ by dividing it by $-\log a$, producing a quantity that is always between 0 and 1.

These observations led us to define what we call the *telescopic relative entropy* (TRE), a particular regularisation of the ordinary relative entropy that is also defined in Hilbert spaces of infinite dimension:

Definition 1. For fixed $a \in (0, 1)$, the a -telescopic relative entropy between states ρ and σ is given by

$$S_a(\rho \parallel \sigma) := \frac{1}{-\log(a)} S(\rho \parallel a\rho + (1 - a)\sigma). \quad (1)$$

Furthermore, we define

$$S_0(\rho \parallel \sigma) := \lim_{a \rightarrow 0} S_a(\rho \parallel \sigma) \quad (2)$$

$$S_1(\rho \parallel \sigma) := \lim_{a \rightarrow 1} S_a(\rho \parallel \sigma). \quad (3)$$

We'll show below that these limits exist.

The origin of the name is that the operation $\sigma \mapsto a\rho + (1 - a)\sigma$ acts like a 'telescope' with 'magnification factor' $1/(1 - a)$, bringing the state σ closer to the 'vantage point' ρ and bringing observed pairs of states σ_i closer to each other.

The purpose of this paper is to initiate the study of this quantity. The telescoping operation $\sigma \mapsto a\rho + (1 - a)\sigma$ and subsequent scaling of the relative

entropy by $1/(-\log a)$ may seem like a fairly innocuous operation, but has a number of far-reaching and sometimes unexpected consequences. Because of the linearity of the telescoping operation, the TRE inherits most of the desirable properties of the ordinary relative entropy. However, a host of additional relations in the form of sharp inequalities may be derived that in the case of the ordinary relative entropy simply make no sense, because the constants appearing in the inequality would be infinite. At the end of this paper, we briefly consider the telescoping operation in the context of the relative Tsallis entropies. We exploit the same techniques used for the TRE to obtain a new and shorter proof of a lower bound on the relative Tsallis entropies in terms of the trace norm distance, $1 - \text{Tr } \rho^{1-p} \sigma^p \leq \|\rho - \sigma\|_1 / 2$ [1].

2 Preliminaries

For any self-adjoint operator X on a Hilbert space \mathcal{H} , we denote by $\text{supp } X$ the support of X , i.e. the subspace of \mathcal{H} which is the orthogonal complement of $\ker X$, the kernel of X . The projector on the support of X will be denoted by $\{X\}$. We denote by P_X the orthogonal projector from \mathcal{H} onto $\text{supp } X$, so that P_X^* is the injection of $\text{supp } X$ back into \mathcal{H} . Thus $P_X^* P_X = \{X\}$. The *compression of A to the support of X* , which we'll denote by $A|_X$, is the operator with domain $\text{supp } X$ given by

$$A|_X = P_X A P_X^*.$$

By definition, for any positive operator $X \geq 0$, we have $X|_X > 0$, strictly.

Two quantum states are mutually orthogonal, denoted $\rho \perp \sigma$, iff $\text{Tr } \rho \sigma = 0$.

For any self-adjoint operator X , X_+ will denote the positive part $X_+ = (X + |X|)/2$. It features in an expression for the trace norm distance between states:

$$T(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1 = \text{Tr } (\rho - \sigma)_+. \quad (4)$$

The trace of the positive part has the variational characterisation $\text{Tr } X_+ = \max_P \text{Tr } X P$, where the maximisation is over all self-adjoint projectors. Hence, for all such projectors P , $\text{Tr } X P \leq \text{Tr } X_+$.

The Pinsker bound is a lower bound on the ordinary relative entropy in terms of trace norm distance [7].

$$S(\rho || \sigma) \geq 2T(\rho, \sigma)^2. \quad (5)$$

No upper bound in terms of the trace norm distance is possible, because the relative entropy can be infinite.

We will also need the following integral representation of the logarithm: for $x > 0$, we have

$$\log x = \int_0^\infty ds \left(\frac{1}{1+s} - \frac{1}{x+s} \right). \quad (6)$$

This immediately provides an integral representation for the telescopic relative entropy:

$$\begin{aligned} S_a(\rho \parallel \sigma) &= \frac{1}{\log a} \int_0^\infty ds \operatorname{Tr} \rho[(\rho + s)^{-1} - (a\rho + (1-a)\sigma + s)^{-1}] \end{aligned} \quad (7)$$

$$= \frac{1}{\log a} \int_0^\infty ds \operatorname{Tr} \rho(\rho + s)^{-1} (1-a)(\sigma - \rho) (a\rho + (1-a)\sigma + s)^{-1}. \quad (8)$$

Another integral we will encounter is $\int_0^\infty ds x/(x+s)^2$. For $x = 0$, the integral obviously gives 0. For $x > 0$ it gives 1. Hence

$$\int_0^\infty ds (\rho + s)^{-1} \rho (\rho + s)^{-1} = \{\rho\}. \quad (9)$$

From integral representation (6) we get an expression for the Fréchet derivative of the matrix logarithm:

$$\left. \frac{d}{dt} \right|_{t=0} \log(A + t\Delta) = \int_0^\infty ds (A + s)^{-1} \Delta (A + s)^{-1}.$$

It will be useful to introduce the following linear map, for $A \geq 0$:

$$\mathcal{T}_A(\Delta) = \int_0^\infty ds (A + s)^{-1} \Delta (A + s)^{-1}. \quad (10)$$

Thus

$$\left. \frac{d}{dt} \right|_{t=0} \log(A + t\Delta) = \mathcal{T}_A(\Delta). \quad (11)$$

It's easy to check that for $A \geq 0$, $\mathcal{T}_A(A) = \{A\}$. Thus, for $A > 0$, we have $\mathcal{T}_A(A) = \mathbb{1}$.

From this integral representation it also follows that, for any self-adjoint A , \mathcal{T}_A preserves the positive semidefinite order: if $X \leq Y$, then $\mathcal{T}_A(X) \leq \mathcal{T}_A(Y)$. By cyclicity of the trace, we see that the map \mathcal{T}_A is self-adjoint: $\operatorname{Tr} B\mathcal{T}_A(\Delta) = \operatorname{Tr} \Delta\mathcal{T}_A(B)$. Moreover, the map is positive semi-definite, in the sense that $\operatorname{Tr} \Delta\mathcal{T}_A(\Delta)$ is positive for any self-adjoint Δ . This follows from the integral representation and the fact that for positive X and self-adjoint Y , $\operatorname{Tr} XYXY = \operatorname{Tr} (X^{1/2}YX^{1/2})^2 \geq 0$.

3 Basic Properties of Telescopic Relative Entropy

From the discussion in the Introduction, we recall that the value of the telescopic relative entropy is always between 0 and 1, even for non-faithful states. Furthermore, it inherits many desirable properties from the ordinary relative entropy: positivity, the fact that it is only zero when ρ and τ are equal (provided $a > 0$), joint convexity in its arguments, and monotonicity under CPT maps.

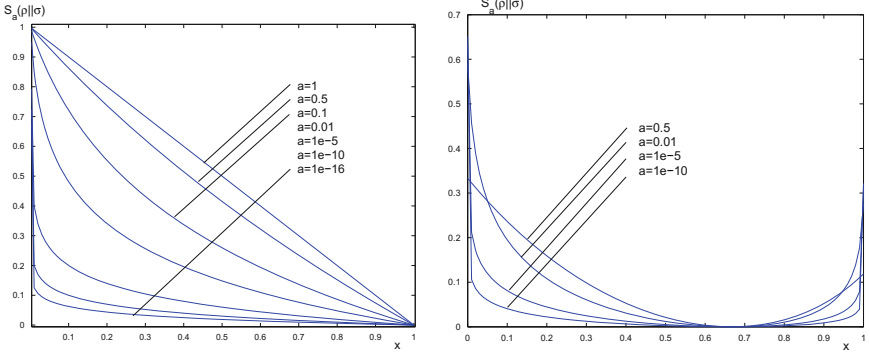


Fig. 1. (a) Telescopic relative entropy $S_a(\rho||\sigma)$ between state $\rho = |0\rangle\langle 0|$ and state $\sigma = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$, with x ranging from 0 to 1, and for various values of a ; (b) same but for $\rho = (2/3)|0\rangle\langle 0| + (1/3)|1\rangle\langle 1|$.

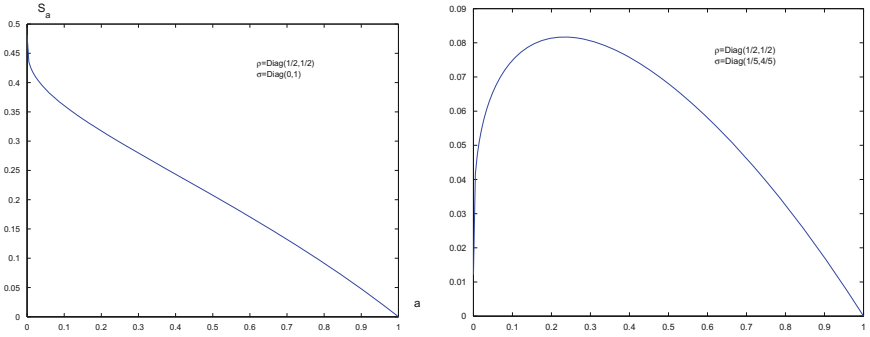


Fig. 2. (a) Telescopic relative entropy $S_a(\rho||\sigma)$ between state $\rho = \mathbb{1}_2/2$ and state $\sigma = |1\rangle\langle 1|$, with a ranging from 0 to 1; (b) same but for $\sigma = (|0\rangle\langle 0| + 4|1\rangle\langle 1|)/5$.

As we do not restrict the arguments of the telescopic relative entropy to states, the definition is also applicable (in a useful way) to non-negative scalars:

$$S_a(b||c) = \frac{b(\log b - \log(ab + (1-a)c))}{-\log a}. \quad (12)$$

For illustrative purposes, we graph the telescopic relative entropy for a variety of qubit state pairs, in Figs. 1 and 2.

3.1 S_0 and S_1

One might think that the 1-telescopic relative entropy would be quite useless, because for $a = 1$, $S(\rho||a\rho + (1-a)\sigma) = S(\rho||\rho) = 0$. Nevertheless, it is a non-trivial quantity due to the normalisation by $1/(-\log a)$. Likewise, one might mistakenly think S_0 is essentially the ordinary relative entropy; it is far from it,

and for the same reason. Indeed, for any pair of states with finite ordinary relative entropy, e.g. when both states are faithful, S_0 is 0, due to the normalisation. The 0-telescopic relative entropy shows its true colours exactly in those cases when the ordinary relative entropy yields $+\infty$.

In fact, for S_0 and S_1 we have the following closed form expressions:

Theorem 1. *For any pair of states ρ, σ ,*

$$S_0(\rho \parallel \sigma) = 1 - \text{Tr } \rho\{\sigma\} \quad (13)$$

$$S_1(\rho \parallel \sigma) = 1 - \text{Tr } \sigma\{\rho\}. \quad (14)$$

In particular, when σ is pure, $S_0(\rho \parallel \sigma) = 1 - \text{Tr } \rho\sigma$, and when ρ is pure, $S_1(\rho \parallel \sigma) = 1 - \text{Tr } \rho\sigma$. When σ is faithful, $S_0(\rho \parallel \sigma) = 0$; when ρ is faithful, $S_1(\rho \parallel \sigma) = 0$.

Proof. Consider first the limit $a \rightarrow 1$. Using de l'Hôpital's rule we find

$$\lim_{a \rightarrow 1} \frac{1-a}{-\log a} = 1.$$

Hence, by representation (8),

$$\lim_{a \rightarrow 1} S_a(\rho \parallel \sigma) = - \int_0^\infty ds \text{Tr } \rho(\rho + s)^{-1} (\sigma - \rho) (\rho + s)^{-1}.$$

Therefore, from (9) we get the required

$$\lim_{a \rightarrow 1} S_a(\rho \parallel \sigma) = -\text{Tr } (\sigma - \rho)\{\rho\} = 1 - \text{Tr } \sigma\{\rho\}.$$

For the limit $a \rightarrow 0$ some more work is needed. Let us w.l.o.g. assume that $(\rho + \sigma)/2$ is faithful; otherwise we take the compression of ρ and σ to the support of $(\rho + \sigma)/2$. Again we use an integral representation, but in its more basic form (7). To calculate the limit $a \rightarrow 0$ we apply de l'Hôpital's rule to the whole expression and get

$$\begin{aligned} & S_0(\rho \parallel \sigma) \\ &= \lim_{a \rightarrow 0} a \frac{d}{da} \int_0^\infty ds \text{Tr } \rho[(\rho + s)^{-1} - (a\rho + (1-a)\sigma + s)^{-1}] \\ &= \lim_{a \rightarrow 0} \int_0^\infty ds \text{Tr } a\rho(a\rho + (1-a)\sigma + s)^{-1} (\rho - \sigma) (a\rho + (1-a)\sigma + s)^{-1} \\ &= \lim_{a \rightarrow 0} \int_0^\infty ds \text{Tr } (\rho - \sigma)(a\rho + (1-a)\sigma + s)^{-1} a\rho (a\rho + (1-a)\sigma + s)^{-1}. \end{aligned}$$

Here, the first factor a comes from the derivative of $\log a$.

Because of our assumption that $(\rho + \sigma)/2$ is faithful, $a\rho + (1-a)\sigma$ is faithful for any $a \in (0, 1)$. Therefore, the integral

$$\int_0^\infty ds (a\rho + (1-a)\sigma + s)^{-1} (a\rho + (1-a)\sigma) (a\rho + (1-a)\sigma + s)^{-1}$$

yields the identity operator $\mathbb{1}$. Using this fact, we can rewrite our last expression for S_0 as

$$\begin{aligned}
 S_0(\rho \parallel \sigma) &= \lim_{a \rightarrow 0} \text{Tr}(\rho - \sigma) \left[\mathbb{1} - \int_0^\infty ds \right. \\
 &\quad \left. (a\rho + (1-a)\sigma + s)^{-1} (1-a)\sigma (a\rho + (1-a)\sigma + s)^{-1} \right] \\
 &= \text{Tr}(\rho - \sigma) \left[\mathbb{1} - \int_0^\infty ds (\sigma + s)^{-1} \sigma (\sigma + s)^{-1} \right] \\
 &= \text{Tr}(\rho - \sigma)(\mathbb{1} - \{\sigma\}) \\
 &= 1 - \text{Tr} \rho \{\sigma\},
 \end{aligned}$$

as required. \square

3.2 Pure States

From Theorem 1 we can derive the equalities

$$S_0(\rho \parallel \sigma) = S_1(\rho \parallel \sigma) = T(\rho, \sigma)^2, \quad (15)$$

for pure ρ and σ .

In fact, when ρ and σ are pure, there is a one-to-one relation between $S_a(\rho \parallel \sigma)$ and $T(\rho, \sigma)$ for any value of $a \in [0, 1]$. Although the relation is somewhat complicated, in practice it shows that $S_a(\rho \parallel \sigma)$ is only slightly bigger than $T(\rho, \sigma)^2$ for $a \in (0, 1)$.

Theorem 2. *Let ρ, σ be two pure states with trace norm distance $t = \|\rho - \sigma\|_1/2$. Then, for $a \in (0, 1)$,*

$$S_a(\rho \parallel \sigma) = \frac{1}{-2 \log a} \left(-\log \frac{w}{4} - \frac{1-w/(2a)}{\sqrt{1-w}} \log \frac{1+\sqrt{1-w}}{1-\sqrt{1-w}} \right), \quad (16)$$

where

$$w := 4a(1-a)t^2. \quad (17)$$

Proof. By a suitable unitary transformation, the problem can be transformed to a two-dimensional one, with in particular

$$\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1-t & \sqrt{t(1-t)} \\ \sqrt{t(1-t)} & t \end{pmatrix}.$$

The telescopic relative entropy is then given by

$$S_a(\rho \parallel \sigma) = \frac{1}{-\log a} (-\log (a\rho + (1-a)\sigma))_{1,1}$$

and after some basic calculations this reduces to the given formula. \square

For example, let ρ and σ be two pure two-level states, with the angle between their respective Bloch vectors equal to θ . Since their trace norm distance is equal to $t = |\sin(\theta/2)|$, we have $w = 2a(1-a)(1 - \cos \theta)$.

4 Comparison to Trace Norm Distance

In this section, we provide bounds on the telescopic relative entropy in terms of the trace norm distance.

It's very easy to derive a lower bound from the Pinsker lower bound on the ordinary relative entropy (5).

Theorem 3. *For two quantum states ρ, σ ,*

$$S_a(\rho \parallel \sigma) \geq \frac{(1-a)^2}{-\log(a)} 2T(\rho, \sigma)^2. \quad (18)$$

Proof. Noting that $T(\rho, \tau) = (1-a)T(\rho, \sigma)$, this is a trivial consequence of the bound $S(\rho \parallel \tau) \geq 2T(\rho, \tau)^2$. \square

While there is no upper bound on the ordinary relative entropy in terms of the trace norm distance, we can find an upper bound on the telescopic relative entropy. This bound has a very simple form, but is nevertheless the strongest one possible.

Theorem 4. *With $\tau = a\rho + (1-a)\sigma$,*

$$S(\rho \parallel \tau) \leq -\log(a)T(\rho, \sigma). \quad (19)$$

This immediately gives our first important relation for the TRE.

Corollary 1. *For any $a \in (0, 1)$,*

$$S_a(\rho \parallel \sigma) \leq T(\rho, \sigma). \quad (20)$$

Equality can be obtained for any value of $t = T(\rho, \sigma)$ in dimension 3 and higher by choosing $\rho = \text{Diag}(t, 0, 1-t)$ and $\sigma = \text{Diag}(0, t, 1-t)$.

A second and unsuspected corollary is a strengthening of a very well-known inequality (see, e.g. [8], Theorem 3.7) for the entropy of an ensemble of two states: for any two states ρ, σ and $(p, 1-p)$ a probability distribution,

$$S(p\rho + (1-p)\sigma) \leq pS(\rho) + (1-p)S(\sigma) + h(p), \quad (21)$$

where $h(p) = -p \log p - (1-p) \log(1-p)$ is the binary Shannon entropy. This inequality is equivalent to *subadditivity of the von Neumann entropy* (w.r.t. ordinary addition) for positive (non-normalised) operators: for any $A, B \geq 0$

$$S(A+B) \leq S(A) + S(B). \quad (22)$$

Indeed, substituting $A = p\rho$ and $B = (1-p)\sigma$ yields (21).

The quantity $S(p\rho + (1-p)\sigma) - (pS(\rho) + (1-p)S(\sigma))$ is known as the *Holevo quantity* $\chi(\mathcal{E})$ for the ensemble $\mathcal{E} = \{(p, \rho), (1-p, \sigma)\}$ (of cardinality 2). The bound says that $\chi(\mathcal{E}) \leq h(p)$. Using Theorem 4, we get a sharper bound:

Corollary 2. For any ensemble $\mathcal{E} = \{(p, \rho), (1 - p, \sigma)\}$ of cardinality 2,

$$\chi(\mathcal{E}) \leq h(p) T(\rho, \sigma). \quad (23)$$

Proof. Let $\tau = p\rho + (1 - p)\sigma$. Notice that $S(\tau) - (pS(\rho) + (1 - p)S(\sigma))$ is equal to $pS(\rho || \tau) + (1 - p)S(\sigma || \tau)$. Applying inequality (19) to both terms gives $-p \log(p) T(\rho, \sigma) - (1 - p) \log(1 - p) T(\rho, \sigma)$ as an upper bound. \square

Question. As inequality (21) immediately generalises to ensembles of any cardinality ([6], Sect. 11.3.6), namely, $\chi(\mathcal{E}) \leq H(p)$ (where $H(p)$ is the Shannon entropy of the probability distribution of \mathcal{E}), it is fair to ask for a similar generalisation of the Corollary.

In [10], related upper bounds were studied. For cardinality 2, a bound was found in terms of the probability p and the Uhlmann fidelity between ρ and σ , $F = \|\sqrt{\rho}\sqrt{\sigma}\|_1$. For cardinality 3, a generalisation was conjectured in [4]. For general cardinalities a bound was proven that is sharper than $H(p)$ and is expressed in terms of the so-called exchange entropy [10].

We now present the proof of Theorem 4. It relies on the properties of the Fréchet derivative of the matrix logarithm given in Sect. 2.

Proof of Theorem 4.

Let ρ and σ be two given states, and $\tau = a\rho + (1 - a)\sigma$. Define $s = (1 - a)/a$, which is a non-negative number. Thus $\tau = a(\rho + s\sigma)$. W.l.o.g. we will assume that $\rho + s\sigma$ is full rank.

Let $\Delta := \rho - \sigma$, $t := T(\rho, \sigma) = \|\Delta\|_1 / 2$ and $\omega := \Delta/t$. Obviously, ω has trace 0 and trace norm 2. Let its Jordan decomposition be $\omega = \omega_+ - \omega_-$. Thus $\omega \leq \omega_+$ and $\text{Tr } \omega_+ = \text{Tr } \omega_- = 1$.

Now consider the expression $s \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(\sigma)$. Since $\mathcal{T}_{\rho+s\sigma}(\sigma) \geq 0$, and $\omega \leq \omega_+$, we have

$$\begin{aligned} s \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(\sigma) &= \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(s\sigma) \\ &\leq \text{Tr } \omega_+ \mathcal{T}_{\rho+s\sigma}(s\sigma) \\ &\leq \text{Tr } \omega_+ \mathcal{T}_{\rho+s\sigma}(\rho + s\sigma) \\ &= \text{Tr } \omega_+ \mathbf{1} \\ &= 1. \end{aligned}$$

Then, noting that $\rho = \sigma - t\omega$,

$$\begin{aligned} (1 + s) \text{Tr } \rho \mathcal{T}_{\rho+s\sigma}(\sigma) &= \text{Tr } (\rho + s\rho) \mathcal{T}_{\rho+s\sigma}(\sigma) \\ &= \text{Tr } (\rho + s\sigma - st\omega) \mathcal{T}_{\rho+s\sigma}(\sigma) \\ &= \text{Tr } (\rho + s\sigma) \mathcal{T}_{\rho+s\sigma}(\sigma) - ts \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(\sigma) \\ &= \text{Tr } \sigma \mathcal{T}_{\rho+s\sigma}(\rho + s\sigma) - ts \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(\sigma) \\ &= \text{Tr } \sigma - ts \text{Tr } \omega \mathcal{T}_{\rho+s\sigma}(\sigma) \\ &\geq 1 - t. \end{aligned}$$

Therefore,

$$\mathrm{Tr} \rho \mathcal{T}_{\rho+s\sigma}(\sigma) \geq \frac{1-t}{1+s}.$$

Integrating over s from 0 to $(1-a)/a$ then yields

$$\mathrm{Tr} \rho \log(\rho + (1-a)\sigma/a) - \mathrm{Tr} \rho \log(\rho) \geq (1-t) \log(1/a),$$

which becomes, after adding $\log a$ to both sides,

$$\mathrm{Tr} \rho \log(a\rho + (1-a)\sigma) - \mathrm{Tr} \rho \log(\rho) \geq t \log(a),$$

which is equivalent to the statement of the theorem. \square

5 Cases of Maximality

The following theorem characterises those cases when the telescopic relative entropy achieves its maximal value of 1.

Theorem 5. *For any $a \in (0, 1)$, $S_a(\rho \parallel \sigma) = 1$ iff $\rho \perp \sigma$.*

Proof. We have $S_a(\rho \parallel \sigma) = 1$ iff $\mathrm{Tr} \rho \log(a\rho) = \mathrm{Tr} \rho \log(a\rho + (1-a)\sigma)$ or, putting $X = a\rho$ and $Y = (1-a)\sigma$, iff $\mathrm{Tr} X \log X = \mathrm{Tr} X \log(X + Y)$. Since $X, Y \geq 0$, operator monotonicity of the logarithm gives $\mathrm{Tr} X \log(X + Y) \geq \mathrm{Tr} X \log X$. We want to characterise the cases of equality. One direction is obvious; if X and Y are orthogonal, clearly we have equality.

To prove that there are no other possibilities, assume $\mathrm{Tr} X(\log(X + Y) - \log X) = 0$. Consider first the case $X > 0$. Define $Z = \log(X + Y) - \log X$. Because of monotonicity of the logarithm we have $Z \geq 0$, hence the assumption, $\mathrm{Tr} XZ = 0$, implies $Z = 0$, i.e. $\log(X + Y) = \log X$. As the logarithm is invertible on the set of positive operators, this can only be true iff $Y = 0$.

Now consider the general case $X \geq 0$, and assume X has a non-trivial kernel. Then we can decompose the Hilbert space \mathcal{H} as the direct sum $\mathcal{H} = \mathrm{supp} X \oplus \ker X$. We have $X = X|_X \oplus 0$, with $X|_X > 0$. W.l.o.g. we can assume that $X + Y > 0$, so that its logarithm is well-defined. By the convention to take $\lim_{x \rightarrow 0} x \log x = 0$, $\mathrm{Tr} X \log X$ is well-defined, too, and equal to $\mathrm{Tr} X|_X \log X|_X$. The assumption $\mathrm{Tr} X(\log(X + Y) - \log X) = 0$ can then be written as $\mathrm{Tr} X|_X(\log(X + Y)|_X - \log(X|_X)) = 0$. Let us therefore define $Z = \log(X + Y)|_X - \log(X|_X)$.

As can be expected, $Z \geq 0$. To prove this, put $X' = X|_X \oplus \epsilon \mathbb{1}$. By operator monotonicity of the logarithm, $\log(X' + Y) - \log X' \geq 0$, for all $\epsilon > 0$. In particular, the compression to $\mathrm{supp} X$ is positive too: $\log(X' + Y)|_X - \log(X')|_X \geq 0$. Since X' is defined as a direct sum of X and $\epsilon \mathbb{1}$, $\log(X')|_X = \log(X'|_X) = \log(X|_X)$. Since $\lim_{\epsilon \rightarrow 0} X' + Y = X + Y$, we get, indeed, $\log(X + Y)|_X - \log(X|_X) \geq 0$.

The assumption reduces to $\mathrm{Tr} X|_X Z = 0$. Because $X|_X > 0$ and $Z \geq 0$, this implies $Z = 0$.

This implies $Y|_X = 0$, so that, indeed, Y must be orthogonal to X . \square

6 Relative Tsallis Entropies

The relative Tsallis entropies are parameterised modifications of the relative entropy given by

$$Q_p(\rho \parallel \sigma) := \frac{1}{p}(1 - \text{Tr} \rho^{1-p} \sigma^p),$$

where p satisfies $0 \leq p \leq 1$.

Just as we have done for the relative entropy, one can define the telescopic relative Tsallis entropy, even though the problem of infinite values does not pose itself here; indeed, $\text{Tr} \rho^{1-p} \sigma^p$ is always between 0 and 1. Nevertheless, some interesting relationships occur when telescoping the relative Tsallis entropies. In particular, by exploiting the methods used in Sect. 4 we obtain a shorter and much simpler proof of an inequality already proven in [1].

Let us therefore consider the quantity $\text{Tr} \rho^{1-p}(a\rho + (1-a)\sigma)^p$. Firstly, let us determine its extremal values for fixed values of a . Clearly, the maximum is still 1, achieved when $\rho = \sigma$. The minimal value, however, is now a^p . This follows easily from operator monotonicity of the fractional power $x \mapsto x^p$ when $0 \leq p \leq 1$. Indeed,

$$\begin{aligned} \text{Tr} \rho^{1-p}(a\rho + (1-a)\sigma)^p &\geq \text{Tr} \rho^{1-p}(a\rho)^p \\ &= a^p \text{Tr} \rho^{1-p} \rho^p = a^p \text{Tr} \rho = a^p. \end{aligned}$$

Equality can be achieved for orthogonal ρ and σ .

Hence, we define the telescopic relative Tsallis entropies (TRTE) as follows:

Definition 2.

$$Q_{p,a}(\rho \parallel \sigma) = \frac{1}{1-a^p}(1 - \text{Tr} \rho^{1-p}(a\rho + (1-a)\sigma)^p). \quad (24)$$

By the above, $Q_{p,a}$ takes values between 0 and 1. The limiting values for $p \rightarrow 0$ and $p \rightarrow 1$ are

$$\lim_{p \rightarrow 0^+} Q_{p,a}(\rho \parallel \sigma) = S_a(\rho \parallel \sigma), \quad (25)$$

(easily checked using l'Hôpital's rule) and

$$\lim_{p \rightarrow 1} Q_{p,a}(\rho \parallel \sigma) = 1 - \text{Tr} \{\rho\} \sigma = S_1(\rho \parallel \sigma), \forall a. \quad (26)$$

We now show that a sharper upper bound is given by the trace norm distance between ρ and σ .

Theorem 6.

$$Q_{p,a}(\rho \parallel \sigma) \leq T(\rho, \sigma). \quad (27)$$

By (25), the limiting case $p \rightarrow 0^+$ reduces to Corollary 1. The limiting case $a \rightarrow 0$ reduces to the inequality $1 - \text{Tr} \rho^{1-p} \sigma^p \leq T(\rho, \sigma)$, which was instrumental in proving optimality of the Chernoff bound in symmetric hypothesis testing and which was proven by other means in [1].

Just as we did for the operator logarithm, we can define a linear map based on the Fréchet derivative of the fractional power function x^p , via

$$\left. \frac{d}{dt} \right|_{t=0} (A + t\Delta)^p =: \mathcal{T}_{A;p}(\Delta).$$

Since $x \mapsto x^p$ is a non-negative operator monotone function for $0 \leq p \leq 1$, the fractional power of a positive operator A can be written as the integral

$$A^p = \int_0^\infty d\mu_p(s) (A + s)^{-1} A,$$

where $d\mu_p(s)$ is a certain measure, parameterised by p , that is positive for $0 \leq p \leq 1$. Its Fréchet derivative is therefore given by

$$\begin{aligned} \left. \frac{d}{dt} \right|_{t=0} (A + t\Delta)^p &= \int_0^\infty d\mu_p(s) ((A + s)^{-1} \Delta - (A + s)^{-1} \Delta (A + s)^{-1} A) \\ &= \int_0^\infty d\mu_p(s) s(A + s)^{-1} \Delta (A + s)^{-1}. \end{aligned}$$

Therefore, $\mathcal{T}_{A;p}$ has the integral representation

$$\mathcal{T}_{A;p}(\Delta) = \int_0^\infty d\mu_p(s) s(A + s)^{-1} \Delta (A + s)^{-1}. \tag{28}$$

From this representation we easily derive the following properties:

1. $\text{Tr } X\mathcal{T}_{A;p}(Y) = \text{Tr } Y\mathcal{T}_{A;p}(X)$ for any X and Y ;
2. the map $\mathcal{T}_{A;p}$ preserves the positive definite ordering;
3. in particular, $\mathcal{T}_{A;p}(B)$ is positive for positive B ;
4. for $0 < p < 1$, $\mathcal{T}_{A;p}(A^{1-p}) = p\{A\}$.

The last property follows from

$$\begin{aligned} \mathcal{T}_{A;p}(A^{1-p}) &= \left. \frac{d}{dt} \right|_{t=0} (A + tA^{1-p})^p \\ &= pA^{p-1}A^{1-p} = p\{A\}. \end{aligned}$$

Here, negative fractional powers of A are defined in terms of the pseudoinverse A^\dagger as $A^{-s} := (A^\dagger)^s$; thus $A^{-s}A^s = (A^\dagger A)^s = \{A\}^s = \{A\}$. Using these properties, we can easily prove the theorem.

Proof of Theorem 6. Let $\Delta = \rho - \sigma$, and $t = T(\rho, \sigma)$ then Δ has Jordan decomposition $\Delta = t\omega_+ - t\omega_-$, where ω_+ and ω_- are orthogonal density operators. Then

$$\begin{aligned} \text{Tr } (a\rho)^{1-p} \mathcal{T}_{a\rho+(1-a)\sigma;p}(\Delta) &\leq \text{Tr } (a\rho)^{1-p} \mathcal{T}_{a\rho+(1-a)\sigma;p}(t\omega_+) \\ &\leq \text{Tr } (a\rho + (1-a)\sigma)^{1-p} \mathcal{T}_{a\rho+(1-a)\sigma;p}(t\omega_+) \\ &= \text{Tr } t\omega_+ \mathcal{T}_{a\rho+(1-a)\sigma;p}((a\rho + (1-a)\sigma)^{1-p}) \\ &= \text{Tr } t\omega_+ p\{a\rho + (1-a)\sigma\} \\ &\leq pt. \end{aligned}$$

In the first line we used the fact that $\Delta \leq t\omega_+$ and property 2; in the second line we used operator monotonicity of x^{1-p} and property 3; in the third line we used property 1, and in the fourth property 4. In the last line we used the fact that $\text{Tr } XY \leq 1$ when X is a density operator and Y is a projector.

Exploiting the inequality just obtained yields

$$\begin{aligned} 1 - \text{Tr } \rho^{1-p}(a\rho + (1-a)\sigma)^p &= \text{Tr } \rho^{1-p}(\rho^p - (a\rho + (1-a)\sigma)^p) \\ &= \int_a^1 da \frac{d}{da} \text{Tr } \rho^{1-p}(a\rho + (1-a)\sigma)^p \\ &= \int_a^1 da \text{Tr } \rho^{1-p} \mathcal{T}_{a\rho+(1-a)\sigma;p}(\rho - \sigma) \\ &\leq \int_a^1 da a^{p-1} pt = (1 - a^p)t, \end{aligned}$$

which is equivalent to the statement of the theorem. \square

7 Future Work

In forthcoming papers we will explore further properties of the telescopic relative entropy. One other problem with the ordinary relative entropy is the absence of a triangle inequality, in the sense that no useful upper bound exists on the difference $S(\rho \parallel \sigma_1) - S(\rho \parallel \sigma_2)$. Indeed, this difference can be infinite. It turns out that such a bound does exist for the telescopic relative entropy. Together with an upper bound on the difference $S(\rho_1 \parallel \sigma) - S(\rho_2 \parallel \sigma)$ it will be presented and proven in [2].

We will also study an interesting connection with Hamiltonian reconstruction. There is some evidence that the difference $S_a(\rho \parallel \sigma_1) - S_a(\rho \parallel \sigma_2)$ might provide non-trivial lower bounds on the time needed for state σ_1 to evolve unitarily into state σ_2 under the influence of a Hamiltonian with bounded energy.

Acknowledgments. The main part of this work was done at the Institut Mittag-Leffler, Djursholm (Sweden), during an extended stay at its Fall 2010 Semester on Quantum Information Theory.

References

1. Audenaert, K.M.R., Nussbaum, M., Szkoła, A., Verstraete, F.: Commun. Math. Phys. **279**, 251–283 (2008)
2. Audenaert, K.M.R.: Telescopic Relative Entropy – II: Triangle Inequalities. arxiv:1102:3041 (2011)
3. Datta, N.: Min- and max-relative entropies and a new entanglement monotone. IEEE Trans. Inf. Theory **55**, 2816–2826 (2009)
4. Fannes, M., de Melo, F., Roga, W., Życzkowski, K.: Matrices of fidelities for ensembles of quantum states and the Holevo quantity. arXiv:1104.2271 (2011)

5. Lendi, K., Farhadmotamed, F., van Wonderen, A.J.: Regularization of quantum relative entropy in finite dimensions and application to entropy production. *J. Stat. Phys.* **92**(5/6), 1115–1135 (1998)
6. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
7. Ohya, M., Petz, D.: *Quantum Entropy and Its Use*. Springer, Heidelberg (1993)
8. Petz, D.: *Quantum Information Theory and Quantum Statistics*. Springer, Berlin (2008)
9. Renner, R.: Security of quantum key distribution. PhD thesis, ETH Zurich. arXiv:quant-ph/0512258 (2005)
10. Roga, W., Fannes, M., Życzkowski, K.: *Phys. Rev. Lett.* **105**, 040505 (2010)

Approximating the Turaev-Viro Invariant of Mapping Tori is Complete for One Clean Qubit

Stephen P. Jordan¹ and Gorjan Alagic²(✉)

¹ Institute for Quantum Information, California Institute of Technology,
Pasadena, US

sjordan@caltech.edu

² Institute for Quantum Computing, University of Waterloo, Waterloo, Canada
galagic@iqc.ca

Abstract. The Turaev-Viro invariants are scalar topological invariants of three-dimensional manifolds. Here we show that the problem of estimating the Fibonacci version of the Turaev-Viro invariant of a mapping torus is a complete problem for the one clean qubit complexity class (DQC1). This complements a previous result showing that estimating the Turaev-Viro invariant for arbitrary manifolds presented as Heegaard splittings is a complete problem for the standard quantum computation model (BQP). We also discuss a beautiful analogy between these results and previously known results on the computational complexity of approximating the Jones Polynomial.

1 Introduction

Classifying the power of quantum computers is a fundamental problem in quantum information science. The computational power of a general-purpose quantum computer is identified with the complexity class BQP (bounded-error quantum polynomial time). The famous problems of factoring and discrete logarithm, for instance, are in BQP. An essential ingredient of BQP computation is the ability to initialize a large number of qubits into a specific pure state. In some proposed physical implementations, however, this appears to be an extremely difficult task. In 1998, Knill and Laflamme proposed that exponential speedups over classical computers could still be possible, even if one can only initialize a single qubit into a pure state, with the rest of the qubits in the maximally mixed state [17]. The complexity class thus defined is called DQC1 (deterministic quantum computation with one clean qubit), or simply “the one clean qubit class.” This class contains several problems for which no efficient classical algorithms are known. The most basic of these is the problem of estimating the trace of a unitary operator. In fact, trace estimation is DQC1-complete: not only is it in DQC1, but any other problem in DQC1 can be reduced to it.

Finding natural BQP-complete and DQC1-complete problems is essential to our understanding of the computational power afforded by quantum computers. Remarkably, BQP-complete problems can be found in areas of mathematics

without *a priori* close connection to quantum computation. In particular, approximating the Jones polynomial, a famous invariant of links, is a BQP-complete problem [1, 2, 12–14, 29]. The input is an element of the braid group, and the output is an estimate of the Jones polynomial of the so-called *plat closure* of the braid. Estimating the Jones polynomial of the so-called *trace closure* of the braid is DQC1-complete [16, 25].

Recent work [3, 15] showed that (the decision version of) approximating certain invariants of 3-manifolds is a BQP-complete problem. In this formulation, the input is a so-called *Heegaard splitting* of a 3-manifold, specified as an element of the mapping class group. The output is an estimate of the Turaev-Viro invariant of the input manifold. In this article we show that approximating the Turaev-Viro invariant of a 3-manifold specified as a *mapping torus* is a complete problem for the one clean qubit class. In Sect. 5, we use the language of Topological Quantum Field Theories (or TQFTs) to explain the mathematical underpinnings of the relationship between approximating the Jones polynomial of the plat and trace closures, and approximating the Turaev-Viro invariant of Heegaard splittings and mapping tori.

We assume only a basic understanding of topology and quantum computation. Needed concepts in manifold invariants and one clean qubit computation are explained in Sect. 2. Our exposition focuses on the Witten-Reshetikhin-Turaev (or WRT) invariant. This is only a matter of convenience, as it is known that the Turaev-Viro invariant is equal to the absolute square of the WRT invariant [23, 26–28].

2 Background

2.1 Two-Manifolds and Three-Manifolds

We begin by setting down a few basic definitions from low-dimensional topology. Recall that an *n-manifold* is a topological space¹ whose every point has a neighborhood that looks like (i.e., is homeomorphic to) an open subset of \mathbb{R}^n . Simple examples of one-dimensional manifolds include the line \mathbb{R} and the circle S^1 . Simple examples of two-dimensional manifolds include the the plane \mathbb{R}^2 , the sphere S^2 , and the torus $\Sigma_1 = S^1 \times S^1$, which we can visualize as the surface of a donut. More generally, the surface of a donut with g holes is also a two-manifold, which we call the surface of genus g and denote by Σ_g . The genus is a complete invariant of surfaces²: homeomorphic surfaces have the same number of handles (invariance), and non-homeomorphic surfaces have a different number of handles (completeness).

The simplest example of a 3-manifold is \mathbb{R}^3 itself. A nontrivial example is found by taking the product of Σ_1 with a third circle; the result is the three-dimensional torus $T^3 = S^1 \times S^1 \times S^1$. Given a surface Σ_g , the *cylinder* $\Sigma_g \times [0, 1]$

¹ More precisely, a second-countable Hausdorff space.

² In this work, we implicitly assume that all surfaces are closed, compact, connected and orientable.

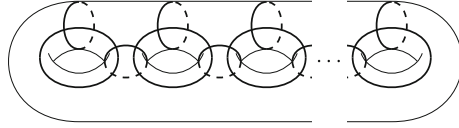


Fig. 1. A Dehn twist is a 2π rotation about a closed curve. The Dehn twists along the $3g - 1$ curves illustrated here constitute a standard set of generators for the mapping class group of the genus g surface.

is a 3-manifold whose boundary consists of two copies of Σ_g (specifically, the bottom $\Sigma_g \times \{0\}$ and the top $\Sigma_g \times \{1\}$.) We can turn the cylinder into a 3-manifold without boundary by choosing a homeomorphism $f : \Sigma_g \rightarrow \Sigma_g$ and gluing each point on the top to its image under f on the bottom. The result is the *mapping torus* of f :

$$T_{g,f} = \frac{\Sigma_g \times [0, 1]}{(x, 1) \sim (f(x), 0)}.$$

For example, choosing $g = 1$ and f to be the identity map, we see that $T_{1, \mathbb{1}} = T^3$. A useful example of a nontrivial self-homeomorphism of Σ_g is the so-called Dehn twist. To visualize a Dehn twist, imagine cutting the handle of Σ_1 to get a tube, performing a 2π twist on one end of the tube, and then gluing the handle back together. In general, a Dehn twist can be performed around any noncontractible closed curve.

The (homeomorphism class of) the mapping torus $T_{g,f}$ depends only on the isotopy class of f . The orientation-preserving self-homeomorphisms of Σ_g form a group under composition. This group, taken modulo isotopy, is called the mapping class group of Σ_g , and is denoted $\text{MCG}(g)$. $\text{MCG}(g)$ is generated by the Dehn twists about the $3g - 1$ canonical curves shown in Fig. 1. Any mapping torus $T_{g,f}$ is thus described by a word in the Dehn twist generators of $\text{MCG}(g)$.

2.2 The Witten-Reshetikhin-Turaev Invariants

Recall that the genus is an invariant of surfaces because it assigns the same number to homeomorphic surfaces. One can also define invariants of 3-manifolds, although none are as simple and powerful as the genus. In the 1990s, Witten, Reshetikhin, and Turaev discovered a family of 3-manifold invariants arising from their work in Topological Quantum Field Theory. While these invariants can be defined for arbitrary 3-manifolds, we only concern ourselves with the special case of mapping tori, where the definitions are relatively straightforward. Specifically, the Witten-Reshetikhin-Turaev (WRT) invariant of a mapping torus $T_{g,f}$ is equal to the trace of f in a certain projective representation of the mapping class group $\text{MCG}(g)$. Note that the WRT function is only a topological invariant up to a phase (see [3]). In general, the WRT invariant is parametrized by a quantum group, such as $\text{SU}(N)_k$ or $\text{SO}(N)_k$. Although some of our results apply more

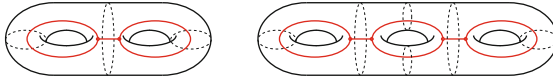


Fig. 2. The dashed lines indicate a set of cuts that decomposes the surface into two three-punctured-spheres (“pants”). Dual to this is a trivalent graph called the “spine,” in red. The genus two and genus three cases are shown here.

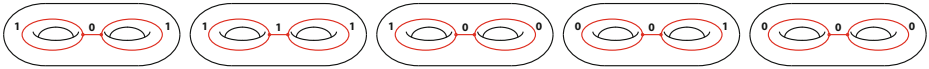


Fig. 3. The Fibonacci model’s fusion rules allow five labelings of the standard spine of the genus two surface. This means that the WRT representation of $MCG(2)$ is five-dimensional.

generally, we focus on the case of $SO(3)_3$, sometimes called the Fibonacci model. In this case, the description of the representation is particularly simple, and can be understood with no background in quantum groups.

The Fibonacci representation is defined as follows. Any genus g surface (for $g > 1$) can be cut into three-punctured spheres, resulting in a so-called pants decomposition. Dual to such a decomposition is a trivalent graph on the surface, called a spine. As illustrated in Fig. 2, the spine has one vertex for every pant in the decomposition. Whenever two pants meet at a puncture, the spine has an edge between the corresponding vertices. While a surface admits many spines (and corresponding pants decompositions), we call the one shown in Fig. 2 the *standard spine*. We label the edges of the standard spine by so-called anyon types, with fusion rules enforced at each vertex. For the Fibonacci model, there are only two anyon types: 0 and 1, and only one fusion rule: no vertex can have exactly two edges labeled 0 incident on it. The case $g = 2$ is pictured in Fig. 3. The formal span (over \mathbb{C}) of all such labelings associates a finite-dimensional vector space to the surface. Different spines yield different bases for this same space. We can move between these spines (and the corresponding bases) by means of two “moves,” the F-move:

$$\begin{array}{c} \text{Diagram 1} \end{array} = \sum_n F_{kln}^{ijm} \begin{array}{c} \text{Diagram 2} \end{array}$$

and the S-move:

$$\begin{array}{c} \text{Diagram 1} \end{array} = \sum_k S_{jk}^i \begin{array}{c} \text{Diagram 2} \end{array}$$

For the Fibonacci model F_{abc}^{def} is as follows

$$\begin{aligned}
 \begin{array}{c} | \\ \diagdown \\ \text{0} \\ \diagup \\ | \\ | \end{array} &= \frac{2}{1+\sqrt{5}} \begin{array}{c} | \\ \diagdown \\ \text{0} \\ \diagup \\ | \\ | \end{array} + \sqrt{\frac{2}{1+\sqrt{5}}} \begin{array}{c} | \\ \diagdown \\ \text{1} \\ \diagup \\ | \\ | \end{array} \\
 \begin{array}{c} | \\ \diagdown \\ \text{1} \\ \diagup \\ | \\ | \end{array} &= \sqrt{\frac{2}{1+\sqrt{5}}} \begin{array}{c} | \\ \diagdown \\ \text{0} \\ \diagup \\ | \\ | \end{array} + \frac{-2}{1+\sqrt{5}} \begin{array}{c} | \\ \diagdown \\ \text{1} \\ \diagup \\ | \\ | \end{array}
 \end{aligned}$$

with all other values equal to zero or one as dictated by the fusion rules. As one can calculate using the prescription described in [3], S_{jk}^i is given in the Fibonacci model by

$$\begin{aligned}
 DS_{00}^0 &= 1 \\
 DS_{10}^0 = DS_{01}^0 &= \frac{1+\sqrt{5}}{2} \\
 DS_{11}^0 &= 1 + \frac{1+\sqrt{5}}{2} e^{i4\pi/5} \\
 DS_{11}^1 &= \sqrt{\frac{1+\sqrt{5}}{2}} (1 - e^{i4\pi/5})
 \end{aligned}$$

with $D = \sqrt{1 + \left(\frac{1+\sqrt{5}}{2}\right)^2}$ and all other values of S_{jk}^i equal to zero by the fusion rules.

The space described above is the underlying vector space for the Fibonacci representation of $MCG(g)$. We define this representation in the basis corresponding to the standard spine. Since the mapping class group is finitely-generated, it suffices to describe the images of the Dehn twist generators. Any such generator is a 2π twist along some canonical curve c from Fig. 1. It is not hard to check that, by applying at most one F-move and one S-move, the standard spine can be adjusted so that c is a cut in the corresponding pants decomposition. In this basis, the Dehn twist about c induces a diagonal linear transformation. To each labeling of the spine corresponds a basis vector, and this basis vector obtains a phase determined by the label on the edge of the spine that intersects c . In the Fibonacci model, edges labeled 0 obtain a phase of 1, and edges labeled 1 obtain a phase of $e^{i3\pi/5}$. In the standard spine basis, the matrix corresponding to the Dehn twist about c is thus simply a product of at most five matrices: at most two of the moves pictured above, followed by a diagonal matrix, followed by the inverse moves to return to the original basis. The WRT invariant of the mapping torus $T_{g,f}$ is now simply the trace of the Fibonacci representation, evaluated at f .

2.3 One Clean Qubit

In some proposed implementations of quantum computers, such as nuclear magnetic resonance (NMR) the most difficult task is initializing qubits into a pure

state. In 1998, Knill and Laflamme proposed that exponential speedups over classical computation might be possible without pure state initialization. To mathematically investigate this possibility, they introduced the one clean qubit model [17]. In this model, one is given an initial state ρ with n qubits in the maximally mixed state, and one qubit in the pure state $|0\rangle$.

$$\rho = |0\rangle\langle 0| \otimes \frac{\mathbb{1}}{2^n}$$

One then applies any quantum circuit of $\text{poly}(n)$ gates to this state, and measures the first qubit in the computational basis. Computational problems are solved by performing polynomially many such experiments, each starting with the initial state ρ , and recording the output statistics. The class of decision problems solvable with bounded probability of error using this procedure is called DQC1.

DQC1 contains several computational problems not known to be solvable in polynomial time on classical computers. Most fundamentally, given a description of a quantum circuit of T gates implementing the unitary transformation U on n qubits, a one clean qubit computer can estimate the normalized trace $\frac{\text{Tr}U}{2^n}$ to within $\pm\epsilon$ in time $O(T/\epsilon^2)$ by means of the circuit shown in Fig. 4. Furthermore, this problem of estimating the trace of a quantum circuit is DQC1-hard [17, 24, 25]. Efficient one clean qubit algorithms have been discovered for estimating certain quadratically signed weight enumerators [18] and estimating certain Jones [25] and HOMFLY [16] polynomials. A version of the Jones polynomial problem is DQC1-complete [25], and has been demonstrated experimentally with NMR [20, 22]. A certain problem of approximating partition functions for quantum systems is also DQC1-hard [6].

In many ways, it is surprising that one clean qubit computers can do any non-trivial computations at all. If all $n+1$ qubits were maximally mixed, the resulting state would be invariant under all unitaries. Furthermore, DQC1 computations involve very little entanglement [7–11, 19]. Ambainis *et al.* give an impossibility proof against a certain natural approach to simulating standard quantum computers using one clean qubit computers, and on the other hand show that one clean qubit computers can efficiently simulate classical logarithmic depth (NC1) computations [4].

The DQC1 complexity class is robust against a variety of modifications to the computational model. The class of computational problems solvable in polynomial time with up to logarithmically many clean qubits is the same as

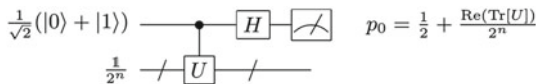


Fig. 4. By repeating this one clean qubit computation, and recording the fraction of 0 outcomes, one estimates the real part of $\text{Tr}[U]/2^n$. Similarly, by initializing the clean qubit to $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$, one obtains $p_0 = \frac{1}{2} + \frac{\text{Im}(\text{Tr}[U])}{2^n}$.

that solvable in polynomial time with one clean qubit [25]. If the clean qubit is not pure, but has $1/\text{poly}(n)$ polarization, the set of efficiently solvable problems also remains DQC1 [17]. As shown in Appendix A, the one clean qudit model on d -dimensional qudits is equivalent in power to the one clean qubit model, for any constant d .

3 Algorithm

In this section we construct an efficient one clean qubit algorithm for approximating the Fibonacci WRT invariant of a mapping torus. Generalizing to other tensor categories such as $SU(N)_k$ and $SO(N)_k$ is straightforward. The main idea of the algorithm is, given a word w in the Dehn twist generators of $\text{MCG}(g)$, to find a quantum circuit of $\text{poly}(w, g)$ gates on $\text{poly}(g)$ qubits whose trace is equal to the WRT invariant of the 3-manifold $T_{g,w}$. This trace can then be approximated by means of the circuit in Fig. 4. For this purpose, we encode the allowed labelings of a spine of Σ_g into qubits, and then construct a quantum circuit implementing the Fibonacci representation of $\text{MCG}(g)$ on this encoding. The most obvious encoding would be to directly assign one qubit to store the particle type for each edge of the spine. However, a one clean qubit computer yields the normalized trace over all 2^n bitstrings, of which only an exponentially small fraction represent valid spine labelings in this encoding.

We instead construct a many-to-one map

$$\varphi : \{0, 1\}^{\beta(3g-3)} \rightarrow \{\text{valid labelings}\}$$

with $\beta = O(\log |g|)$ such that the preimage of each spine-labeling consists of approximately the same number of bitstrings. That is, $|\varphi^{-1}(x)|$ is approximately independent of x . Thus, the normalized trace of the Fibonacci representation of $w \in \text{MCG}(g)$ acting on the φ -encoded labelings of the spine of Σ_g is approximately equal to $\text{WRT}(T_{g,w})$. We construct φ following a method introduced in [16]. We assign a register of $\beta = O(\log |g|)$ qubits to each edge of the spine. The bitstring contained in register i is interpreted as an integer $0 \leq x_i \leq 2^\beta - 1$. We then assign a threshold T_i so that $x_i \leq T_i$ encodes a zero label on edge i , and $x_i > T_i$ encodes a one label. By carefully choosing the thresholds T_1, \dots, T_{3g-3} we ensure that $|\varphi^{-1}(x)|$ is approximately independent of x .

Number the edges of the spine from one to $3g-3$, left to right and top to bottom, as illustrated in Fig. 5. Let $s_1, \dots, s_{3g-3} \in \{0, 1\}^{3g-3}$ be the labels of these edges. The uniform probability distribution over all fusion-consistent labelings

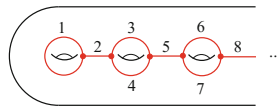


Fig. 5. We number the edges of the standard spine from left to right, with ambiguities resolved by ordering from top to bottom.

of the spine induces a probability distribution $p_g(s_1, \dots, s_{3g-3})$ over $\{0, 1\}^{3g-3}$, with zero probability for strings that violate fusion rules, and uniform probability for the rest. For the genus- g standard spine, we define $p_g(s_i | s_1, \dots, s_{i-1})$ to be the conditional probability that label i takes the value s_i given that labels 1 through $i-1$ take the values s_1, \dots, s_{i-1} . For a register representing a label s_i we choose the threshold dependent on the values of s_1, \dots, s_{i-1} according to

$$T_i(g; s_1, \dots, s_{i-1}) = \lceil 2^\beta p_g(0 | s_1, \dots, s_{i-1}) \rceil. \quad (1)$$

One can see that this choice ensures that a uniformly selected assignment of bitstrings to the registers yields a uniform distribution over fusion-consistent labelings, up to the errors induced by rounding. Hence, $|\varphi^{-1}(x)|$ is approximately independent of x . More precisely, let

$$\begin{aligned} \tilde{p}_g(0 | s_1, \dots, s_{i-1}) &= T_i(g; s_1, \dots, s_{i-1}) / 2^\beta \\ \tilde{p}_g(1 | s_1, \dots, s_{i-1}) &= 1 - \tilde{p}_g(0 | s_1, \dots, s_{i-1}) \end{aligned}$$

Thus,

$$\begin{aligned} |\varphi^{-1}(s_1, \dots, s_{3g-3})| &= 2^{\beta(3g-3)} \tilde{p}_g(s_{3g-3} | s_1, \dots, s_{3g-4}) \times \\ &\quad \times \tilde{p}_g(s_{3g-4} | s_1, \dots, s_{3g-5}) \times \dots \times p(s_1) \\ &= 2^{\beta(3g-3)} (p_g(s_{3g-3} | s_1, \dots, s_{3g-4}) \pm O(2^{-\beta})) \times \\ &\quad \times \dots \times (p_g(s_1) \pm O(2^{-\beta})) \\ &= p_g(s_1, \dots, s_{3g-3}) \pm O(g2^{-\beta}). \end{aligned}$$

Thus it suffices to choose $\beta = O(\log g)$. Furthermore, by the locality of the fusion rules, $p_g(s_i | s_1, \dots, s_{i-1})$ is always independent of s_1, \dots, s_{i-3} . We may thus write

$$\begin{aligned} p_g(s_i | s_1, \dots, s_{i-1}) &= p_g(s_i, s_{i-1}, s_{i-2}; i) \\ T_i(g; s_1, \dots, s_{i-1}) &= T_i(g; s_i, s_{i-1}, s_{i-2}). \end{aligned} \quad (2)$$

As illustrated in Fig. 6, the Fibonacci representation of a Dehn twist from the standard generating set is a unitary transformation acting on at most five spine labels. Because the encoding φ is many-to-one, the unitary transformation on these spine labels does not uniquely define a unitary operation on the bitstrings encoding them. We say that a pair of spine-labelings is *connected* if the Fibonacci representation of a Dehn twist from the standard set of generators has a nonzero matrix element between them. By choosing a bijection $b_{x,y}$ between the encodings of each pair of connected spin-labelings we define a unitary transformation on the encodings: if the matrix element between labeling x and y is $\rho_{x,y}$ then,

$$U_{i,j} = \begin{cases} \rho_{x,y} & \text{if } \varphi(i) = x, \varphi(j) = y, \text{ and } b_{x,y}(i) = j \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

is a corresponding unitary representation on the encodings. Our choice of bijections does not matter. We may for concreteness match bitstrings by lexicographic

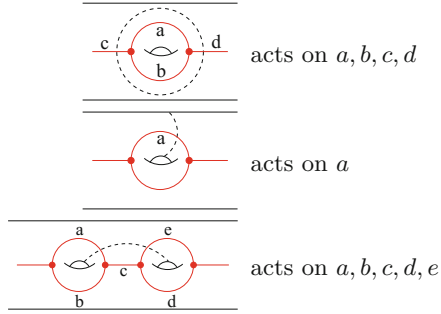


Fig. 6. The Fibonacci representation of a Dehn twist (shown as a dashed line) from the standard generating set is a unitary transformation acting on at most five spine labels.

ordering. One can verify that U is a direct sum of many copies of the Fibonacci representation ρ . (The rounding involved in (1) introduces a minor technical complication, whose resolution may be found in [16].)

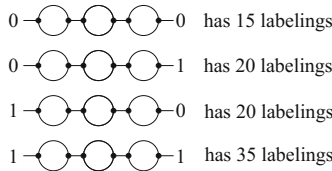
For any of the standard Dehn twist generators, $U_{i,j}$ acts on at most 5β qubits, which encode the spine-labels on which ρ acts. The matrix elements by which U acts on these qubits depends on the corresponding thresholds. By (2), these depend on at most two additional registers of qubits, which encode the two spine labels to the left of those being acted upon. Thus, for any of the standard Dehn twist generators, $U_{i,j}$ is a controlled unitary acting on at most 5β target qubits and 2β control qubits. Recalling that $\beta = O(\log |g|)$, we can apply the standard construction from Section 4.5 of [21] to implement this unitary transformation with $\text{poly}(|g|)$ quantum gates, provided each matrix element of $U_{i,j}$ can be computed efficiently. By (3), one sees that the only potentially difficult part of computing the matrix elements of **3** is the computation of the thresholds. An efficient classical algorithm for this task is given in Appendix C.

4 Hardness

In this section we prove that the problem of estimating the normalized WRT Fibonacci invariant of a mapping torus, given by a polynomial-length word in the standard Dehn twist generators of the mapping class group, to within $\pm\epsilon$ is DQC1-hard for $\epsilon < 1/3900$. Generalizing our hardness proof beyond the Fibonacci model seems less straightforward than generalizing our algorithm. However, we consider it likely to be possible. Extending hardness to larger values of ϵ we leave as an open problem. To prove hardness, we reduce from the problem of estimating the absolute value of the normalized trace of a quantum circuit. A proof of the hardness of absolute trace estimation is given in Appendix B. We thus require an efficient procedure that, given a description of a quantum circuit for implementing a unitary U , outputs a description of a mapping torus (i.e., a word in the Dehn twist generators) whose WRT invariant

is close to the trace of U . It turns out to be convenient to suppose that U is a quantum circuit acting on a collection of 5-dimensional qudits (“qupents”). As shown in Appendix A, this makes no difference: the one-clean-qubit model is equivalent to the one-clean-qupent model.

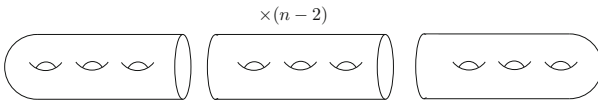
Let U be a quantum circuit of G gates acting on n qupents arranged in a line. Without loss of generality, we may assume that each gate acts either on a single qupents or a pair of neighboring qupents. To prove hardness, we first define a many-to-one encoding $\psi : S_{3n} \rightarrow \{0, 1, 2, 3, 4\}^n$, where S_{3n} is the set of fusion-consistent labelings of the standard spine of the surface of genus $3n$. We divide the genus- $3n$ surface into n segments, each having three handles. The number of fusion-consistent labelings for a genus-three segment with two punctures depends on the labels on the incoming and outgoing edges, as shown below.



In all cases, the number of fusion-consistent labelings is a multiple of five. Thus, in every case a qupents can be encoded in the space of labelings, together with a “gauge” qudit, whose value we ignore, which has dimension 3, 4, or 7, depending on the labels of the incoming edges. Thus the size $|\psi^{-1}(z)|$ of the preimage of any $z \in \{0, 1, 2, 3, 4\}^n$ is exactly independent of z . Given any unitary U acting on n qupents, there corresponds a unitary acting on the span of S_{3n} which acts as U on the encoded qupents, and as the identity on the gauge qudits. We call this the ψ -encoding of U .

As shown in [14], the Fibonacci representation of the mapping class group of the genus $g > 1$ surface is dense in the corresponding unitary group, modulo phase. Thus, given any unitary operation on n qupents, we can find a sequence of Dehn twists which approximates its ψ -encoding arbitrarily closely. The trace of the ψ -encoding is thus equal to the trace of the original quantum circuit, up to a phase. The remaining question is whether this reduction can be done efficiently.

Cutting the genus- $3n$ surface into n equal segments yields $n - 2$ genus-3 doubly-punctured surfaces, and two genus-3 singly-punctured surfaces, as shown below.



One can pants-decompose a punctured surface, thereby associating the surface to a spine. The spine has one “external” edge for each puncture, which attaches to the rest of the spine at only one vertex. Upon labeling the spine, we can associate the label of any external edge with the corresponding puncture. The Fibonacci representation may then be extended to the label-preserving mapping

class group of the punctured surface. This group includes all the standard Dehn twists, together with braiding of punctures with the other punctures of the same label. In the Fibonacci representation, braiding of zero-labeled punctures has no effect, thus a zero-labeled puncture is equivalent to the absence of a puncture.

Theorem 6.2 of [14] states that for any fixed labels on the punctures, the Fibonacci representation of the label-preserving mapping class group of the r -punctured genus- g surface is dense in the corresponding unitary group modulo phase, provided $g + r > 1$. Thus, given any one-qubit gate, the Solovay-Kitaev theorem [21] efficiently yields a sequence of Dehn twists and braid moves on the corresponding genus-3 singly-punctured or doubly-punctured surface, whose Fibonacci representation approximates the ψ -encoded gate arbitrarily closely. Similarly, one efficiently approximates two-qubit gates by moves on genus-6 surfaces with one or two punctures.

We must modify the above construction so as not to use any braiding of punctures. On the leftmost or rightmost qubits there is no problem; the corresponding surfaces have only one puncture, and therefore Theorem 6.2 implies density without using any braiding moves. Similarly, on any of the central surfaces, Theorem 6.2 implies density without using any braiding moves if at least one of the punctures has a zero label. We can ensure this prior to the application of any given gate by adapting the “inchworm” technique from [25], as described in Appendix D. In this method, we bring a pair of zero labels adjacent to the target segment, then implement the desired gate there, and carry the zeros to the segment where the next gate is to be implemented. At the end, we return these zeros to their original location among the leftmost six handles. As discussed in Appendix D, the inchworm construction entails some overhead in ϵ , which gives rise to the value $1/3900$.

In the above construction, we need density on two-punctured segments in which one puncture is guaranteed to be labeled zero, and the other puncture has unknown label. Theorem 6.2 of [14] implies density separately in the subspace in which the other label is zero and in which the other label is one. Because these subspaces have different dimension (20 and 15, respectively) we may apply the decoupling Lemma from [1], which shows that a sequence of Dehn twists can be found to approximate arbitrary pairs of independent unitaries on these two subspaces, as desired.

5 Analogy with Jones Polynomials

In this paper we have shown that estimating the Turaev-Viro invariant of a mapping torus in the Fibonacci model is DQC1-complete. In [3], it was shown that estimating the Turaev-Viro invariant of a general 3-manifold presented as a Heegaard splitting is BQP-complete. Similarly, estimating the Jones polynomial of the trace closure of a braid is DQC1-complete [16, 25], while estimating the Jones polynomial of the plat closure of a braid is BQP-complete [1, 2, 12, 13, 29]. This suggests a relationship between trace closures and mapping tori on one hand, and between plat closures and Heegaard splittings on the other. Indeed,

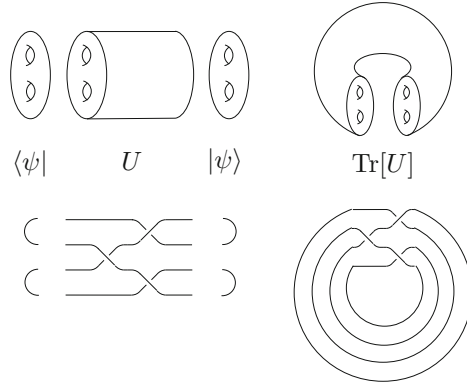


Fig. 7. The problems of estimating the Jones polynomial of the plat closure of a braid and the Turaev-Viro invariant of a Heegaard splitting (left) are BQP-complete. The problems of estimating the Jones polynomial of the trace closure of a braid and the Turaev-Viro invariant of a mapping torus (right) are DQC1-complete. These situations are fundamentally analogous, as discussed in Sect. 5. We stress that the manifold figures are illustrations of the topological ideas behind this analogy, and are not correct two-dimensional projections of the manifolds themselves. In particular, after gluing, the two manifolds shown do not in reality have any boundaries.

such a relationship can be understood in the framework of axiomatic topological quantum field theory, and suggests further generalizations to, for instance, topological invariants of higher dimensional manifolds.

A topological quantum field theory can be axiomatized as a functor T from the category of cobordisms between n -manifolds to the category of linear transformations between vector spaces [5, 28]. That is, to each n -manifold the TQFT associates a vector space, and to any $(n + 1)$ -manifold whose boundary is the union of two disjoint n -manifolds the TQFT associates a linear transformation between the two associated vector spaces. The functorial property means that gluing together two cobordisms and then applying T yields the same linear transformation that is obtained by applying T to each of the two cobordisms and then composing the resulting linear transformations; see Fig. 8. A TQFT maps the empty n -manifold to the base field, which for the examples we consider is always \mathbb{C} . Hence, for M a manifold whose boundary ∂M has a single connected component, $T(M)$ is a map either from \mathbb{C} to the vector space $T(\partial M)$, that is, a vector in $T(\partial M)$, or a map from $T(\partial M)$ to \mathbb{C} , that is, a dual vector. The choice between these two possibilities is determined by the orientation of the cobordism.

Recall that the genus- g handlebody is the 3-manifold whose boundary is the genus- g surface Σ_g . For example, the genus-1 handlebody is simply the solid donut. After assigning an orientation, we may think of a handlebody as a cobordism from the empty manifold to Σ_g , or as a cobordism from Σ_g to the empty manifold. Hence, in the TQFT framework, genus- g handlebodies are associated to vectors or dual vectors. We denote these as $|\psi_g\rangle$ and $\langle\psi_g|$, respectively. These

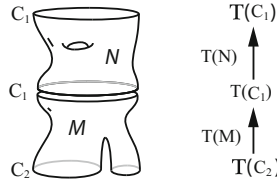


Fig. 8. M can be viewed as a two-manifold with two boundaries: a circle and a pair of circles. The TQFT associates a Hilbert space $T(C_2)$ to the pair of circles, a Hilbert space $T(C_1)$ to the circle, and a linear transformation $T(M) : T(C_2) \rightarrow T(C_1)$ to M . Similarly, $T(N)$ is a linear transformation from $T(C_1)$ to itself. If we glue together M and N along the circle as shown, we obtain a manifold MN with boundaries C_2 and C_1 . The corresponding linear transformation is $T(NM) = T(N) \circ T(M)$.

vectors live in the Hilbert space which the TQFT associates to Σ_g . In the case of the Fibonacci model, this is precisely the vector space defined in Sect. 2.2.

In the Fibonacci model, a cobordism from a surface to itself is mapped to a unitary linear transformation U on the associated Hilbert space³. If the surface is Σ_g , then we may “cap” the cobordism with handlebodies on both ends. The resulting 3-manifold has no boundary, and thus corresponds to a linear map from \mathbb{C} to itself, i.e., a complex number. In this case, this number is the matrix element $\langle \psi_g | U | \psi_g \rangle$, as illustrated in Fig. 7. The problem of estimating a matrix element of the unitary transformation induced by a quantum circuit is BQP-complete, and this fact underlies the BQP-completeness proof for the Turaev-Viro invariant of Heegaard splittings in [3]. Instead of “capping” the two ends of the cobordism with handlebodies, we could have simply glued the two ends together, resulting in a mapping torus. This is again a 3-manifold without boundary, which thus also corresponds to a complex number. In a TQFT, gluing the two ends of a cobordism corresponds to contracting the two indices of the linear transformation. In other words, instead of a single matrix entry, we now obtain the trace of U . Finding the trace of the unitary transformation induced by a quantum circuit is DQC1-complete, and this fact underlies the DQC1-completeness proof for the Turaev-Viro invariant of mapping tori given in this paper.

The situation regarding Jones polynomials is directly analogous. A TQFT gives us a unitary representation of the braid group. Gluing the two ends of a braid together (i.e., taking the trace closure), as illustrated on the righthand side of Fig. 7, corresponds to taking the trace of the unitary and yields a DQC1-complete problem. Caps correspond to vectors and dual vectors depending on orientation, hence capping a braid (taking the plat closure, as illustrated on the lefthand side of Fig. 7) yields a matrix element of the associated unitary transformation, and corresponds to a BQP-complete problem. The analogy can

³ We may think of the cobordism as describing a sort of spacetime evolution, while the unitary transformation describes the corresponding quantum time evolution. Indeed, this was one of the central motivating ideas behind the development of TQFTs.

be tightened further by noting that the braid group B_n is simply the mapping class group of the surface of genus zero and $n + 1$ punctures (that is, the n -punctured disk), whereas in the case of 3-manifold invariants we consider the mapping class group of the genus- g surface with no punctures. On the other hand, it is worth bearing in mind that the notion of equivalence captured by the Jones polynomial is ambient isotopy, in contrast to the Turaev-Viro and WRT invariants, which capture homeomorphism.

The analogy presented here naturally suggests an extension of BQP-completeness and DQC1-completeness results to n -manifold invariants arising from TQFTs at higher n . More generally, one could attempt to isolate a property of pairs, consisting of a group G and one of its representations U , such that estimating matrix entries of U is BQP-complete while estimating the trace of U is DQC1-complete. Perhaps one could find a general theorem encompassing many such results. We leave this as an open problem.

Acknowledgments. We thank Robert König, Ben Reichardt and Edgar Bering for useful discussions and some diagrams. S.J. acknowledges support from the Sherman Fairchild Foundation and NSF grant PHY-0803371. G.A. acknowledges support from NSERC, MITACS and ARO.

A Equivalence Between One Clean Qudit Models

Given a quantum circuit on a -dimensional qudits we wish to construct a quantum circuit on b -dimensional qudits that has the same trace. If $b = ca$ for some integer c then this is easy. We just consider each b -dimensional qudit to be an a -dimensional qudit plus a c -dimensional “gauge” qudit that we ignore. Similarly, if $b^d = ca$ for some integers d, c then we can treat d -tuples of b -dimensional qubits as an a -dimensional qudit plus a c -dimensional gauge qudit. For these encodings, the encoded circuit is easy to construct gate by gate. Given a gate acting on n a -dimensional qudits, we can write down a unitary acting on dn b -dimensional qudits equal to the original gate tensored with the c -dimensional identity on the gauge system. This dn -dimensional gate can be exactly decomposed into a product of $O(b^{2dn})$ 2-qudit gates using the standard construction from Section 4.5 of [21]. Because d and n are constants, this is sufficiently efficient. The normalized trace of the encoded circuit is exactly equal to the normalized trace of the original circuit.

The harder case is when there do not exist integers c and d such that $b^d = ca$. In this case we find $c, d \in \mathbb{Z}$ such that $b^d \simeq ca$. Specifically, suppose we achieve

$$\frac{ca}{b^d} = 1 - \delta \tag{4}$$

for some $\delta \ll 1$. Then we can encode one a -dimensional qudit plus a c -dimensional gauge qudit into d b -dimensional qudits with a few (namely δb^d) noncoding states left over. We can define our encoded gates to act as the identity on these noncoding states. If we make sure the noncoding states are a small fraction of all

b^{dn} states, the normalized trace of the encoded circuit will approximately match the normalized trace of the original circuit.

Let U_a be the original unitary acting on n a -dimensional qudits and let U_b be the unitary acting on dn b -dimensional qudits, in which we encode U_a as described above. Then, U_b acts on b^{dn} states, of which $(ca)^n$ encode states of the original circuit,

$$\frac{\text{Tr}[U_b]}{b^{dn}} = \frac{c^n \text{Tr}[U_a] + (b^{dn} - (ca)^n)}{b^{dn}}.$$

The magnitude of the discrepancy Δ between the normalized traces of U_b and U_a is thus

$$\begin{aligned} \Delta &= \left| \frac{c^n \text{Tr}[U_a] + (b^{dn} - (ca)^n)}{b^{dn}} - \frac{\text{Tr}[U_a]}{a^n} \right| \\ &= \left| \left(\left(\frac{ca}{bd} \right)^n - 1 \right) \frac{\text{Tr}[U_a]}{a^n} + 1 - \left(\frac{ca}{bd} \right)^n \right| \\ &\leq \left| \left(\frac{ca}{bd} \right)^n - 1 \right| \cdot \left| \frac{\text{Tr}[U_a]}{a^n} \right| + \left| 1 - \left(\frac{ca}{bd} \right)^n \right| \\ &\leq \left| \left(\frac{ca}{bd} \right)^n - 1 \right| + \left| 1 - \left(\frac{ca}{bd} \right)^n \right| \\ &= 2 \left| (1 - \delta)^n - 1 \right|. \end{aligned}$$

Thus if

$$\delta = \frac{\epsilon}{n} \tag{5}$$

we have, for small ϵ ,

$$\lim_{n \rightarrow \infty} \Delta = 2 \left| e^{-\epsilon} - 1 \right| \simeq 2\epsilon. \tag{6}$$

Comparing (4), (5), (6), we see that in the limit of large n and small ϵ , in order to achieve error upper bounded by Δ it suffices to obtain

$$\frac{b^d - ca}{b^d} \leq \frac{\Delta}{2n}.$$

For given b, d, a there always exists an integer c such that $b^d - c \leq a$. So we just need to choose d sufficiently large that

$$\frac{a}{b^d} \leq \frac{\Delta}{2n}.$$

Equivalently,

$$d \geq \log_b \left(\frac{2na}{\Delta} \right).$$

A k -qudit gate from U_a thus gets encoded as a dk -qudit gate in U_b . This encoded gate acts on a b^{dk} -dimensional space. We have just shown that it suffices to choose $d = \log_b \left(\frac{2na}{\Delta} \right)$. Thus the encoded k -qudit gate acts on a $\left(\frac{2na}{\Delta} \right)^k$ -dimensional space. Using the construction from section 4.5 of [21], we

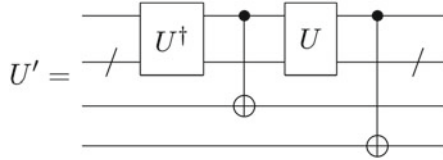
can implement an arbitrary D -dimensional unitary exactly with $O(D^2)$ 2-qudit gates. Thus each k -qudit gate in U_a gets encoded by $O\left(\left(\frac{2na}{\Delta}\right)^{2k}\right)$ elementary gates in U_b . By gate universality, we can assume $k \leq 2$, so our encoding has an overhead quartic in n and $1/\Delta$. This is perhaps not very efficient, but is nevertheless polynomial, and thus suffices to prove the equivalence of DQC1 defined with qudits of any constant dimension.

B Estimating the Absolute Trace is DQC1-Hard

In this section we slightly adapt the proof from [24] to show that estimating the absolute value of the trace of a quantum circuit to within $\pm 1/24$ is a DQC1-complete problem. Consider an arbitrary DQC1 computation. We start with the state $|0\rangle\langle 0| \otimes \frac{\mathbb{1}}{2^n}$, apply an arbitrary quantum circuit U , and then measure the first qubit in the $|0\rangle, |1\rangle$ basis. Changing the initial state of the pure qubit, or changing the measurement basis does not add generality, as these changes can be subsumed into U . The probability of measurement outcome $|0\rangle$ is

$$p_0 = \text{Tr} \left[(|0\rangle\langle 0| \otimes \mathbb{1}) U (|0\rangle\langle 0| \otimes \mathbb{1}/2^n) U^\dagger \right]. \tag{7}$$

Let U' be the unitary implemented by the following quantum circuit on $n + 2$ qubits.



Thus, $p_0 = 2 \frac{\text{Tr} U'}{2^{n+2}}$, as one can see by writing out the trace as a sum over diagonal matrix elements in the computational basis. Because p_0 is real it is also true that $p_0 = 2 \frac{|\text{Tr} U'|}{2^{n+2}}$. Hence estimating the absolute value of the normalized trace of quantum circuits suffices to predict the outcome of any DQC1 experiment.

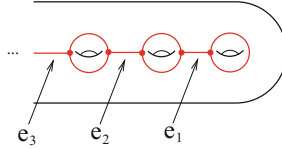
As is standard in the complexity theory of probabilistic computation, “yes” instances of DQC1 are defined to have acceptance probability $2/3$ and “no” instances are defined to have acceptance probability $1/3$. Thus, deciding DQC1 is equivalent to estimating the normalized trace of a quantum circuit to within $\pm 1/6$. The reduction here has a factor of four overhead in normalization, thus estimating the absolute trace to within $\pm 1/24$ is DQC1-complete.

C Efficiently Computing Thresholds

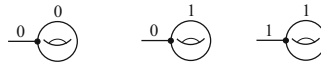
Consider the standard spine of the genus- g surface, numbered as in Fig. 5. Suppose edges 1 through i have been labeled in a fusion-consistent manner with anyon types s_1, \dots, s_i . We wish to compute how many completions there are to

this partial labelling. That is, we wish to compute the number of fusion-consistent strings of $3g - 3$ labels, whose first i labels are given by s_1, \dots, s_i .

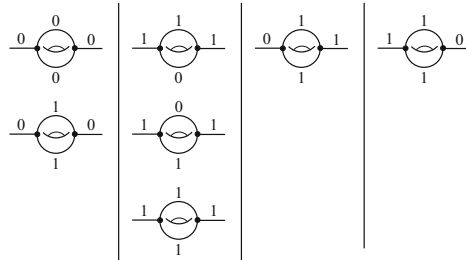
Denote the horizontal edges of the standard spine from right to left by e_1, e_2, \dots , as shown below.



Let $Z_b^{(k)}$ be the number of completions in which the rightmost labeled edge is e_k and has label $b \in \{0, 1\}$. One sees that $Z_0^{(1)} = 2$, and $Z_1^{(1)} = 1$, by the following enumeration of fusion-consistent diagrams.



Furthermore, we have the recurrence relations $Z_0^{(n+1)} = 2Z_0^{(n)} + Z_1^{(n)}$ and $Z_1^{(n+1)} = 3Z_1^{(n-1)} + Z_0^{(n-1)}$, by the following enumeration of fusion-consistent diagrams.



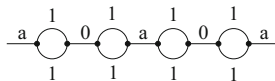
Solving these recurrence relations yields

$$\begin{bmatrix} Z_0^{(n)} \\ Z_1^{(n)} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{n-1} \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

The other two cases—completions starting with an upper curved edge, or a lower curved edge—can be solved similarly. The n^{th} power of a matrix may be computed using $O(\log n)$ operations, thus calculating the number of completions for any i in $O(\log g)$ steps. The corresponding thresholds are then immediately obtained by taking ratios of these.

D Inchworm

Suppose the spine-labeling contains a segment of the following form.

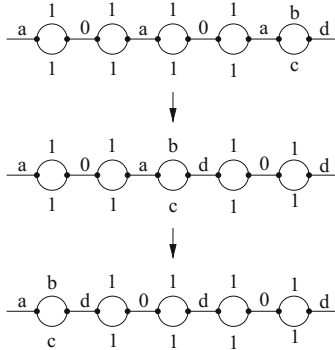


(8)

Here a can be 1 or 0. We call this configuration the inchworm. We may regard

the right instance of $\begin{array}{c} 1 \\ \circlearrowleft \\ \circlearrowright \\ 1 \end{array} \begin{array}{c} 1 \\ \circlearrowleft \\ 0 \\ \circlearrowright \\ 1 \end{array}$ as its head, and the left instance as its tail. We

next show a sequence of two reversible operations by which we can move the inchworm one handle rightward. In the first step the head moves one handle to the right, leaving the tail in place, and in the second step, the tail catches up, hence the name ‘‘inchworm.’’



Examination of the above diagram shows that if the fusion rules are obeyed in the initial configuration, they are also obeyed in the intermediate and final configurations. Furthermore, both steps are reversible (*i.e.* information preserving). Thus, they may be written as permutation matrices acting on the space of allowed configurations, and are therefore unitary. The first unitary transformation can be implemented by local Dehn twists, because the zero in the tail of the inchworm implies density of the Fibonacci representation on the segment to the right of it. The second unitary transformation can be implemented by local Dehn twists because the zero in the head of the inchworm implies density on the segment to the left of it. (In both steps, we are applying density to the twice-punctured genus-4 surface with one puncture labeled zero. There are 75 labelings in which the other puncture is labeled one and 50 labelings in which the other puncture is labeled zero. Thus, the decoupling lemma of [1] implies density *jointly* on these two subspaces.) Repeating this process and its reverse, we may bring the inchworm to any location within the spine.

To use the inchworm construction, we need to ensure that a segment of the form (8) exists in the first place. We may do this by implementing a reversible operation on the leftmost six handles, so that if the configuration (8) is absent, the matrix is strictly off-diagonal, and does not contribute to the trace. Specifically, we consider the leftmost two handles to be an ancilla system, and the next four handles to be the starting location of the inchworm. If these four handles do not take the form (8) we cyclically permute the (five) basis states of the ancilla system. Because this is done on the leftmost six handles, the segment is only singly-punctured, and thus Theorem 6.2 of [14] implies density without braiding.

The noncontributing labelings decrease the normalized WRT by a constant factor, which correspondingly necessitates decreasing the precision parameter ϵ by the same factor. More precisely, in the Fibonacci model, there are 325 fusion-consistent labelings for the spine of the genus-four doubly-punctured surface. Among these, there are two inchworm configurations ($a = 0$ and $a = 1$). Compounding this $2/325$ normalization cost with the precision $\epsilon = 1/24$ obtained in Appendix B for DQC1-hardness of absolute trace, we find that estimating the normalized WRT invariant to within $\pm 1/3900$ is DQC1-hard.

As an aside, we note that the inchworm construction here is simpler than that in [25], in the following sense. The inchworm construction of [25] involved reversible operations on logarithmically large regions. Although the density theorems imply that arbitrary reversible operations can be implemented on these regions, they do not imply that the decomposition into local moves is efficient. Rather this had to be explicitly proven in Appendix D of [25]. In contrast the inchworm construction here involves reversible operations only on $O(1)$ handles, thus no question of efficiency arises.

References

1. Aharonov, D., Arad, I.: The BQP-hardness of approximating the Jones polynomial. *New J. Phys.* **13**, 035019 (2011). arXiv:quant-ph/0605181
2. Aharonov, D., Jones, V., Landau, Z.: A polynomial quantum algorithm for approximating the Jones polynomial. In: *STOC 06* (2006). arXiv:quant-ph/0511096
3. Alagic, G., Jordan, S., König, R., Reichardt, B.: Approximating turaev-Viro 3-manifold invariants is universal for quantum computation. *Phys. Rev. A* **82**, 040302(R) (2010). arXiv:1003.0923
4. Ambainis, A., Schulman, L.J., Vazirani, U.: Computing with highly mixed states. *J. Assoc. Comput. Mach.* **53**(3), 507–531 (2006). A preliminary version appears in 2000 and is available at arXiv:quant-ph/0003136
5. Atiyah, Michael: Topological quantum field theories. *Publ. Mathématiques de l’IHÉS* **68**, 175–186 (1988)
6. Brandão, F.: Entanglement theory and the quantum simulation of many-body physics. Ph.D thesis, Imperial College London (2008). arXiv:0810.0026
7. Datta, A.: Studies on the role of entanglement in mixed-state quantum computation. Ph.D thesis, University of New Mexico (2008). arXiv:0807.4490
8. Datta, A., Flammia, S.T., Caves, C.M.: Entanglement and the power of one qubit. *Phys. Rev. A* **72**, 042316 (2005). arXiv:quant-ph/0505213
9. Datta, A., Gharibian, S.: Signatures of non-classicality in mixed-state quantum computation. *Phys. Rev. A* **79**, 042325 (2009). arXiv:0811.4003
10. Datta, A., Shaji, A., Caves, C.M.: Quantum discord and the power of one qubit. *Phys. Rev. Lett.* **100**, 050502 (2008). arXiv:0709.0548
11. Datta, A., Vidal, G.: On the role of entanglement and correlations in mixed-state quantum computation. *Phys. Rev. A* **75**, 042310 (2007). arXiv:quant-ph/0611157
12. Freedman, M., Kitaev, A., Wang, Z.: Simulation of topological field theories by quantum computers. *Commun. Math. Phys.* **227**, 587–603 (2002). arXiv:quant-ph/0001071
13. Freedman, M., Larsen, M., Wang, Z.: A modular functor which is universal for quantum computation. *Commun. Math. Phys.* **227**, 605 (2002). arXiv:quant-ph/0001108

14. Freedman, Michael H., Larsen, Michael J., Wang, Zhenghan: The two-eigenvalue problem and density of Jones representation of braid groups. *Commun. Math. Phys.* **228**, 177–199 (2002)
15. Garnerone, S., Marzuoli, A., Rasetti, M.: Efficient quantum processing of three-manifold topological invariants. *Adv. Theor. Math. Phys.* **13**(6), 1601–1652 (2009). arXiv:quant-ph/0703037
16. Jordan, S.P., Wocjan, P.: Estimating Jones and HOMFLY polynomials with one clean qubit. *Quantum Inf. Comput.* **9**, 264–289 (2009)
17. Knill, E., Laflamme, R.: Power of one bit of quantum information. *Phys. Rev. Lett.* **81**(25), 5672–5675 (1998). arXiv:quant-ph/9802037
18. Knill, E., Laflamme, R.: Quantum computation and quadratically signed weight enumerators. *Inf. Process. Lett.* **79**(4), 173–179 (2001). arXiv:quant-ph/9909094
19. Luo, Shunlong: Using measurement-induced disturbance to correlations as classical or quantum. *Phys. Rev. A* **77**, 022301 (2008)
20. Marx, R., Fahmy, A., Kauffman, L., Lomonaco, S., Spörl, A., Pomplun, N., Myers, J., Glaser, S.J.: NMR quantum calculations of the Jones polynomial (2009). arxiv:0909.1080
21. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
22. Passante, G., Moussa, O., Ryan, C.A., Laflamme, R.: Experimental approximation of the Jones polynomial with DQC1. *Phys. Rev. Lett.* **103**, 250501 (2009)
23. Roberts, Justin D.: Skein theory and Turaev-Viro invariants. *Topology* **34**, 771–787 (1995)
24. Shepherd, D.: Computation with unitaries and one pure qubit (2006). arXiv:quant-ph/0608132
25. Shor, P.W., Jordan, S.P.: Estimating Jones polynomials is complete for one clean qubit. *Quantum Inf. Comput.* **8**(8/9), 681–714 (2008)
26. Turaev, V.G.: *Topology of shadows*. preprint (1991)
27. Turaev, V.G.: *Quantum Invariants of Knots and 3-manifolds*. de Gruyter Studies in Mathematics, vol. 18. de Gruyter, New York (1994)
28. Walker, K.: On Witten’s 3-manifold invariants. <http://canyon23.net/math/1991TQFTNotes.pdf> (1991)
29. Wocjan, P., Yard, J.: The Jones polynomial: quantum algorithms and applications in quantum complexity theory. *Quantum Inf. Comput.* **8**, 147–180 (2008). arXiv:quant-ph/0603069

Span-Program-Based Quantum Algorithm for Evaluating Unbalanced Formulas

Ben W. Reichardt^(✉)

Institute for Quantum Computing, University of Waterloo, Waterloo, Canada
breic@iqc.ca

Abstract. The formula-evaluation problem is defined recursively. A formula’s evaluation is the evaluation of a gate, the inputs of which are themselves independent formulas. Despite this pure recursive structure, the problem is combinatorially difficult for classical computers.

A quantum algorithm is given to evaluate formulas over any finite boolean gate set. Provided that the complexities of the input subformulas to any gate differ by at most a constant factor, the algorithm has optimal query complexity. After efficient preprocessing, it is nearly time optimal. The algorithm is derived using the span program framework. It corresponds to the composition of the individual span programs for each gate in the formula. Thus the algorithm’s structure reflects the formula’s recursive structure.

1 Introduction

A k -bit *gate* is a function $f : \{0, 1\}^k \rightarrow \{0, 1\}$. A *formula* φ over a set of gates \mathcal{S} is a rooted tree in which each node with k children is associated to a k -bit gate from \mathcal{S} , for $k = 1, 2, \dots$. Any such tree with n leaves naturally defines a function $\varphi : \{0, 1\}^n \rightarrow \{0, 1\}$, by placing the input bits on the leaves in a fixed order and evaluating the gates recursively toward the root. Such functions are often called *read-once* formulas, as each input bit is associated to one leaf only.

The formula-evaluation problem is to evaluate a formula φ over \mathcal{S} on an input $x \in \{0, 1\}^n$. The formula is given, but the input string x must be queried one bit at a time. How many queries to x are needed to compute $\varphi(x)$? We would like to understand this complexity as a function of \mathcal{S} and asymptotic properties of φ . Roughly, larger gate sets allow φ to have less structure, which increases the complexity of evaluating φ . Another important factor is often the balancedness of the tree φ . Unbalanced formulas often seem to be more difficult to evaluate.

For applications, the most important gate set consists of all AND and OR gates. Formulas over this set are known as AND-OR formulas. Evaluating such a formula solves the decision version of a MIN-MAX tree, also known as a two-player game tree. Unfortunately, the complexity of evaluating formulas, even over this limited gate set, is unknown, although important special cases have been solved. The problem over much larger gate sets appears to be combinatorially intractable. For some formulas, it is known that “non-directional” algorithms

that do not work recursively on the structure of the formula perform better than any recursive procedure.

In this article, we show that the formula-evaluation problem becomes dramatically simpler when we allow the algorithm to be a bounded-error quantum algorithm, and allow it coherent query access to the input string x . Fix \mathcal{S} to be any finite set of gates. We give an optimal quantum algorithm for evaluating “almost-balanced” formulas over \mathcal{S} . The balance condition states that the complexities of the input subformulas to any gate differ by at most a constant factor, where complexity is measured by the general adversary bound Adv^\pm . In general, Adv^\pm is the value of an exponentially large semi-definite program (SDP). For a formula φ with constant-size gates, though, $\text{Adv}^\pm(\varphi)$ can be computed efficiently by solving constant-size SDPs for each gate.

To place this work in context, some classical and quantum results for evaluating formulas are summarized in Table 1. The stated upper bounds are on query complexity and not time complexity. However, for the OR_n and balanced $\text{AND}_2\text{-OR}_2$ formulas, the quantum algorithms’ running times are only slower by a poly-logarithmic factor. For the other formulas, the quantum algorithms’ running times are slower by a poly-logarithmic factor provided that:

1. A polynomial-time classical preprocessing step, outputting a string $s(\varphi)$, is not charged for.
2. The algorithms are allowed unit-cost coherent access to $s(\varphi)$.

Our algorithm is based on the framework relating span programs and quantum algorithms from [Rei09]. Previous work has used span programs to develop quantum algorithms for evaluating formulas [RŠ08]. Using this and the observation that the optimal span program witness size for a boolean function f equals the general adversary bound $\text{Adv}^\pm(f)$, Ref. [Rei09] gives an optimal quantum algorithm for evaluating “adversary-balanced” formulas over an arbitrary finite gate set. The balance condition is that each gate’s input subformulas have equal general adversary bounds.

In order to relax this strict balance requirement, we must maintain better control in the recursive analysis. To help do so, we define a new span program complexity measure, the “full witness size.” This complexity measure has implications for developing time- and query-efficient quantum algorithms based on span programs. Essentially, using a second result from [Rei09], that properties of eigenvalue-zero eigenvectors of certain bipartite graphs imply “effective” spectral gaps around zero, it allows quantum algorithms to be based on span programs with free inputs. This can simplify the implementation of a quantum walk on the corresponding graph.

Besides allowing a relaxed balance requirement, our approach has the additional advantage of making the constants hidden in the big- O notation more explicit. The formula-evaluation quantum algorithms in [RŠ08, Rei09] evaluate certain formulas φ using $O(\text{Adv}^\pm(\varphi))$ queries, where the hidden constant depends on the gates in \mathcal{S} in a complicated manner. It is not known how to upper-bound the hidden constant in terms of, say, the maximum fan-in k of a

Table 1. Comparison of some classical and quantum query complexity results for formula evaluation. Here \mathcal{S} is any fixed, finite gate set, and the exponent α is given by $\alpha = \log_2\left(\frac{1+\sqrt{33}}{4}\right) \approx 0.753$. Under certain assumptions, the algorithms' running times are only poly-logarithmically slower.

Formula φ	Randomized, zero-error query complexity $R(\varphi)$	Quantum bounded-error query complexity $Q(\varphi)$
OR_n	n	$\Theta(\sqrt{n})$ [Gro96, BBBV97]
Balanced AND_2 - OR_2	$\Theta(n^\alpha)$ [SW86]	$\Theta(\sqrt{n})$ [FGG08, ACR ⁺ 10]
Well-balanced AND - OR	Tight recursion [SW86]	$\Theta(\sqrt{n})$ [ACR ⁺ 10], (Theorem 8)
Approx.-balanced AND - OR		$\Omega(\sqrt{n})$ [BS04]
Arbitrary AND - OR	$\Omega(n^{0.51})$ [HW91]	$O(\sqrt{n} \log n)$ [Rei11]
Balanced MAJ_3 ($n = 3^d$)	$\Omega((7/3)^d), O(2.654^d)$ [JKS03]	$\Theta(2^d)$ [RŠ08]
Balanced over \mathcal{S}		$\Theta(\text{Adv}^\pm(\varphi))$ [Rei09]
Almost-balanced over \mathcal{S}		$\Theta(\text{Adv}^\pm(\varphi))$ (Theorem 7)

gate in \mathcal{S} . In contrast, the approach we follow here allows bounding this constant by an exponential in k .

It is known that the general adversary bound is a nearly tight lower bound on quantum query complexity for *any* boolean function [Rei09], including in particular boolean formulas. However, this comes with no guarantees on time complexity. The main contribution of this paper is to give a nearly time-optimal algorithm for formula evaluation. The algorithm is also tight for query complexity, removing the extra logarithmic factor from the bound in [Rei09].

Additionally, we apply the same technique to study AND - OR formulas. For this special case, special properties of span programs for AND and for OR gates allow the almost-balance condition to be significantly weakened. Ambainis et al. [ACR⁺10] have studied this case previously. By applying the span program framework, we identify a slight weakness in their analysis. Tightening the analysis extends the algorithm's applicability to a broader class of AND - OR formulas.

A companion paper [Rei11] applies the span program framework to the problem of evaluating *arbitrary* AND - OR formulas. By studying the full witness size for span programs constructed using a novel composition method, it gives an $O(\sqrt{n} \log n)$ -query quantum algorithm to evaluate a formula of size n , for which the time complexity is poly-logarithmically worse after preprocessing. This nearly matches the $\Omega(\sqrt{n})$ lower bound, and improves a $\sqrt{n}2^{O(\sqrt{\log n})}$ -query quantum algorithm from [ACR⁺10]. Reference [Rei11] shares the broader motivation of this paper, to study span program properties and design techniques that lead to time-efficient quantum algorithms.

Sections 1.1 and 1.2 below give further background on the formula-evaluation problem, for classical and quantum algorithms. Section 1.3 precisely states our main theorem, the proof of which is given in Sect. 3 after some background on

span programs. The theorem for approximately balanced AND-OR formulas is stated in Sect. 1.4, and proved in Sect. 4.

1.1 History of the Formula-Evaluation Problem for Classical Algorithms

For a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, let $D(f)$ be the least number of input bit queries sufficient to evaluate f on any input with zero error. $D(f)$ is known as the deterministic decision-tree complexity of f , or the deterministic query complexity of f . Let the randomized decision-tree complexity of f , $R(f) \leq D(f)$, be the least *expected* number of queries required to evaluate f with zero error (i.e., by a Las Vegas randomized algorithm). Let the Monte Carlo decision-tree complexity, $R_2(f) = O(R(f))$, be the least number of queries required to evaluate f with error probability at most $1/3$ (i.e., by a Monte Carlo randomized algorithm).

Classically, formulas over the gate set $\mathcal{S} = \{\text{NAND}_k : k \in \mathbf{N}\}$ have been studied most extensively, where $\text{NAND}_k(x_1, \dots, x_k) = 1 - \prod_{j=1}^k x_j$. By De Morgan's rules, any formula over NAND gates can also be written as a formula in which the gates at an even distance from the formula's root are AND gates and those at an odd distance away are OR gates, with some inputs or the output possibly complemented. Thus formulas over \mathcal{S} are also known as AND-OR formulas.

For any AND-OR formula φ of size n , i.e., on n inputs, $D(\varphi) = n$. However, randomization gives a strict advantage; $R(\varphi)$ and $R_2(\varphi)$ can be strictly smaller. Indeed, let φ_d be the complete, binary AND-OR formula of depth d , corresponding to the tree in which each internal vertex has two children and every leaf is at distance d from the root, with alternating levels of AND and OR gates. Its size is $n = 2^d$. Snir [Sni85] has given a randomized algorithm for evaluating φ_d using in expectation $O(n^\alpha)$ queries, where $\alpha = \log_2\left(\frac{1+\sqrt{33}}{4}\right) \approx 0.753$ [SW86]. This algorithm, known as randomized alpha-beta pruning, evaluates a random subformula recursively, and only evaluates the second subformula if necessary. Saks and Wigderson [SW86] have given a matching lower bound on $R(\varphi_d)$, which Santha has extended to hold for Monte Carlo algorithms, $R_2(\varphi_d) = \Omega(n^\alpha)$ [San95].

Thus the query complexities have been characterized for the complete, binary AND-OR formulas. In fact, the tight characterization works for a larger class of formulas, called "well balanced" formulas by [San95]. This class includes, for example, alternating $\text{AND}_2\text{-OR}_2$ formulas where for some d every leaf is at depth d or $d - 1$, Fibonacci trees and binomial trees [SW86]. It also includes skew trees, for which the depth is the maximal $n - 1$.

For arbitrary AND-OR formulas, on the other hand, little is known. It has been conjectured that complete, binary AND-OR formulas are the easiest to evaluate, and that in particular $R(\varphi) = \Omega(n^\alpha)$ for any size- n AND-OR formula φ [SW86]. However, the best general lower bound is $R(\varphi) = \Omega(n^{0.51})$, due to Heiman and Wigderson [HW91]. Reference [HW91] also extends the result of [SW86] to allow for AND and OR gates with fan-in more than two.

It is perhaps not surprising that formulas over most other gate sets \mathcal{S} are even less well understood. For example, Boppana has asked the complexity of

evaluating the complete ternary majority (MAJ₃) formula of depth d [SW86], and the best published bounds on its query complexity are $\Omega((7/3)^d)$ and $O((2.6537\dots)^d)$ [JKS03]. In particular, the naïve, “directional,” generalization of the randomized alpha-beta pruning algorithm is to evaluate recursively two random immediate subformulas and, if they disagree, then also the third. This algorithm uses $O((8/3)^d)$ expected queries, and is suboptimal. This suggests that the complete MAJ₃ formulas are significantly different from the complete AND-OR formulas.

Heiman, Newman and Wigderson have considered read-once threshold formulas in an attempt to separate the complexity classes TC⁰ from NC¹ [HNW93]. That is, they allow the gate set to be the set of Hamming-weight threshold gates $\{T_m^k : m, k \in \mathbf{N}\}$ defined by $T_m^k : \{0, 1\}^k \rightarrow \{0, 1\}$, $T_m^k(x) = 1$ if and only if the Hamming weight of x is at least m . AND, OR and majority gates are all special cases of threshold gates. Heiman et al. prove that $R(\varphi) \geq n/2^d$ for φ a threshold formula of depth d , and in fact their proof extends to gate sets in which every gate “contains a flip” [HNW93]. This implies that a large depth is necessary for the randomized complexity to be much lower than the deterministic complexity.

Of course there are some trivial gate sets for which the query complexity is fully understood, for example, the set of parity gates. Overall, though, there are many more open problems than results. Despite its structure, formula evaluation appears to be combinatorially complicated. However, there is another approach, to try to leverage the power of quantum computers. Surprisingly, the formula-evaluation problem simplifies considerably in this different model of computation.

1.2 History of the Formula-Evaluation Problem for Quantum Algorithms

In the quantum query model, the input bits can be queried coherently. That is, the quantum algorithm is allowed unit-cost access to the unitary operator O_x , called the input oracle, defined by

$$O_x : |\varphi\rangle \otimes |j\rangle \otimes |b\rangle \mapsto |\varphi\rangle \otimes |j\rangle \otimes |b \oplus x_j\rangle . \quad (1.1)$$

Here $|\varphi\rangle$ is an arbitrary pure state, $\{|j\rangle : j = 1, 2, \dots, n\}$ is an orthonormal basis for \mathbf{C}^n , $\{|b\rangle : b = 0, 1\}$ is an orthonormal basis for \mathbf{C}^2 , and \oplus denotes addition mod two. O_x can be implemented efficiently on a quantum computer given a classical circuit that computes the function $j \mapsto x_j$ [NC00]. For a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, let $Q(f)$ be the number of input queries required to evaluate f with error probability at most $1/3$. It is immediate that $Q(f) \leq R_2(f)$.

Research on the formula-evaluation problem in the quantum model began with the n -bit OR function, OR _{n} . Grover gave a quantum algorithm for evaluating OR _{n} with bounded one-sided error using $O(\sqrt{n})$ oracle queries and $O(\sqrt{n} \log \log n)$ time [Gro96, Gro02]. In the classical case, on the other hand, it is obvious that $R_2(\text{OR}_n)$, $R(\text{OR}_n)$ and $D(\text{OR}_n)$ are all $\Theta(n)$.

Grover’s algorithm can be applied recursively to speed up the evaluation of more general AND-OR formulas. Call a formula *layered* if the gates at the

same depth are the same. Buhrman, Cleve and Wigderson show that a layered, depth- d , size- n AND-OR formula can be evaluated using $O(\sqrt{n} \log^{d-1} n)$ queries [BCW98]. The logarithmic factors come from using repetition at each level to reduce the error probability from a constant to be polynomially small.

Høyer, Mosca and de Wolf [HMW03] consider the case of a unitary input oracle \tilde{O}_x that maps

$$\tilde{O}_x : |\varphi\rangle \otimes |j\rangle \otimes |b\rangle \otimes |0\rangle \mapsto |\varphi\rangle \otimes |j\rangle \otimes (|b \oplus x_j\rangle \otimes |\psi_{x,j,x_j}\rangle + |b \oplus \bar{x}_j\rangle \otimes |\psi_{x,j,\bar{x}_j}\rangle), \quad (1.2)$$

where $|\psi_{x,j,x_j}\rangle, |\psi_{x,j,\bar{x}_j}\rangle$ are pure states with $\| |\psi_{x,j,x_j}\rangle \|^2 \geq 2/3$. Such an oracle can be implemented when the function $j \mapsto x_j$ is computed by a bounded-error, randomized subroutine. Høyer et al. allow access to \tilde{O}_x and \tilde{O}_x^{-1} , both at unit cost, and show that OR_n can still be evaluated using $O(\sqrt{n})$ queries. This *robustness* result implies that the $\log n$ steps of repetition used by [BCW98] are not necessary, and a depth- d layered AND-OR formula can be computed in $O(\sqrt{n} c^{d-1})$ queries, for some constant $c > 1000$. If the depth is constant, this gives an $O(\sqrt{n})$ -query quantum algorithm, but the result is not useful for the complete, binary AND-OR formula, for which $d = \log_2 n$.

In 2007, Farhi, Goldstone and Gutmann presented a quantum algorithm for evaluating complete, binary AND-OR formulas [FGG08]. Their breakthrough algorithm is not based on iterating Grover’s algorithm in any way, but instead runs a quantum walk—analogueous to a classical random walk—on a graph based on the formula. The algorithm runs in time $O(\sqrt{n})$ in a certain continuous-time query model.

Ambainis et al. discretized the [FGG08] algorithm by reinterpreting a correspondence between (discrete-time) random and quantum walks due to Szegedy [Sze04] as a correspondence between continuous-time and discrete-time quantum walks [ACR+10]. Applying this correspondence to quantum walks on certain *weighted* graphs, they gave an $O(\sqrt{n})$ -query quantum algorithm for evaluating “approximately balanced” AND-OR formulas. For example, $\text{MAJ}_3(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee ((x_1 \vee x_2) \wedge x_3)$, so there is a size- 5^d AND-OR formula that computes MAJ_3^d (the complete ternary majority formula of depth d). Since the formula is approximately balanced, $Q(\text{MAJ}_3^d) = O(\sqrt{5}^d)$, better than the $\Omega((7/3)^d)$ classical lower bound.

The [ACR+10] algorithm also applies to arbitrary AND-OR formulas. If φ has size n and depth d , then the algorithm, applied directly, evaluates φ using $O(\sqrt{n} d)$ queries.¹ This can be as bad as $O(n^{3/2})$ if the depth is $d = n$. However, Bshouty, Cleve and Eberly have given a formula rebalancing procedure that takes AND-OR formula φ as input and outputs an equivalent AND-OR formula φ' with depth $d' = 2^{O(\sqrt{\log n})}$ and size $n' = n 2^{O(\sqrt{\log n})}$ [BCE91, BB94]. The formula φ' can then be evaluated using $O(\sqrt{n'} d') = \sqrt{n} 2^{O(\sqrt{\log n})}$ queries.

¹ Actually, [ACR+10, Section 7] only shows a bound of $O(\sqrt{n} d^{3/2})$ queries, but this can be improved to $O(\sqrt{n} d)$ using the bounds on $\sigma_{\pm}(\varphi)$ below [ACR+10, Definition 1].

Our understanding of *lower* bounds for the formula-evaluation problem progressed in parallel to this progress on quantum algorithms. There are essentially two techniques, the *polynomial* and *adversary* methods, for lower-bounding quantum query complexity.

- The polynomial method, introduced in the quantum setting by Beals et al. [BBC⁺01], is based on the observation that after making q oracle O_x queries, the probability of any measurement result is a polynomial of degree at most $2q$ in the variables x_j .
- Ambainis generalized the classical hybrid argument, to consider the system’s entanglement when run on a superposition of inputs [Amb02]. A number of variants of Ambainis’s bound were soon discovered, including weighted versions [HNS02, BS04, Amb06, Zha05], a spectral version [BSS03], and a version based on Kolmogorov complexity [LM04]. These variants can be asymptotically stronger than Ambainis’s original unweighted bound, but are equivalent to each other [ŠS06]. We therefore term it simply “the adversary bound,” denoted by Adv.

The adversary bound is well-suited for lower-bounding the quantum query complexity for evaluating formulas. For example, Barnum and Saks proved that for any size- n AND-OR formula φ , $\text{Adv}(\varphi) = \sqrt{n}$, implying the lower bound $Q(\varphi) = \Omega(\sqrt{n})$ [BS04]. Thus the [ACR⁺10] algorithm is optimal for approximately balanced AND-OR formulas, and is nearly optimal for arbitrary AND-OR formulas. This is a considerably more complete solution than is known classically.

It is then natural to consider formulas over larger gate sets. The adversary bound continues to work well, because it transforms nicely under function composition:

Theorem 1 (Adversary bound composition [Amb06, LLS06, HLŠ05]). *Let $f : \{0, 1\}^k \rightarrow \{0, 1\}$ and let $f_j : \{0, 1\}^{m_j} \rightarrow \{0, 1\}$ for $j = 1, 2, \dots, k$. Define $g : \{0, 1\}^{m_1} \times \dots \times \{0, 1\}^{m_k} \rightarrow \{0, 1\}$ by $g(x) = f(f_1(x_1), \dots, f_k(x_k))$. Let $s = (\text{Adv}(f_1), \dots, \text{Adv}(f_k))$. Then*

$$\text{Adv}(g) = \text{Adv}_s(f). \tag{1.3}$$

See Definition 3 for the definition of the adversary bound with “costs,” Adv_s . The Adv bound equals Adv_s with uniform, unit costs $s = \vec{1}$. For a function f , $\text{Adv}(f)$ can be computed using a semi-definite program in time polynomial in the size of f ’s truth table. Therefore, Theorem 1 gives a polynomial-time procedure for computing the adversary bound for a formula φ over an arbitrary finite gate set: compute the bounds for subformulas, moving from the leaves toward the root. At an internal node f , having computed the adversary bounds for the input subformulas f_1, \dots, f_k , Eq. (1.3) says that the adversary bound for g , the subformula rooted at f , equals the adversary bound for the *gate* f with certain costs. Computing this requires $2^{O(k)}$ time, which is a constant if $k = O(1)$. For example, if f is an OR_k or AND_k gate, then $\text{Adv}_{(s_1, \dots, s_k)}(f) = \sqrt{\sum_j s_j^2}$, from

which follows immediately the [BS04] result $\text{Adv}(\varphi) = \sqrt{n}$ for a size- n AND-OR formula φ .

A special case of Theorem 1 is when the functions f_j all have equal adversary bounds, so $\text{Adv}(g) = \text{Adv}(f)\text{Adv}(f_1)$. In particular, for a function $f : \{0, 1\}^k \rightarrow \{0, 1\}$ and a natural number $d \in \mathbf{N}$, let $f^d : \{0, 1\}^{k^d} \rightarrow \{0, 1\}$ denote the complete, depth- d formula over f . That is, $f^1 = f$ and $f^d(x) = f(f^{d-1}(x_1, \dots, x_{k^{d-1}}), \dots, f^{d-1}(x_{k^{d-k^{d-1}+1}}, \dots, x_{k^d}))$ for $d > 1$. Then we obtain:

Corollary 1. For any function $f : \{0, 1\}^k \rightarrow \{0, 1\}$,

$$\text{Adv}(f^d) = \text{Adv}(f)^d . \quad (1.4)$$

In particular, Ambainis defined a boolean function $f : \{0, 1\}^4 \rightarrow \{0, 1\}$ that can be represented exactly by a polynomial of degree two, but for which $\text{Adv}(f) = 5/2$ [Amb06]. Thus f^d can be represented exactly by a polynomial of degree 2^d , but by Corollary 1, $\text{Adv}(f^d) = (5/2)^d$. For this function, the adversary bound is strictly stronger than any bound obtainable using the polynomial method. Many similar examples are given in [HLŠ06]. However, for other functions, the adversary bound is asymptotically worse than the polynomial method [ŠS06, AS04, Amb05].

In 2007, though, Høyer et al. discovered a strict generalization of Adv that also lower-bounds quantum query complexity [HLŠ06]. We call this new bound the *general adversary bound*, or Adv^\pm . For example, for Ambainis's four-bit function f , $\text{Adv}^\pm(f) \geq 2.51$ [HLŠ06]. Like the adversary bound, $\text{ADV}_s^\pm(f)$ can be computed in time polynomial in the size of f 's truth table, and also composes nicely:

Theorem 2 ([HLŠ07, Rei09]). *Under the conditions of Theorem 1,*

$$\text{Adv}^\pm(g) = \text{ADV}_s^\pm(f) . \quad (1.5)$$

In particular, if $\text{Adv}^\pm(f_1) = \dots = \text{Adv}^\pm(f_k)$, then we have $\text{Adv}^\pm(g) = \text{Adv}^\pm(f) \text{Adv}^\pm(f_1)$.

Define a formula φ to be *adversary balanced* if at each internal node, the general adversary bounds of the input subformulas are equal. In particular, by Theorem 2 this implies that $\text{Adv}^\pm(\varphi)$ is equal to the product of the general adversary bounds of the gates along any path from the root to a leaf. Complete, layered formulas are an example of adversary-balanced formulas.

Returning to upper bounds, Reichardt and Špalek [RŠ08] generalized the algorithmic approach started by [FGG08]. They gave an optimal quantum algorithm for evaluating adversary-balanced formulas over a considerably extended gate set, including in particular all functions $\{0, 1\}^k \rightarrow \{0, 1\}$ for $k \leq 3$, 69 inequivalent four-bit functions, and the gates AND_k , OR_k , PARITY_k and EQUAL_k , for $k = O(1)$. For example, $Q(\text{MAJ}_3^d) = \Theta(2^d)$.

The [RŠ08] result follows from a framework for developing formula-evaluation quantum algorithms based on *span programs*. A span program, introduced by Karchmer and Wigderson [KW93], is a certain linear-algebraic way of defining a function, which corresponds closely to eigenvalue-zero eigenvectors of certain bipartite graphs. [RŠ08] derived a quantum algorithm for evaluating certain concatenated span programs, with a query complexity upper-bounded by the span program *witness size*, denoted wsize . In particular, a special case of [RŠ08, Theorem 4.7] is:

Theorem 3 ([RŠ08]). *Fix a function $f : \{0, 1\}^k \rightarrow \{0, 1\}$. If span program P computes f , then*

$$Q(f^d) = O(\text{wsize}(P)^d) . \quad (1.6)$$

From Theorem 2, this result is optimal if $\text{wsize}(P) = \text{Adv}^\pm(f)$. The question therefore becomes how to find optimal span programs. Using an ad hoc search, [RŠ08] found optimal span programs for a variety of functions with $\text{Adv}^\pm = \text{Adv}$. Further work automated the search, by giving a semi-definite program (SDP) for the optimal span program witness size for any given function [Rei09]. Remarkably, the SDP's value always equals the general adversary bound:

Theorem 4 ([Rei09]). *For any function $f : \{0, 1\}^n \rightarrow \{0, 1\}$,*

$$\inf_P \text{wsize}(P) = \text{Adv}^\pm(f) , \quad (1.7)$$

where the infimum is over span programs P computing f . Moreover, this infimum is achieved.

This result greatly extends the gate set over which the formula-evaluation algorithm of [RŠ08] works optimally. For example, combined with Theorem 3, it implies that $\lim_{d \rightarrow \infty} Q(f^d)^{1/d} = \text{Adv}^\pm(f)$ for every boolean function f . More generally, Theorem 4 allows the [RŠ08] algorithm to be run on formulas over any finite gate set \mathcal{S} . A factor is lost that depends on the gates in \mathcal{S} , but it will be a constant for \mathcal{S} finite. Combining Theorem 4 with [RŠ08, Theorem 4.7] gives:

Theorem 5 ([Rei09]). *Let \mathcal{S} be a finite set of gates. Then there exists a quantum algorithm that evaluates an adversary-balanced formula φ over \mathcal{S} using $O(\text{Adv}^\pm(\varphi))$ input queries. After efficient classical preprocessing independent of the input x , and assuming unit-time coherent access to the preprocessed classical string, the running time of the algorithm is $\text{Adv}^\pm(\varphi)(\log \text{Adv}^\pm(\varphi))^{O(1)}$.*

In the discussion so far, we have for simplicity focused on query complexity. The query complexity is an information-theoretic quantity that does not charge for operations independent of the input string, even though these operations may require many elementary gates to implement. For practical algorithms, it is important to be able to bound the algorithm's *running time*, which counts the cost of implementing the input-independent operations. Theorem 5 puts an optimal bound on the query complexity, and also puts a nearly optimal bound

on the algorithm's time complexity. In fact, all of the query-optimal algorithms so far discussed are also nearly time optimal.

In general, though, an upper bound on the query complexity does not imply an upper bound on the time complexity. Reference [Rei09] also generalized the span program framework of [RS08] to apply to quantum algorithms not based on formulas. The main result of [Rei09] is:

Theorem 6 ([Rei09]). *For any function $f : \mathcal{D} \rightarrow \{1, 2, \dots, m\}$, with $\mathcal{D} \subseteq \{0, 1\}^n$, $Q(f)$ satisfies*

$$Q(f) = \Omega(\text{Adv}^\pm(f)) \tag{1.8}$$

$$\text{and } Q(f) = O\left(\text{Adv}^\pm(f) \frac{\log \text{Adv}^\pm(f)}{\log \log \text{Adv}^\pm(f)} \log(m) \log \log m\right). \tag{1.9}$$

Theorem 6 in particular allows us to compute the query complexity of formulas, up to the logarithmic factor. It does *not* give any guarantees on running time. However, the analysis required to prove Theorem 6 also leads to significantly simpler proofs of Theorem 5 and the AND-OR formula results of [ACR⁺10, FGG08]. Moreover, we will see that it allows the formula-evaluation algorithms to be extended to formulas that are not adversary balanced.

1.3 Quantum Algorithm for Evaluating Almost-Balanced Formulas

We give a formula-evaluation algorithm that is both query-optimal, without a logarithmic overhead, and, after an efficient preprocessing step, nearly time optimal. Define almost balance as follows:

Definition 1. *Consider a formula φ over a gate set \mathcal{S} . For a vertex v in the corresponding tree, let φ_v denote the subformula of φ rooted at v , and, if v is an internal vertex, let g_v be the corresponding gate. The formula φ is β -balanced if for every vertex v , with children c_1, c_2, \dots, c_k ,*

$$\frac{\max_j \text{Adv}^\pm(\varphi_{c_j})}{\min_j \text{Adv}^\pm(\varphi_{c_j})} \leq \beta . \tag{1.10}$$

(If c_j is a leaf, $\text{Adv}^\pm(\varphi_{c_j}) = 1$.) *Formula φ is almost balanced if it is β -balanced for some $\beta = O(1)$.*

In particular, an adversary-balanced formula is 1-balanced. We will show:

Theorem 7. *Let \mathcal{S} be a fixed, finite set of gates. Then there exists a quantum algorithm that evaluates an almost-balanced formula φ over \mathcal{S} using $O(\text{Adv}^\pm(\varphi))$ input queries. After polynomial-time classical preprocessing independent of the input, and assuming unit-time coherent access to the preprocessed string, the running time of the algorithm is $\text{Adv}^\pm(\varphi)(\log \text{Adv}^\pm(\varphi))^{O(1)}$.*

Theorem 7 is significantly stronger than Theorem 5, which requires exact balance. There are important classes of exactly balanced formulas, such as complete, layered formulas. In fact, it is sufficient that the multiset of gates along the simple path from the root to a leaf not depend on the leaf. Moreover, sometimes different gates have the same Adv^\pm bound; see [HLŠ06] for examples. Even still, exact adversary balance is a very strict condition.

The proof of Theorem 7 is based on the span program framework developed in Ref. [Rei09]. In particular, [Rei09, Theorem 9.1] gives *two* quantum algorithms for evaluating span programs. The first algorithm is based on a discrete-time simulation of a continuous-time quantum walk. It applies to arbitrary span programs, and is used, in combination with Theorem 4, to prove Theorem 6. However, the simulation incurs a logarithmic query overhead and potentially worse time complexity overhead, so this algorithm is not suitable for proving Theorem 7.

The second algorithm in [Rei09] is based directly on a discrete-time quantum walk, similar to previous optimal formula-evaluation algorithms [ACR⁺10, RŠ08]. However, this algorithm does not apply to an arbitrary span program. A bound is needed on the operator norm of the entry-wise absolute value of the weighted adjacency matrix for a corresponding graph. Further graph sparsity conditions are needed for the algorithm to be time efficient (see Theorem 9).

Unfortunately, the span program from Theorem 4 will not generally satisfy these conditions. Theorem 4 gives a *canonical* span program ([Rei09, Definition 5.1]). Even for a simple formula, the optimal canonical span program will typically correspond to a dense graph with large norm.

An example should clarify the problem. Consider the AND-OR formula $\psi(x) = ((x_1 \wedge x_2) \vee x_3) \wedge x_4 \vee (x_5 \wedge [x_6 \vee x_7])$, and consider the two graphs in Fig. 1. For an input $x \in \{0, 1\}^7$, modify the graphs by attaching dangling edges to every vertex j for which $x_j = 0$. Observe then that each graph has an eigenvalue-zero eigenvector supported on vertex 0—called a *witness*—if and only if $\psi(x) = 1$. The graphs correspond to different span programs computing ψ , and the quantum algorithm works essentially by running a quantum walk starting at vertex 0 in order to detect the witness. The graph on the left is a significantly simplified version of a canonical span program for ψ , and its density still makes it difficult to implement the quantum walk.

We will be guided by the second, simpler graph. Instead of applying Theorem 4 to φ as a whole, we apply it separately to every gate in the formula. We then compose these span programs, one per gate, according to the formula, using *direct-sum composition* (Definition 6). In terms of graphs, direct-sum composition attaches the output vertex of one span program’s graph to an input vertex of the next [RŠ08]. This leads to a graph whose structure somewhat follows the structure of the formula φ , as the graph in Fig. 1(b) follows the structure of ψ . (However, the general case will be more complicated than shown, as we are plugging together constant-size graph gadgets, and there may be duplication of some subgraphs.)

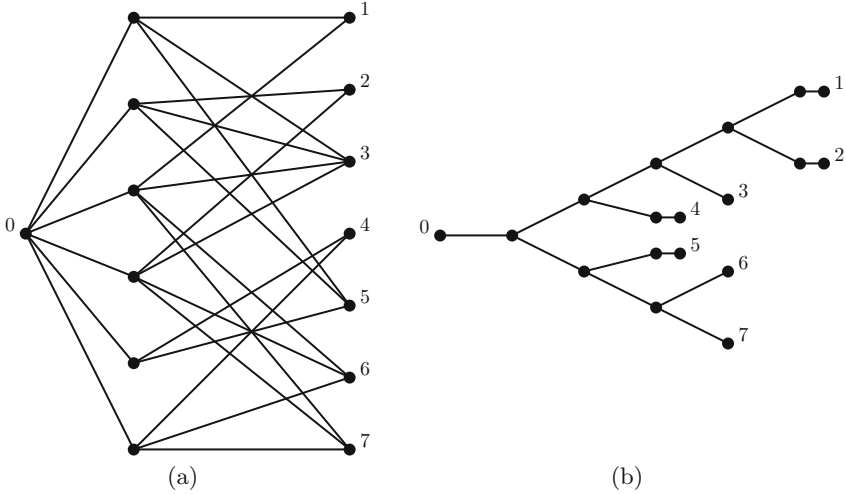


Fig. 1. Graphs corresponding to two span programs both computing the same function.

Direct-sum composition keeps the maximum degree and norm of the graph under control—each is at most twice its value for the worst single gate. Therefore the second [Rei09] algorithm applies. However, direct-sum composition also leads to additional overhead. In particular, a witness in the first graph will be supported only on numbered vertices (note that the graph is bipartite), whereas a witness in the second graph will be supported on some of the internal vertices as well. This means roughly that the second witness will be harder to detect, because after normalization its overlap on vertex 0 will be smaller. Scale both witnesses so that the amplitude on vertex 0 is one. The *witness size* (wsize) measures the squared length of the witness only on numbered vertices, whereas the *full witness size* (fwsiz) measures the squared length on all vertices. For [Rei09], it was sufficient to consider only span program witness size, because for canonical span programs like in Fig. 1(a) the two measures are equal. (For technical reasons, we will actually define fwsiz to be $1 + \text{wsize}$ even in this case.) For our analysis, we will need to bound the full witness size in terms of the witness size. We maintain this bound in a recursion from the formula’s leaves toward its root.

A span program is called *strict* if every vertex on one half of the bipartite graph is either an input vertex (vertices 1–7 in the graphs of Fig. 1) or the output vertex (vertex 0). Thus the first graph in the example above corresponds to a strict span program, and the second does not. The original definition of span programs, in [KW93], allowed for only strict span programs. This was sensible because any other vertices on the input/output part of the graph’s bipartition can always be projected away, yielding a strict span program that computes the same function. For developing time-efficient quantum algorithms, though, it seems important to consider span programs that are not strict. Unfortunately, going backwards, e.g., from 1(a) to 1(b), is probably difficult in general.

Theorem 7 does *not* follow from the formula-evaluation techniques of [RŠ08], together with Theorem 3 from [Rei09]. This tempting approach falls into intractable technical difficulties. In particular, the same span program can be used at two vertices v and w in φ only if $g_v = g_w$ and the general adversary bounds of v 's input subformulas are the same as those for w 's inputs up to simultaneous scaling. In general, then, an almost-balanced formula will require an unbounded number of different span programs. However, the analysis in [RŠ08] loses a factor that depends badly on the individual span programs. Since the dependence is not continuous, even showing that the span programs in use all lie within a compact set would not be sufficient to obtain an $O(1)$ upper bound. In contrast, the approach we follow here allows bounding the lost factor by an exponential in k , uniformly over different gate imbalances.

1.4 Quantum Algorithm to Evaluate Approximately Balanced AND-OR Formulas

Ambainis et al. [ACR⁺10] use a weaker balance criterion for AND-OR formulas than Definition 1. They define an AND-OR formula to be approximately balanced if $\sigma_-(\varphi) = O(1)$ and $\sigma_+(\varphi) = O(n)$. Here n is the size of the formula, i.e., the number of leaves, and $\sigma_-(\varphi)$ and $\sigma_+(\varphi)$ are defined by:

Definition 2. For each vertex v in a formula φ , let

$$\begin{aligned}\sigma_-(v) &= \max_{\xi} \sum_{w \in \xi} \frac{1}{\text{Adv}^{\pm}(\varphi_w)} \\ \sigma_+(v) &= \max_{\xi} \sum_{w \in \xi} \text{Adv}^{\pm}(\varphi_w)^2 \ ,\end{aligned}\tag{1.11}$$

with each maximum taken over all simple paths ξ from v to a leaf. Let $\sigma_{\pm}(\varphi) = \sigma_{\pm}(r)$, where r is the root of φ .

Recall that $\text{Adv}^{\pm}(\varphi) = \text{Adv}(\varphi) = \sqrt{n}$ for an AND-OR formula. Definition 1 is a stricter balance criterion because β -balance of a formula φ implies (by Lemma 3) that $\sigma_-(\varphi)$ and $\sigma_+(\varphi)$ are both dominated by geometric series. However, the same steps followed by the proof of Theorem 7 still suffice for proving the [ACR⁺10] result, and, in fact, for strengthening it. We show:

Theorem 8. Let φ be an AND-OR formula of size n . Then after polynomial-time classical preprocessing that does not depend on the input x , $\varphi(x)$ can be evaluated by a quantum algorithm with error at most $1/3$ using $O(\sqrt{n} \sigma_-(\varphi))$ input queries. The algorithm's running time is $\sqrt{n} \sigma_-(\varphi) (\log n)^{O(1)}$ assuming unit-cost coherent access to the preprocessed string.

For the special case of AND-OR formulas with $\sigma_-(\varphi) = O(1)$, Theorem 8 strengthens Theorem 7. The requirement that $\sigma_-(\varphi) = O(1)$ allows for some gates in the formula to be very unbalanced. Theorem 8 also strengthens

[ACR⁺10, Theorem 1] because it does not require that $\sigma_+(\varphi) = O(n)$. For example, a formula that is biased near the root, but balanced at greater depths can have $\sigma_-(\varphi) = O(1)$ and $\sigma_+(\varphi) = \omega(n)$. By substituting the bound $\sigma_-(\varphi) = O(\sqrt{d})$ for a depth- d formula [ACR⁺10, Definition 3], a corollary of Theorem 8 is that a depth- d , size- n AND-OR formula can be evaluated using $O(\sqrt{nd})$ queries. This improves the depth-dependence from [ACR⁺10], and matches the dependence from an earlier version of that article [Amb07].

The essential reason that the Definition 1 balance condition can be weakened is that for the specific gates AND and OR, by writing out the optimal span programs explicitly we can prove that they satisfy stronger properties than are necessarily true for other functions.

2 Span Programs

2.1 Definitions

We briefly recall some definitions from [Rei09, Section 2]. Additionally, we define a span program complexity measure, the full witness size, that charges even for the “free” inputs. This quantity is important for developing quantum algorithms that are time efficient as well as query efficient.

For a natural number n , let $[n] = \{1, 2, \dots, n\}$. For a finite set X , let \mathbf{C}^X be the inner product space $\mathbf{C}^{|X|}$ with orthonormal basis $\{|x\rangle : x \in X\}$. For vector spaces V and W over \mathbf{C} , let $\mathcal{L}(V, W)$ be the set of linear transformations from V into W , and let $\mathcal{L}(V) = \mathcal{L}(V, V)$. For $A \in \mathcal{L}(V, W)$, $\|A\|$ is the operator norm of A . For a string $x \in \{0, 1\}^n$, let \bar{x} denote its bitwise complement.

Definition 3 ([HLŠ05, HLŠ07]). *For finite sets C, E and $\mathcal{D} \subseteq C^n$, let $f : \mathcal{D} \rightarrow E$. An adversary matrix for f is a real, symmetric matrix $\Gamma \in \mathcal{L}(\mathbf{C}^{\mathcal{D}})$ that satisfies $\langle x | \Gamma | y \rangle = 0$ whenever $f(x) \neq f(y)$.*

The general adversary bound for f , with costs $s \in [0, \infty)^n$, is

$$ADV_s^\pm(f) = \max_{\substack{\text{adversary matrices } \Gamma: \\ \forall j \in [n], \|\Gamma \circ \Delta_j\| \leq s_j}} \|\Gamma\|. \tag{2.1}$$

Here $\Gamma \circ \Delta_j$ denotes the entry-wise matrix product between Γ and $\Delta_j = \sum_{x,y: x_j \neq y_j} |x\rangle\langle y|$. The (nonnegative-weight) adversary bound for f , with costs s , is defined by the same maximization, except with Γ restricted to have nonnegative entries. In particular, $ADV_s^\pm(f) \geq \text{Adv}_s(f)$.

Letting $\vec{1} = (1, 1, \dots, 1)$, the adversary bound for f is $\text{Adv}(f) = \text{Adv}_{\vec{1}}(f)$ and the general adversary bound for f is $\text{Adv}^\pm(f) = \text{Adv}_{\vec{1}}^\pm(f)$. By [HLŠ07], $Q(f) = \Omega(\text{Adv}^\pm(f))$.

Definition 4 (Span program [KW93]). *A span program P consists of a natural number n , a finite-dimensional inner product space V over \mathbf{C} , a “target”*

vector $|t\rangle \in V$, disjoint sets I_{free} and $I_{j,b}$ for $j \in [n]$, $b \in \{0,1\}$, and “input vectors” $|v_i\rangle \in V$ for $i \in I_{\text{free}} \cup \bigcup_{j \in [n], b \in \{0,1\}} I_{j,b}$.

To P corresponds a function $f_P : \{0,1\}^n \rightarrow \{0,1\}$, defined on $x \in \{0,1\}^n$ by

$$f_P(x) = \begin{cases} 1 & \text{if } |t\rangle \in \text{Span}(\{|v_i\rangle : i \in I_{\text{free}} \cup \bigcup_{j \in [n]} I_{j,x_j}\}) \\ 0 & \text{otherwise} \end{cases} \quad (2.2)$$

Some additional notation is convenient. Fix a span program P . Let $I = I_{\text{free}} \cup \bigcup_{j \in [n], b \in \{0,1\}} I_{j,b}$. Let $A \in \mathcal{L}(\mathbf{C}^I, V)$ be given by $A = \sum_{i \in I} |v_i\rangle\langle i|$. For $x \in \{0,1\}^n$, let $I(x) = I_{\text{free}} \cup \bigcup_{j \in [n]} I_{j,x_j}$ and $\Pi(x) = \sum_{i \in I(x)} |i\rangle\langle i| \in \mathcal{L}(\mathbf{C}^I)$. Then $f_P(x) = 1$ if $|t\rangle \in \text{Range}(A\Pi(x))$. A vector $|w\rangle \in \mathbf{C}^I$ is said to be a witness for $f_P(x) = 1$ if $\Pi(x)|w\rangle = |w\rangle$ and $A|w\rangle = |t\rangle$. A vector $|w'\rangle \in V$ is said to be a witness for $f_P(x) = 0$ if $\langle t|w'\rangle = 1$ and $\Pi(x)A^\dagger|w'\rangle = 0$.

Definition 5 (Witness size). Consider a span program P , and a vector $s \in [0, \infty)^n$ of nonnegative “costs.” Let $S = \sum_{j \in [n], b \in \{0,1\}, i \in I_{j,b}} \sqrt{s_j} |i\rangle\langle i| \in \mathcal{L}(\mathbf{C}^I)$. For each input $x \in \{0,1\}^n$, define the witness size of P on x with costs s , $\text{wsize}_s(P, x)$, as follows:

$$\text{wsize}_s(P, x) = \begin{cases} \min_{|w\rangle: A\Pi(x)|w\rangle=|t\rangle} \|S|w\rangle\|^2 & \text{if } f_P(x) = 1 \\ \min_{\substack{|w'\rangle: \langle t|w'\rangle=1 \\ \Pi(x)A^\dagger|w'\rangle=0}} \|SA^\dagger|w'\rangle\|^2 & \text{if } f_P(x) = 0 \end{cases} \quad (2.3)$$

The witness size of P with costs s is

$$\text{wsize}_s(P) = \max_{x \in \{0,1\}^n} \text{wsize}_s(P, x) . \quad (2.4)$$

Define the full witness size $\text{fwsiz}_s(P)$ by letting $S^f = S + \sum_{i \in I_{\text{free}}} |i\rangle\langle i|$ and

$$\text{fwsiz}_s(P, x) = \begin{cases} \min_{|w\rangle: A\Pi(x)|w\rangle=|t\rangle} (1 + \|S^f|w\rangle\|^2) & \text{if } f_P(x) = 1 \\ \min_{\substack{|w'\rangle: \langle t|w'\rangle=1 \\ \Pi(x)A^\dagger|w'\rangle=0}} (\|w'\|^2 + \|SA^\dagger|w'\rangle\|^2) & \text{if } f_P(x) = 0 \end{cases} \quad (2.5)$$

$$\text{fwsiz}_s(P) = \max_{x \in \{0,1\}^n} \text{fwsiz}_s(P, x) . \quad (2.6)$$

When the subscript s is omitted, the costs are taken to be uniform, $s = \vec{1} = (1, 1, \dots, 1)$, e.g., $\text{fwsiz}(P) = \text{fwsiz}_{\vec{1}}(P)$. The witness size is defined in [RŠ08]. The full witness size is defined in [Rei09, Section 8], but is not named there. A *strict* span program has $I_{\text{free}} = \emptyset$, so $S^f = S$, and a *monotone* span program has $I_{j,0} = \emptyset$ for all j [Rei09, Definition 4.9].

2.2 Quantum Algorithm to Evaluate a Span Program Based on Its Full Witness Size

[Rei09, Theorem 9.3] gives a quantum query algorithm for evaluating span programs based on the full witness size. The algorithm is based on a quantum walk on a certain graph. Provided that the degree of the graph is not too large, it can actually be implemented efficiently.

Theorem 9 ([Rei09, Theorem 9.3]). *Let P be a span program. Then f_P can be evaluated using*

$$T = O(\text{fwsz}(P) \parallel \text{abs}(A_{G_P}) \parallel) \quad (2.7)$$

quantum queries, with error probability at most $1/3$. Moreover, if the maximum degree of a vertex in G_P is d , then the time complexity of the algorithm for evaluating f_P is at most a factor of $(\log d)(\log(T \log d))^{O(1)}$ worse, after classical preprocessing and assuming constant-time coherent access to the preprocessed string.

Proof. (sketch) The query complexity claim is actually slightly weaker than [Rei09, Theorem 9.3], which allows the target vector to be scaled downward by a factor of $\sqrt{\text{fwsz}(P)}$.

The time-complexity claim will follow from the proof of [Rei09, Theorem 9.3], in [Rei09, Prop. 9.4, Theorem 9.5]. The algorithm for evaluating $f_P(x)$ uses a discrete-time quantum walk on the graph $G_P(x)$. If the maximum degree of a vertex in G_P is d , then each coin reflection can be implemented using $O(\log d)$ single-qubit unitaries and queries to the preprocessed string [GR02, CNW10]. Finally, the $(\log(T \log d))^{O(1)}$ factor comes from applying the Solovay-Kitaev Theorem [KSV02] to compile the single-qubit unitaries into products of elementary gates, to precision $1/O(T \log d)$. \square

We remark that together with [Rei09, Theorem 3.1], Theorem 9 gives a way of transforming a one-sided-error quantum algorithm into a span program, and back into a quantum algorithm, such that the time complexity is nearly preserved, after preprocessing. This is only a weak equivalence, because aside from requiring preprocessing the algorithm from Theorem 9 also has two-sided error. To some degree, though, it complements the equivalence results for best span program witness size and bounded-error quantum *query* complexity [Rei09, Theorem 7.1, Theorem 9.2].

2.3 Direct-Sum Span Program Composition

Let us study the full witness size of the direct-sum composition of span programs. We begin by recalling the definition of direct-sum composition.

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and $S \subseteq [n]$. For $j \in [n]$, let m_j be a natural number, with $m_j = 1$ for $j \notin S$. For $j \in S$, let $f_j : \{0, 1\}^{m_j} \rightarrow \{0, 1\}$. Define $y : \{0, 1\}^{m_1} \times \cdots \times \{0, 1\}^{m_n} \rightarrow \{0, 1\}^n$ by

$$y(x)_j = \begin{cases} f_j(x_j) & \text{if } j \in S \\ x_j & \text{if } j \notin S \end{cases} \quad (2.8)$$

Define $g : \{0, 1\}^{m_1} \times \cdots \times \{0, 1\}^{m_n} \rightarrow \{0, 1\}$ by $g(x) = f(y(x))$. For example, if $S = [n] \setminus \{1\}$, then

$$g(x) = f(x_1, f_2(x_2), \dots, f_n(x_n)) \quad (2.9)$$

Given span programs for the individual functions f and f_j for $j \in S$, we will construct a span program for g . We remark that although we are here requiring that the inner functions f_j act on disjoint sets of bits, this assumption is not necessary for the definition. It simplifies the notation, though, for the cases $S \neq [n]$, and will suffice for our applications.

Let P be a span program computing $f_P = f$. Let P have inner product space V , target vector $|t\rangle$ and input vectors $|v_i\rangle$ indexed by I_{free} and I_{jc} for $j \in [n]$ and $c \in \{0, 1\}$.

For $j \in [n]$, let $s_j \in [0, \infty)^{m_j}$ be a vector of costs, and let $s \in [0, \infty)^{\sum m_j}$ be the concatenation of the vectors s_j . For $j \in S$, let P^{j0} and P^{j1} be span programs computing $f_{P^{j1}} = f_j : \{0, 1\}^{m_j} \rightarrow \{0, 1\}$ and $f_{P^{j0}} = \neg f_j$, with $r_j = \text{wsize}_{s_j}(P^{j0}) = \text{wsize}_{s_j}(P^{j1})$. For $c \in \{0, 1\}$, let P^{jc} have inner product space V^{jc} with target vector $|t^{jc}\rangle$ and input vectors indexed by I_{free}^{jc} and I_{kb}^{jc} for $k \in [m_j]$, $b \in \{0, 1\}$. For $j \notin S$, let $r_j = s_j$.

Let $I_S = \bigcup_{j \in S, c \in \{0, 1\}} I_{jc}$. Define $\varsigma : I_S \rightarrow [n] \times \{0, 1\}$ by $\varsigma(i) = (j, c)$ if $i \in I_{jc}$. The idea is that ς maps i to the input span program that must evaluate to 1 in order for $|v_i\rangle$ to be available in P .

There are several ways of composing the span programs P and P^{jc} to obtain a span program Q computing the composed function $f_Q = g$ with $\text{wsize}_s(Q) \leq \text{wsize}_r(P)$ [Rei09, Defs. 4.4, 4.5, 4.6]. We focus on direct-sum composition.

Definition 6 ([Rei09, Definition 4.5]). *The direct-sum-composed span program Q^\oplus is defined by:*

- The inner product space is $V^\oplus = V \oplus \bigoplus_{j \in S, c \in \{0, 1\}} (\mathbf{C}^{I_{jc}} \otimes V^{jc})$. Any vector in V^\oplus can be uniquely expressed as $|u\rangle_V + \sum_{i \in I_S} |i\rangle \otimes |u_i\rangle$, where $|u\rangle \in V$ and $|u_i\rangle \in V^{\varsigma(i)}$.
- The target vector is $|t^\oplus\rangle = |t\rangle_V$.
- The free input vectors are indexed by $I_{\text{free}}^\oplus = I_{\text{free}} \cup I_S \cup \bigcup_{j \in S, c \in \{0, 1\}} (I_{jc} \times I_{\text{free}}^{jc})$ with, for $i \in I_{\text{free}}^\oplus$,

$$|v_i^\oplus\rangle = \begin{cases} |v_i\rangle_V & \text{if } i \in I_{\text{free}} \\ |v_i\rangle_V - |i\rangle \otimes |t^{jc}\rangle & \text{if } i \in I_{jc} \text{ and } j \in S \\ |i'\rangle \otimes |v_{i''}\rangle & \text{if } i = (i', i'') \in I_{jc} \times I_{\text{free}}^{jc} \end{cases} \quad (2.10)$$

- The other input vectors are indexed by $I_{(jk)b}^\oplus$ for $j \in [n]$, $k \in [m_j]$, $b \in \{0, 1\}$. For $j \notin S$, $I_{(j1)b}^\oplus = I_{jb}$, with $|v_i^\oplus\rangle = |v_i\rangle_V$ for $i \in I_{(j1)b}^\oplus$. For $j \in S$, let $I_{(jk)b}^\oplus = \bigcup_{c \in \{0, 1\}} (I_{jc} \times I_{kb}^{jc})$. For $i \in I_{jc}$ and $i' \in I_{kb}^{jc}$, let

$$|v_{i'i'}^\oplus\rangle = |i\rangle \otimes |v_{i'}\rangle. \quad (2.11)$$

By [Rei09, Theorem 4.3], $f_{Q^\oplus} = g$ and $\text{wsize}_s(Q^\oplus) \leq \text{wsize}_r(P)$. (While that theorem is stated only for the case $S = [n]$, it is trivially extended to other $S \subset [n]$.) We give a bound on how quickly the full witness size can grow relative to the witness size:

Lemma 1. *Under the above conditions, for each input $x \in \{0, 1\}^{m_1} \times \dots \times \{0, 1\}^{m_n}$, with $y = y(x)$,*

- *If $g(x) = 1$, let $|w\rangle$ be a witness to $f_P(y) = 1$ such that*

$$\sum_{j \in [n], i \in I_{jy_j}} r_j |w_i|^2 = \text{wsize}_r(P, y).$$

Then

$$\frac{\text{fsize}_s(Q^\oplus, x)}{\text{wsize}_r(P, y)} \leq \sigma(y, |w\rangle) + \frac{1 + \sum_{i \in I_{\text{free}}} |w_i|^2}{\text{wsize}_r(P, y)}$$

$$\text{where } \sigma(y, |w\rangle) = \max_{\substack{j \in S: \\ \exists i \in I_{jy_j} \text{ with } \langle i | w \rangle \neq 0}} \frac{\text{fsize}_{s_j}(P^{jy_j})}{\text{wsize}_{s_j}(P^{jy_j})}. \quad (2.12)$$

- *If $g(x) = 0$, let $|w'\rangle$ be a witness to $f_P(y) = 0$ such that*

$$\sum_{j \in [n], i \in I_{j\bar{y}_j}} r_j |\langle w' | v_i \rangle|^2 = \text{wsize}_r(P, y).$$

Then

$$\frac{\text{fsize}_s(Q^\oplus, x)}{\text{wsize}_r(P, y)} \leq \sigma(\bar{y}, |w'\rangle) + \frac{\| |w'\rangle \|^2}{\text{wsize}_r(P, y)}$$

$$\text{where } \sigma(\bar{y}, |w'\rangle) = \max_{\substack{j \in S: \\ \exists i \in I_{j\bar{y}_j} \text{ with } \langle v_i | w' \rangle \neq 0}} \frac{\text{fsize}_{s_j}(P^{j\bar{y}_j})}{\text{wsize}_{s_j}(P^{j\bar{y}_j})}. \quad (2.13)$$

If $S = \emptyset$, then $\sigma(y, |w\rangle)$ and $\sigma(\bar{y}, |w'\rangle)$ should each be taken to be 1 in the above equations.

Proof. We follow the proof of [Rei09, Theorem 4.3], except keeping track of the full witness size. Note that if $S = \emptyset$, then Eqs. (2.12) and (2.13) are immediate by definition of $\text{fsize}_s(Q^\oplus, x)$.

Let $I(y)' = I(y) \setminus I_{\text{free}} = \bigcup_{j \in [n]} I_{jy_j}$.

In the first case, $g(x) = 1$, for $j \in S$ let $|w^{jy_j}\rangle \in \mathbf{C}^{I^{jy_j}}$ be a witness to $f_{P^{jy_j}}(x_j) = 1$ such that $\text{fsize}_s(P^{jy_j}, x_j) = 1 + \sum_{i \in I_{\text{free}}^{jy_j}} |w_i^{jy_j}|^2 + \sum_{k \in [m_j], i \in I_{k(x_j)_k}^{jy_j}} (s_j)_k |w_i^{jy_j}|^2$. As in [Rei09, Theorem 4.3], let $|w^\oplus\rangle \in \mathbf{C}^{I^\oplus(x)}$ be given by

$$w_i^\oplus = \begin{cases} w_i & \text{if } i \in I(y) \\ w_{i'} w_{i''}^{s(i')} & \text{if } i = (i', i'') \text{ with } i' \in I(y)' \cap I_S, i'' \in I^{s(i')}(x) \\ 0 & \text{otherwise} \end{cases} \quad (2.14)$$

Then $|w^\oplus\rangle$ is a witness for $f_{Q^\oplus}(x) = 1$, and we compute

$$\begin{aligned}
\text{fwsizes}_s(Q^\oplus, x) &\leq 1 + \sum_{i \in I_{\text{free}}^\oplus} |w_i^\oplus|^2 + \sum_{\substack{j \in [n], k \in [m_j], \\ i \in I_{(j,k)(x_j)_k}^\oplus}} (s_j)_k |w_i^\oplus|^2 \\
&= 1 + \sum_{i \in I_{\text{free}}} |w_i|^2 + \sum_{j \in [n] \setminus S, i \in I_{jx_j}} s_j |w_i|^2 \\
&\quad + \sum_{j \in S, i \in I_{jy_j}} |w_i|^2 \left(1 + \sum_{i' \in I_{\text{free}}^{jy_j}} |w_{i'}^{jy_j}|^2 \right. \\
&\quad \left. + \sum_{k \in [m_j], i' \in I_{k(x_j)_k}^{jy_j}} (s_j)_k |w_{i'}^{jy_j}|^2 \right) \\
&= 1 + \sum_{i \in I_{\text{free}}} |w_i|^2 + \sum_{j \in [n] \setminus S, i \in I_{jx_j}} s_j |w_i|^2 \\
&\quad + \sum_{j \in S, i \in I_{jy_j}} |w_i|^2 \text{fwsizes}_{s_j}(P^{jy_j}, x_j).
\end{aligned} \tag{2.15}$$

Equation (2.12) follows using the bound $\text{fwsizes}_{s_j}(P^{jy_j}, x_j) \leq \sigma(y, |w\rangle)r_j$ for $j \in S$, and $s_j = r_j$ for $j \notin S$.

Next consider the case $g(x) = 0$. For $j \in S$, let $|u^{j\bar{y}_j}\rangle \in V^{j\bar{y}_j}$ be a witness for $f_{P^{j\bar{y}_j}}(x_j) = 0$ with $\text{fwsizes}_s(P^{j\bar{y}_j}, x_j) = \| |u^{j\bar{y}_j}\rangle \|^2 + \sum_{k \in [m_j], i \in I_{k(x_j)_k}^{j\bar{y}_j}} (s_j)_k |\langle v_i | u^{j\bar{y}_j} \rangle|^2$. As in [Rei09, Theorem 4.3], let

$$|u^\oplus\rangle = |w'\rangle_V + \sum_{i \in I_S \setminus I(y)} \langle v_i | w' \rangle |i\rangle \otimes |u^{s(i)}\rangle. \tag{2.16}$$

Then $|u^\oplus\rangle$ is a witness for $f_{Q^\oplus}(x) = 0$, and, moreover,

$$\begin{aligned}
\text{fwsizes}_s(Q^\oplus, x) &\leq \| |u^\oplus\rangle \|^2 + \sum_{j \in [n], k \in [m_j], i \in I_{(j,k)(x_j)_k}^\oplus} (s_j)_k |\langle v_i^\oplus | u^\oplus \rangle|^2 \\
&= \| |u^\oplus\rangle \|^2 + \sum_{\substack{j \in [n] \setminus S \\ i \in I_{j\bar{x}_j}}} s_j |\langle v_i^\oplus | u^\oplus \rangle|^2 \\
&\quad + \sum_{\substack{j \in S, k \in [m_j], \\ i \in I_{j\bar{y}_j}, i' \in I_{k(x_j)_k}^{j\bar{y}_j}}} (s_j)_k |\langle v_{i'}^\oplus | u^\oplus \rangle|^2
\end{aligned}$$

$$\begin{aligned}
 &= \|w'\|^2 + \sum_{\substack{j \in [n] \setminus S \\ i \in I_{j\bar{x}_j}}} s_j |\langle v_i | w' \rangle|^2 & (2.17) \\
 &+ \sum_{j \in S, i \in I_{j\bar{y}_j}} |\langle v_i | w' \rangle|^2 \left(\|u^{j\bar{y}_j}\|^2 \right. \\
 &+ \left. \sum_{k \in [m_j], i' \in I_{\frac{j\bar{y}_j}{k(x_j)_k}}} (s_j)_k |\langle v_{i'} | u^{j\bar{y}_j} \rangle|^2 \right) \\
 &= \|w'\|^2 + \sum_{\substack{j \in [n] \setminus S \\ i \in I_{j\bar{x}_j}}} r_j |\langle v_i | w' \rangle|^2 \\
 &+ \sum_{j \in S, i \in I_{j\bar{y}_j}} |\langle v_i | w' \rangle|^2 \text{fwsz}_{s_j}(P^{j\bar{y}_j}, x_j) .
 \end{aligned}$$

Equation (2.13) follows using the bound $\text{fwsz}_{s_j}(P^{j\bar{y}_j}, x_j) \leq \sigma(\bar{y}, |w')r_j$ for $j \in S$. \square

Lemma 1 is a key step in the formula-evaluation results in this article and [Rei11]. It is used to track the full witness size for span programs recursively composed in a direct-sum manner along a formula. The proof of Theorem 7 will require the lemma with the weaker bounds $\sigma(y, |w), \sigma(\bar{y}, |w') \leq \max_{j \in S, c \in \{0,1\}} \text{fwsz}_{s_j}(P^{jc})/\text{wsz}_{s_j}(P^{jc})$. Theorem 8 will use only the slightly stronger bounds $\sigma(y, |w) \leq \max_{j \in S} \text{fwsz}_{s_j}(P^{jy_j})/\text{wsz}_{s_j}(P^{jy_j}), \sigma(\bar{y}, |w') \leq \max_{j \in S} \text{fwsz}_{s_j}(P^{j\bar{y}_j})/\text{wsz}_{s_j}(P^{j\bar{y}_j})$. However, the proof of [Rei11, Theorem 1.1] will require the bounds of Eqs. (2.12) and (2.13).

3 Evaluation of Almost-Balanced Formulas

In this section, we will apply the span program framework from [Rei09] to prove Theorem 7. Our algorithm will be given by applying Theorem 9 to a certain span program. Before beginning the proof, though, we will give two necessary lemmas.

Consider a span program P with corresponding weighted graph G_P , from [Rei09, Definition 8.2]. We will need a bound on the operator norm of $\text{abs}(A_{G_{P_v}})$, the entry-wise absolute value of the weighted adjacency matrix $A_{G_{P_v}}$. If P is *canonical* [Rei09, Definition 5.1], then we can indeed obtain such a bound in terms of the witness size of P :

Lemma 2. *Let $s \in (0, \infty)^k$, and let P be a canonical span program computing a function $f : \{0, 1\}^k \rightarrow \{0, 1\}$ with input vectors indexed by the set I . Assume that for each $x \in \{0, 1\}^k$ with $f(x) = 0$, an optimal witness to $f_P(x) = 0$ is $|x$ itself. Then*

$$\| \text{abs}(A_{G_P}) \| \leq 2^k \left(1 + \frac{\text{wsz}_s(P)}{\min_{j \in [k]} s_j} \right) + |I| . \tag{3.1}$$

Proof. Recall from [Rei09, Definition 5.1], that P being in canonical form implies that its target vector is $|t\rangle = \sum_{x:f(x)=0} |x\rangle$, and that the matrix A whose columns are the input vectors of P can be expressed as

$$A = \sum_{i \in I} |v_i\rangle\langle i| = \sum_{j \in [k], x:f(x)=0} |x\rangle\langle j, \bar{x}_j| \otimes \langle v_{xj}| . \quad (3.2)$$

By assumption, for each $x \in f^{-1}(0)$,

$$\sum_{j \in [k]} s_j \| |v_{xj}\rangle \|^2 = \text{wsize}_s(P, x) \leq \text{wsize}_s(P) . \quad (3.3)$$

In particular, letting $\sigma = \min_{j \in [k]} s_j > 0$, we can bound

$$\begin{aligned} \sum_{j \in [k]} \| |v_{xj}\rangle \|^2 &\leq \frac{1}{\sigma} \sum_{j \in [k]} s_j \| |v_{xj}\rangle \|^2 \\ &\leq \frac{\text{wsize}_s(P)}{\sigma} . \end{aligned} \quad (3.4)$$

The rest of the argument follows from the definition of the weighted adjacency matrix A_{G_P} . From [Rei09, Definition 8.1, Prop. 8.8], $\| \text{abs}(A_{G_P}) \| \leq \| \text{abs}(B_{G_P}) \|^2$, where B_{G_P} is the *biadjacency* matrix corresponding to P ,

$$B_{G_P} = \begin{pmatrix} |t\rangle & A \\ 0 & \mathbf{1} \end{pmatrix} , \quad (3.5)$$

and $\mathbf{1}$ is an $|I| \times |I|$ identity matrix. Now bound $\| \text{abs}(B_{G_P}) \|$ by its Frobenius norm:

$$\begin{aligned} \| \text{abs}(A_{G_P}) \| &\leq \| \text{abs}(B_{G_P}) \|^2 \\ &\leq \| \text{abs}(B_{G_P}) \|_F^2 \\ &= \| |t\rangle \|^2 + \sum_{\substack{x:f(x)=0, \\ j \in [k]}} \| |v_{xj}\rangle \|^2 + |I| \\ &\leq 2^k + 2^k \max_{x:f(x)=0} \sum_{j \in [k]} \| |v_{xj}\rangle \|^2 + |I| . \end{aligned} \quad (3.6)$$

Equation (3.1) follows by substituting in Eq. (3.4). \square

An important quantity in the proof of Theorem 7 will be $\sigma_{-}(\varphi)$, from Definition 2. For an almost-balanced formula φ , $\sigma_{-}(\varphi) = O(1)$.

Lemma 3. *Consider a β -balanced formula φ over a gate set \mathcal{S} in which every gate depends on at least two input bits. Then for every vertex v , with children c_1, c_2, \dots, c_k ,*

$$\frac{\text{Adv}^{\pm}(\varphi_v)}{\max_j \text{Adv}^{\pm}(\varphi_{c_j})} \geq \sqrt{1 + \frac{1}{\beta^2}} . \quad (3.7)$$

In particular,

$$\sigma_{-}(\varphi) \leq (2 + \sqrt{2})\beta^2 . \quad (3.8)$$

Proof. Consider a vertex v with corresponding gate $g = g_v : \{0, 1\}^k \rightarrow \{0, 1\}$. By Theorem 2, $\text{Adv}^\pm(\varphi_v) = \text{Adv}^\pm_s(g)$, where $s_j = \text{Adv}^\pm(\varphi_{c_j})$. It is immediate from the definitions that $\text{ADV}_s^\pm(g) \geq \text{Adv}_s(g)$. We will show that $\text{Adv}_s(g) \geq \sqrt{1 + 1/\beta^2}(\max_j s_j)$, using that $\max_j s_j / \min_j s_j \leq \beta$.

Use the weighted minimax formulation of the adversary bound from [HLS07, Theorem 18]:

$$\text{Adv}_s(g) = \min_P \max_{\substack{x, y \in \{0, 1\}^k \\ g(x) \neq g(y)}} \frac{1}{\sum_{j: x_j \neq y_j} \sqrt{p_x(j)p_y(j)/s_j}}, \tag{3.9}$$

where the minimization is over all choices of probability distributions p_x over $[k]$ for $x \in \{0, 1\}^k$.

Since the adversary bound is monotone increasing in each weight, the worst case is when all but one of the weights are equal to $\max_j s_j / \beta$. Since for a scalar c , $\text{Adv}_{cs}(g) = c\text{Adv}_s(g)$, we may scale so that one weight is β and all other weights are 1. Assume that the first weight is $s_1 = \beta$; the other $k - 1$ cases, $s_2 = \beta$ and so on, are symmetrical. Assume also that g depends on the first bit; otherwise $\text{Adv}_s^\pm(g)$ will not depend on s_1 so one of the other cases will be worse. Therefore, there exist inputs $x, y \in \{0, 1\}^k$ that differ only on the first bit, but for which $g(x) \neq g(y)$.

Since the function g depends on at least two input bits, there also exists a third input $z \in \{0, 1\}^k$ with $x_1 = z_1$ but $g(z) = g(y) \neq g(x)$. Indeed, if $g(z) = g(x)$ for every z with $z_1 = x_1$, and if $g(z) = g(y)$ for every z with $z_1 = y_1$, then g depends only on the first bit.

By Eq. (3.9),

$$\text{ADV}_s^\pm(g) \geq \min_{p_x, p_y, p_z} \max \left\{ \frac{1}{\sqrt{p_x(1)p_y(1)/s_1}}, \frac{1}{\sum_{\substack{j \geq 2 \\ x_j \neq z_j}} \sqrt{p_x(j)p_z(j)/s_j}} \right\} \tag{3.10}$$

where the minimization is over only the three probability distributions p_x, p_y and p_z . In the above expression, we may clearly take $p_y(1) = 1$ and $p_y(j) = 0$ for $j \geq 2$. We may also use the Cauchy-Schwarz inequality to bound the second term above, and finally substitute $s_1 = \beta, s_j = 1$ for $j \geq 2$ to obtain,

$$\text{ADV}_s^\pm(g) \geq \min_{p_x} \max \left\{ \frac{\beta}{\sqrt{p_x(1)}}, \frac{1}{\sqrt{\sum_{j \geq 2} p_x(j)}} \right\}. \tag{3.11}$$

The optimum is achieved for $p_x(1) = \beta^2 / (1 + \beta^2)$, so $\text{Adv}_s^\pm(g) \geq \sqrt{1 + \beta^2}$, as claimed.

To derive Eq. (3.8), note that $\beta \geq 1$ necessarily. Then the sum $\sigma_-(\varphi)$ is dominated by the geometric series

$$\sum_{k=0}^{\infty} \left(1 + \frac{1}{\beta^2}\right)^{-k/2}, \tag{3.12}$$

which is at most $(2 + \sqrt{2})\beta^2$, with equality at $\beta = 1$. □

Note that the 1-balanced formulas over $\mathcal{S} = \{\text{OR}_2\}$ satisfy the inequality (3.7) with equality and come arbitrarily close to saturating the inequality (3.8).

With Lemmas 2 and 3 in hand, we are ready to prove Theorem 7.

Proof. (of Theorem 7) First of all, we may assume without loss of generality that every gate in \mathcal{S} depends on at least two input bits. Indeed, if a gate $g : \{0, 1\}^k \rightarrow \{0, 1\}$ depends on no input bits, i.e., is the constant 0 or constant 1 function, then g can be eliminated from any formula over \mathcal{S} without changing the adversary balance condition, since $\text{ADV}_s^\pm(g) = 0$ for all cost vectors $s \in [0, \infty)^k$. If a gate $g : \{0, 1\}^k \rightarrow \{0, 1\}$ depends only on one input bit, say the first bit, then $\text{ADV}_s^\pm(g) = s_1$ for all cost vectors s , and therefore similarly g can be eliminated without affecting the adversary balance condition.

Consider φ an n -variable, β -balanced, read-once formula over the finite gate set \mathcal{S} . Let r be the root of φ . We begin by recursively constructing a span program P_φ that computes φ and has witness size $\text{wsiz}(P_\varphi) = \text{Adv}^\pm(\varphi)$. P_φ is constructed using direct-sum composition of span programs for each node in φ . (Direct-sum composition is also the composition method used in [RŠ08].)

The construction works recursively, starting at the leaves of φ and moving toward the root. Consider an internal vertex v , with children c_1, \dots, c_k . Let $\alpha_j = \text{Adv}^\pm(\varphi_{c_j})$, where φ_{c_j} is the subformula of φ rooted at c_j (Definition 1). In particular, if c_j is a leaf, then $\alpha_j = 1$. Assume that for $j \in [k]$ we have inductively constructed span programs $P_{\varphi_{c_j}}$ and $P_{\varphi_{c_j}}^\dagger$ computing φ_{c_j} and $\neg\varphi_{c_j}$, respectively, with $\text{wsiz}(P_{\varphi_{c_j}}) = \text{wsiz}(P_{\varphi_{c_j}}^\dagger) = \alpha_j$. Apply [Rei09, Theorem 6.1], a generalization of Theorem 4, twice to obtain span programs P_v and P_v^\dagger computing $f_{P_v} = g_v$ and $f_{P_v^\dagger} = \neg g_v$, with $\text{wsiz}_\alpha(P_v) = \text{wsiz}_\alpha(P_v^\dagger) = \text{ADV}_\alpha^\pm(g_v) = \text{Adv}^\pm(\varphi_v)$.

Then let P_{φ_v} and $P_{\varphi_v}^\dagger$ be the direct-sum-composed span programs of P_v and P_v^\dagger , respectively, with the span programs $P_{\varphi_{c_j}}$, $P_{\varphi_{c_j}}^\dagger$ according to the formula φ . By definition of direct-sum composition, the graph $G_{P_{\varphi_v}}$ is built by replacing the input edges of G_{P_v} with the graphs $G_{P_{\varphi_{c_j}}}$ or $G_{P_{\varphi_{c_j}}^\dagger}$; and similarly for $G_{P_{\varphi_v}^\dagger}$. Some examples are given in [Rei09, Appendix B] and in [RŠ08]. By [Rei09, Theorem 4.3], P_{φ_v} (resp. $P_{\varphi_v}^\dagger$) computes φ_v ($\neg\varphi_v$) with $\text{wsiz}(P_{\varphi_v}) = \text{wsiz}(P_{\varphi_v}^\dagger) = \text{Adv}^\pm(\varphi_v)$.

Let $P_\varphi = P_{\varphi_r}$. We wish to apply Theorem 9 to P_φ to obtain a quantum algorithm, but to do so will need some more properties of the span programs P_v and P_v^\dagger . Recall from [Rei09, Theorem 5.2] that each P_v may be assumed to be in canonical form, satisfying in particular that for any input $y \in \{0, 1\}^k$ with $g_v(y) = 0$ an optimal witness is $|y\rangle \in \mathbf{C}^{g_v^{-1}(0)}$ itself. Therefore, Lemma 2 applies, and we obtain

$$\| \text{abs}(A_{G_{P_v}}) \| = 2^k \left(1 + \frac{\text{wsiz}_\alpha(P_v)}{\min_j \alpha_j} \right) + |I|, \quad (3.13)$$

where $|I|$ is the number of input vectors in P_v . Now use

$$\begin{aligned} \frac{\text{wsize}_\alpha(P_v)}{\min_j \alpha_j} &= \frac{\max_j \alpha_j}{\min_j \alpha_j} \frac{\text{Adv}^\pm_\alpha(g_v)}{\max_j \alpha_j} \\ &\leq \beta k, \end{aligned} \tag{3.14}$$

where we have applied Eq. (1.10) and also $\text{ADV}^\pm_\alpha(g_v)/\max_j \alpha_j \leq \text{Adv}^\pm(g_v) \leq k$. Additionally, by [Rei09, Lemma 6.6], we may assume that $|I| \leq 2k^2 2^k$. Thus

$$\|\text{abs}(A_{G_{P_v}})\| = \beta 2^{O(k)}. \tag{3.15}$$

By repeating this argument for the negated function $\neg g_v$ computed by a dual span program P_v^\dagger ([Rei09, Lemma 4.1]), we also have $\|\text{abs}(A_{G_{P_v^\dagger}})\| = \beta 2^{O(k)}$.

A consequence is that

$$\|\text{abs}(A_{G_{P_\varphi}})\| = \beta 2^{O(k_{\max})} \tag{3.16}$$

where k_{\max} is the maximum fan-in of any gate used in φ . Indeed, G_{P_φ} is built by “plugging together” the graphs G_{P_v} and $G_{P_v^\dagger}$ for the different vertices v . Split the graph G_{P_φ} into two pieces, G_0 and G_1 , comprising those subgraphs G_{P_v} and $G_{P_v^\dagger}$ for which the distance of v from r is even or odd, respectively. Then $\|\text{abs}(A_{G_{P_\varphi}})\| \leq \|\text{abs}(A_{G_0})\| + \|\text{abs}(A_{G_1})\|$. Since each G_b is the disconnected union of graphs G_{P_v} and $G_{P_v^\dagger}$, $\|\text{abs}(A_{G_b})\| \leq \max_v \max\{\|\text{abs}(A_{G_{P_v}})\|, \|\text{abs}(A_{G_{P_v^\dagger}})\|\}$.

Let us bound the full witness size of P_φ .

Lemma 4. *Let v be a vertex of φ . Then*

$$\max\{\text{fwsz}(P_{\varphi_v}), \text{fwsz}(P_{\varphi_v}^\dagger)\} \leq \sigma_-(v) \text{Adv}^\pm(\varphi_v). \tag{3.17}$$

Proof. The proof is by induction in the maximum distance from v to a leaf. The base case, that all of v ’s inputs are themselves leaves is by definition of P_v and P_v^\dagger , since then $\sigma_-(v) = 1 + 1/\text{Adv}^\pm(g_v)$.

Let v have children c_1, \dots, c_k . By Lemma 1 with $s = \overline{1}$ and $S = \{j \in [k] : c_j \text{ is not a leaf}\}$,

$$\frac{\text{fwsz}(P_{\varphi_v})}{\text{Adv}^\pm(\varphi_v)} \leq \frac{1}{\text{Adv}^\pm(\varphi_v)} + \max_{j \in S} \max \left\{ \frac{\text{fwsz}(P_{\varphi_{c_j}})}{\text{Adv}^\pm(\varphi_{c_j})}, \frac{\text{fwsz}(P_{\varphi_{c_j}}^\dagger)}{\text{Adv}^\pm(\varphi_{c_j})} \right\}. \tag{3.18}$$

In the case $\varphi_v(x) = 1$, this follows since P_v is strict, so in Eq. (2.12) the sum over I_{free} is zero. In the case $\varphi_v(x) = 0$, this follows since P_v is in canonical form, so in Eq. (2.13), $\|w'\|^2 = 1$.

Now by induction, the right-hand side is at most $\text{Adv}^\pm(\varphi_v)^{-1} + \max_{j \in S} \sigma_-(\varphi_{c_j}) = \sigma_-(v)$. \square

In particular, applying Lemma 4 for the case $v = r$, we find

$$\text{fwsz}(P_\varphi) \leq \sigma_-(\varphi) \text{Adv}^\pm(\varphi) = O(\beta^2 \text{Adv}^\pm(\varphi)) \tag{3.19}$$

since $\sigma_-(\varphi) = O(\beta^2)$ by Lemma 3. Combining Eqs. (3.16) and (3.19) gives

$$\text{fsize}(P_\varphi) \|\text{abs}(A_{G_{P_\varphi}})\| = \beta^3 2^{O(k_{\max})} \text{Adv}^\pm(\varphi) . \quad (3.20)$$

This is $O(\text{Adv}^\pm(\varphi))$; since the gate set \mathcal{S} is fixed and finite, $k_{\max} = O(1)$. Theorem 7 now follows from Theorem 9. \square

Note that the lost constant in the theorem grows cubically in the balance parameter β and exponentially in the maximum fan-in k_{\max} of a gate in \mathcal{S} . It is conceivable that this exponential dependence can be improved.

For future reference, we state separately the bound used above to derive Eq. (3.16).

Lemma 5. *If P_φ is the direct-sum composition along a formula φ of span programs P_v and P_v^\dagger , then*

$$\|\text{abs}(A_{G_P})\| \leq 2 \max_{v \in \varphi} \max\{\|\text{abs}(A_{G_{P_v}})\|, \|\text{abs}(A_{G_{P_v^\dagger}})\|\} . \quad (3.21)$$

If the span programs P_v are monotone, then $\|\text{abs}(A_{G_P})\| \leq 2 \max_v \|\text{abs}(A_{G_{P_v}})\|$.

The claim for monotone span programs follows because then the dual span programs P_v^\dagger are not used in P_φ .

4 Evaluation of Approximately Balanced AND-OR Formulas

The proof of Theorem 8 will again be a consequence of Lemma 1 and Theorem 9.

We will use the following strict, monotone span programs for fan-in-two AND and OR gates:

Definition 7. *For $s_1, s_2 > 0$, define span programs $P_{\text{AND}}(s_1, s_2)$ and $P_{\text{OR}}(s_1, s_2)$ computing AND_2 and OR_2 , $\{0, 1\}^2 \rightarrow \{0, 1\}$, respectively, by*

$$P_{\text{AND}}(s_1, s_2) : |t\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad |v_1\rangle = \begin{pmatrix} \beta_1 \\ 0 \end{pmatrix}, \quad |v_2\rangle = \begin{pmatrix} 0 \\ \beta_2 \end{pmatrix} \quad (4.1)$$

$$P_{\text{OR}}(s_1, s_2) : |t\rangle = \delta, \quad |v_1\rangle = \epsilon_1, \quad |v_2\rangle = \epsilon_2 \quad (4.2)$$

Both span programs have $I_{1,1} = \{1\}$, $I_{2,1} = \{2\}$ and $I_{\text{free}} = I_{1,0} = I_{2,0} = \emptyset$. Here the parameters $\alpha_j, \beta_j, \delta, \epsilon_j$, for $j \in [2]$, are given by

$$\alpha_j = (s_j/s_p)^{1/4} \quad \beta_j = 1 \quad (4.3)$$

$$\delta = 1 \quad \epsilon_j = (s_j/s_p)^{1/4} , \quad (4.4)$$

where $s_p = s_1 + s_2$. Let $\alpha = \sqrt{\alpha_1^2 + \alpha_2^2}$ and $\epsilon = \sqrt{\epsilon_1^2 + \epsilon_2^2}$.

Note that $\alpha, \epsilon \in (1, 2^{1/4}]$. They are largest when $s_1 = s_2$.

Claim. The span programs $P_{\text{AND}}(s_1, s_2)$ and $P_{\text{OR}}(s_1, s_2)$ satisfy:

$$\begin{aligned} \text{wsize}_{(\sqrt{s_1}, \sqrt{s_2})}(P_{\text{AND}}, x) &= \begin{cases} \sqrt{s_p} & \text{if } x \in \{11, 10, 01\} \\ \frac{\sqrt{s_p}}{2} & \text{if } x = 00 \end{cases} \\ \text{wsize}_{(\sqrt{s_1}, \sqrt{s_2})}(P_{\text{OR}}, x) &= \begin{cases} \sqrt{s_p} & \text{if } x \in \{00, 10, 01\} \\ \frac{\sqrt{s_p}}{2} & \text{if } x = 11 \end{cases} \end{aligned} \quad (4.5)$$

Proof. These are calculations using Definition 5 for the witness size. Letting $\sigma = (\sqrt{s_1}, \sqrt{s_2})$, $Q = P_{\text{AND}}(s_1, s_2)$ and $R = P_{\text{OR}}(s_1, s_2)$, we have

$$\text{wsize}_{\sigma}(Q, 11) = \left(\frac{\alpha_1}{\beta_1}\right)^2 \sqrt{s_1} + \left(\frac{\alpha_2}{\beta_2}\right)^2 \sqrt{s_2} = \sqrt{s_p} \quad (4.6)$$

$$\text{wsize}_{\sigma}(Q, 10) = \left(\frac{\beta_2}{\alpha_2}\right)^2 \sqrt{s_2} = \sqrt{s_p} \quad (4.7)$$

$$\text{wsize}_{\sigma}(Q, 00) = \left(\left(\frac{\alpha_1}{\beta_1}\right)^2 \frac{1}{\sqrt{s_1}} + \left(\frac{\alpha_2}{\beta_2}\right)^2 \frac{1}{\sqrt{s_2}} \right)^{-1} = \frac{\sqrt{s_p}}{2} \quad (4.8)$$

$$\text{wsize}_{\sigma}(Q, 01) = \left(\frac{\beta_1}{\alpha_1}\right)^2 \sqrt{s_1} = \sqrt{s_p} \quad (4.9)$$

and

$$\text{wsize}_{\sigma}(R, 11) = \delta^2 \left(\frac{\epsilon_1^2}{\sqrt{s_1}} + \frac{\epsilon_2^2}{\sqrt{s_2}} \right)^{-1} = \frac{\sqrt{s_p}}{2} \quad (4.10)$$

$$\text{wsize}_{\sigma}(R, 10) = \left(\frac{\delta}{\epsilon_1}\right)^2 \sqrt{s_1} = \sqrt{s_p} \quad (4.11)$$

$$\text{wsize}_{\sigma}(R, 00) = \left(\frac{\epsilon_1}{\delta}\right)^2 \sqrt{s_1} + \left(\frac{\epsilon_2}{\delta}\right)^2 \sqrt{s_2} = \sqrt{s_p} \quad (4.12)$$

$$\text{wsize}_{\sigma}(R, 01) = \left(\frac{\delta}{\epsilon_2}\right)^2 \sqrt{s_2} = \sqrt{s_p} . \quad (4.13)$$

It is not a coincidence that $\text{wsize}_{\sigma}(Q, x) = \text{wsize}_{\sigma}(R, \bar{x})$ for all $x \in \{0, 1\}^2$. This can be seen as a consequence of De Morgan's laws and span program duality—see [Rei09, Lemma 4.1]. \square

Proof. (of Theorem 8) Let φ be an AND-OR formula of size n , i.e., on n input bits.

First expand out the formula so that every AND gate and every OR gate has fan-in two. This expansion can be carried out without increasing $\sigma_{-}(\varphi)$ by more than a factor of 10:

Lemma 6 ([ACR⁺10, Lemma 8]) *For any AND-OR formula φ , one can efficiently construct an equivalent AND-OR formula φ' of the same size, such that all gates in φ' have fan-in at most two, and $\sigma_{-}(\varphi') = O(\sigma_{-}(\varphi))$.*

Therefore we may assume that φ is a formula over fan-in-two AND and OR gates.

Now use direct-sum composition to compose the AND and OR gates according to the formula φ , as in the proof of Theorem 7. Since the span programs for AND and OR are monotone, direct-sum composition does not make use of dual span programs computing NAND or NOR. Therefore there is no need to specify these span programs. At a vertex v , set the weights s_1 and s_2 to equal the sizes of v 's two input subformulas. Let P_v be the span program used at vertex v , P_{φ_v} be the span program thus constructed for the subformula φ_v , and P_φ be the span program constructed computing φ . With this choice of weights, it follows from Claim 4 and [Rei09, Theorem 4.3] that $\text{wsize}(P_{\varphi_v}) = \text{Adv}^\pm(\varphi_v) = \text{Adv}(\varphi_v)$.

Notice that for all $s_1, s_2 \in [0, \infty)$, $\|\text{abs}(A_{G_{P_{\text{AND}}}(s_1, s_2)}})\| = O(1)$ and $\|\text{abs}(A_{G_{P_\varphi}})\| = O(1)$. Therefore, by Lemma 5, we obtain that $\|\text{abs}(A_{G_{P_\varphi}})\| = O(1)$.

Thus to apply Theorem 9 we need only bound $\text{fsize}(P_\varphi)$. Lemma 4 does not apply, because for $P_{\text{AND}}(s_1, s_2)$, an optimal witness $|w'\rangle$ to $f_{P_{\text{AND}}}(x) = 0$ might have $\| |w'\rangle \|^2 > 1$, as each $\alpha_j < 1$. (Lemma 4 would apply had we set the parameters to be $\alpha_1 = \alpha_2 = 1$, $\beta_j = (s_p/s_j)^{1/4}$, but then $\|A_{G_{P_{\text{AND}}}}\|$ would not necessarily be $O(1)$.) However, analogous to Lemma 4, we will show:

Lemma 7. *Let v be a vertex of φ . Then*

$$\text{fsize}(P_{\varphi_v}, x) \leq \begin{cases} \sigma_-(v)\text{Adv}(\varphi_v) & \text{if } \varphi_v(x) = 1 \\ 2\sigma_-(v)\text{Adv}(\varphi_v) - 1 & \text{if } \varphi_v(x) = 0 \end{cases} \quad (4.14)$$

Proof. The proof is by induction in the maximum distance from v to a leaf. The base case, that v 's two inputs are themselves leaves is by definition of P_v , since then $\sigma_-(v) = 1 + 1/\sqrt{2}$.

Let v have children c_1 and c_2 . We will use Lemma 1 with $s = \vec{1}$, $S = \{j \in [2] : c_j \text{ is not a leaf}\}$.

If $\varphi_v(x) = 1$, then since P_v is a strict span program, i.e., $I_{\text{free}} = \emptyset$, Eq. (2.12) gives

$$\frac{\text{fsize}(P_{\varphi_v}, x)}{\text{Adv}(\varphi_v)} \leq \frac{1}{\text{Adv}(\varphi_v)} + \max_{j \in S} \frac{\text{fsize}(P_{\varphi_{c_j}})}{\text{Adv}(\varphi_{c_j})}. \quad (4.15)$$

By induction, the right-hand side is at most $1/\text{Adv}(\varphi_v) + \max_j \sigma_-(c_j) = \sigma_-(v)$.

If $\varphi_v(x) = 0$ and g_v is an OR gate, then the unique witness $|w'\rangle$ for P_v has $\| |w'\rangle \| = 1$, from Definition 7. From Eq. (2.13) and the induction hypothesis,

$$\begin{aligned} \frac{\text{fsize}(P_{\varphi_v}, x)}{\text{Adv}^\pm(\varphi_v)} &\leq \frac{1}{\text{Adv}(\varphi_v)} + \max_{j \in S} \left(2\sigma_-(c_j) - \frac{1}{\text{Adv}(\varphi_{c_j})} \right) \\ &< 2\sigma_-(v) - \frac{1}{\text{Adv}(\varphi_v)}, \end{aligned} \quad (4.16)$$

as claimed.

Therefore assume that $\varphi_v(x) = 0$ and g_v is an AND gate. Let s_1 and s_2 be the sizes of the two input subformulas to v , $s_p = s_1 + s_2 = \text{Adv}(\varphi_v)^2$, and assume without loss of generality that $\varphi_{c_1}(x) = 0$. If $\varphi_{c_2}(x) = 0$ as well, then assume without loss of generality that $2\sigma_-(c_1) - \frac{1}{\sqrt{s_1}} \geq 2\sigma_-(c_2) - \frac{1}{\sqrt{s_2}}$, so $\sigma(\bar{y}) \leq 2\sigma_-(c_1) - \frac{1}{\sqrt{s_1}}$. Then the witness $|w'\rangle$ may be taken to be $|w'\rangle = (1/\alpha_1, 0) = ((s_p/s_1)^{1/4}, 0)$. From Eq. (2.13),

$$\begin{aligned} \frac{\text{fwsiz}e(P_{\varphi_v}, x)}{\text{Adv}^\pm(\varphi_v)} &\leq \frac{\sqrt{s_p/s_1}}{\text{Adv}^\pm(\varphi_v)} + \sigma(\bar{y}) \\ &\leq \frac{1}{\sqrt{s_1}} + \left(2\sigma_-(c_1) - \frac{1}{\sqrt{s_1}}\right) \\ &< 2\sigma_-(v) - \frac{1}{\sqrt{s_p}}, \end{aligned} \tag{4.17}$$

as claimed. \square

In particular, applying Lemma 7 for the case $v = r$, we find

$$\text{fwsiz}e(P_\varphi) \leq 2\sigma_-(\varphi)\text{Adv}(\varphi) = 2\sigma_-(\varphi)\sqrt{n}. \tag{4.18}$$

Theorem 8 now follows from Theorem 9. \square

5 Open Problems

In order to begin to relax the balance condition for general formulas, it seems that we need a better understanding of the canonical span programs. For example, can the norm bound Lemma 2 be improved?

Although the two-sided bounded-error quantum query complexity of evaluating formulas is beginning to be understood, the zero-error quantum query complexity [BCWZ99] appears to be more complicated. For example, the exact and zero-error quantum query complexities for OR_n are both n [BBC⁺01]. On the other hand, Ambainis et al. [ACGT10] use the [ACR⁺10] algorithm as a subroutine in the construction of a self-certifying, zero-error quantum algorithm that makes $O(\sqrt{n} \log^2 n)$ queries to evaluate the balanced binary AND-OR formula. It is not known how to relax the balance requirement or extend the gate set.

Can we develop further methods for constructing span programs with small full witness size, norm and maximum degree? A companion paper [Rei11] studies reduced tensor-product span program composition in order to complement the direct-sum composition that we have used here.

The case of formulas over non-boolean gates may be more complicated [Rei09], but is still intriguing.

Acknowledgements. I thank Andrew Landahl and Robert Špalek for helpful discussions. Research supported by NSERC and ARO-DTO.

References

- [ACGT10] Ambainis, A., Childs, A.M., Le Gall, F., Tani, S.: The quantum query complexity of certification. *Quantum Inf. Comput.* **10**, 181–188 (2010) (arXiv:0903.1291[quant-ph])
- [ACR⁺10] Ambainis, A., Childs, A.M., Reichardt, B.W., Špalek, R., Zhang, S.: Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer. *SIAM J. Comput.* **39**(6), 2513–2530 (2010). (Earlier version in FOCS'07)
- [Amb02] Ambainis, A.: Quantum lower bounds by quantum arguments. *J. Comput. Syst. Sci.* **64**, 750–767 (2002). (arXiv:quant-ph/0002066. Earlier version in STOC'00)
- [Amb05] Ambainis, A.: Polynomial degree and lower bounds in quantum complexity: collision and element distinctness with small range. *Theory Comput.* **1**, 37–46 (2005). (arXiv:quant-ph/0305179)
- [Amb06] Ambainis, A.: Polynomial degree vs. quantum query complexity. *J. Comput. Syst. Sci.* **72**(2), 220–238 (2006). (arXiv:quant-ph/0305028. Earlier version in FOCS'03)
- [Amb07] Ambainis, A.: A nearly optimal discrete query quantum algorithm for evaluating NAND formulas (2007). (arXiv:0704.3628[quant-ph])
- [AS04] Aaronson, S., Shi, Y.: Quantum lower bounds for the collision and the element distinctness problem. *J. ACM* **51**(4), 595–605 (2004)
- [BB94] Bonet, M.L., Buss, S.R.: Size-depth tradeoffs for Boolean. *Inf. Process. Lett.* **49**(3), 151–155 (1994)
- [BBBV97] Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.: Strengths and weaknesses of quantum computing. *SIAM J. Comput.* **26**(5), 1510–1523 (1997). (arXiv:quant-ph/9701001)
- [BBC⁺01] Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. *J. ACM* **48**(4), 778–797 (2001). (arXiv:quant-ph/9802049. Earlier version in FOCS'98)
- [BCE91] Bshouty, N.H., Cleve, R., Eberly, W.: Size-depth tradeoffs for algebraic formulae. In: *Proceedings of the 32nd IEEE FOCS*, pp. 334–341 (1991)
- [BCW98] Buhrman, H., Cleve, R., Wigderson, A.: Quantum vs. classical communication and computation. In: *Proceedings of the 30th ACM STOC*, pp. 63–68 (1998) (arXiv:quant-ph/9802040)
- [BCWZ99] Buhrman, H., Cleve, R., de Wolf, R., Zalka, C.: Bounds for small-error and zero-error quantum algorithms. In: *Proceedings of the 40th IEEE FOCS*, pp. 358–368 (1999) (arXiv:cs/9904019[cs.CC])
- [BS04] Barnum, H., Saks, M.: A lower bound on the quantum query complexity of read-once functions. *J. Comput. Syst. Sci.* **69**(2), 244–258 (2004). (arXiv:quant-ph/0201007)
- [BSS03] Barnum, H., Saks, M., Szegedy, M.: Quantum query complexity and semi-definite programming. In: *Proceedings of the 18th IEEE, Complexity*, pp. 179–193 (2003)
- [CNW10] Chiang, C.-F., Nagaj, D., Wocjan, P.: Efficient circuits for quantum walks. *Quantum Inf. Comput.* **10**(5–6), 420–434 (2010) (arXiv:0903.3465 [quant-ph])
- [FGG08] Farhi, E., Goldstone, J., Gutmann, S.: A quantum algorithm for the Hamiltonian NAND tree. *Theory Comput.* **4**, 169–190 (2008). (arXiv:quant-ph/0702144)

- [GR02] Grover, L.K., Rudolph, T.: Creating superpositions that correspond to efficiently integrable probability distributions (2002) (arXiv:quant-ph/0208112)
- [Gro96] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th ACM STOC, pp. 212–219 (1996) (arXiv:quant-ph/9605043)
- [Gro02] Grover, L.K.: Tradeoffs in the quantum search algorithm (2002) (arXiv:quant-ph/0201152)
- [HLŠ05] Høyer, P., Lee, T., Špalek, R.: Tight adversary bounds for composite functions (2005) (arXiv:quant-ph/0509067)
- [HLŠ06] Høyer, P., Lee, T., Špalek, R.: Source codes of semidefinite programs for ADV^\pm . [http://www.ucw.cz/robert/papers/adv/\(2006\)](http://www.ucw.cz/robert/papers/adv/(2006))
- [HLŠ07] Høyer, P., Lee, T., Špalek, R.: Negative weights make adversaries stronger. In: Proceedings of the 39th ACM STOC, pp. 526–535 (2007) (arXiv:quant-ph/0611054)
- [HMW03] Høyer, P., Mosca, M., de Wolf, R.: Quantum search on bounded-error inputs. ICALP 2003. LNCS, vol. 2719, pp. 291–299. Springer, Heidelberg (2003)
- [HNS02] Høyer, P., Neerbek, J., Shi, Y.: Quantum complexities of ordered searching, sorting, and element distinctness. *Algorithmica* **34**(4), 429–448 (2002). (arXiv:quant-ph/0102078. Special issue on Quantum Computation and Cryptography)
- [HNW93] Heiman, Rafi, Newman, Ilan, Wigderson, Avi: On read-once threshold formulae and their randomized decision tree complexity. *Theoret. Comput. Sci.* **107**(1), 63–76 (1993)
- [HW91] Heiman, R., Wigderson, A.: Randomized vs. deterministic decision tree complexity for read-once boolean functions. *Comput. Complex.* **1**(4), 311–329 (1991). (Earlier version in *Structure in Complexity Theory '91*)
- [JKS03] Jayram, T.S., Kumar, R., Sivakumar, D.: Two applications of information complexity. In: Proceedings of the 35th ACM STOC, pp. 673–682 (2003)
- [KSV02] Kitaev, A.Y., Shen, A.H., Vyalı, M.N.: *Classical and Quantum Computation*, vol. 47 of Graduate Studies in Mathematics. American Mathematical Society, Providence (2002)
- [KW93] Karchmer, M., Wigderson, A.: On span programs. In: Proceedings of the 8th IEEE Symposium on Structure in Complexity Theory, pp. 102–111 (1993)
- [LLS06] Laplante, S., Lee, T., Szegedy, M.: The quantum adversary method and classical formula size lower bounds. *Comput. Complex.* **15**, 163–196 (2006). (arXiv:quant-ph/0501057. Earlier version in *Complexity'05*)
- [LM04] Laplante, S., Magniez, F.: Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. In: Proceedings of the 19th IEEE, Complexity, pp. 294–304 (2004) (arXiv:quant-ph/0311189)
- [NC00] Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
- [Rei09] Reichardt, B.W.: Span programs and quantum query complexity: the general adversary bound is nearly tight for every boolean function. Extended abstract in: Proceedings of the 50th IEEE FOCS, pp. 544–551 (2009) (arXiv:0904.2759[quant-ph])
- [Rei11] Reichardt, B.W.: Faster quantum algorithm for evaluating game trees. In: Proceedings of the 22nd ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 546–559 (2011) (arXiv:0907.1623[quant-ph])

- [RŠ08] Reichardt, B.W., Špalek, R.: Span-program-based quantum algorithm for evaluating formulas. In: Proceedings of the 40th ACM STOC, pp. 103–112 (2008) (arXiv:0710.2630[quant-ph])
- [San95] Santha, M.: On the Monte Carlo decision tree complexity of read-once formulae. *Random Struct. Algorithms* **6**(1):75–87 (1995) (Earlier version in Proc. 6th IEEE Structure in Complexity Theory, 1991)
- [Sni85] Snir, M.: Lower bounds on probabilistic linear decision trees. *Theor. Comput. Sci.* **38**, 69–82 (1985)
- [ŠS06] Špalek, R., Szegedy, M.: All quantum adversary methods are equivalent. *Theor. Comput.* **2**(1):1–18 (2006) (arXiv:quant-ph/0409116. Earlier version in ICALP’05)
- [SW86] Saks, M., Wigderson, A.: Probabilistic Boolean decision trees and the complexity of evaluating game trees. In: Proceedings of the 27th IEEE FOCS, pp. 29–38 (1986)
- [Sze04] Szegedy, M.: Quantum speed-up of Markov chain based algorithms. In: Proceedings of the 45th IEEE FOCS, pp. 32–41 (2004)
- [Zha05] Zhang, S.: On the power of Ambainis’s lower bounds. *Theor. Comput. Sci.* **339**(2–3):241–256 (2005) (arXiv:quant-ph/0311060. Earlier version in ICALP’04)

Self-Testing Graph States

Matthew McKague^(✉)

Centre for Quantum Technologies, National University of Singapore,
Singapore, Singapore
matthew.mckague@gmail.com

Abstract. We give a construction for a self-test for any connected graph state. In other words, for each connected graph state we give a set of non-local correlations that can only be achieved (quantumly) by that particular graph state and certain local measurements. The number of correlations considered is small, being linear in the number of vertices in the graph. We also prove robustness for the test.

1 Introduction

Self-testing is a process where a skeptical classical user attempts to verify the operation of a collection of quantum devices without trusting any of them *a priori*. Importantly, we wish to make as few assumptions as possible about the operation of the devices and in particular we do not bound the dimension of the state space for each device. However we do make the necessary assumption that the quantum devices are not allowed to communicate with each other. Despite these severe restrictions on our knowledge it is possible to devise self-tests for a number of different situations.

Self-testing was first introduced by Mayers and Yao [MY04] who described a self-test for a maximally entangled pair of qubits (EPR pair) along with a small set of local measurements. Meanwhile, self-testing of gates was introduced by van Dam et al. [vMMS00] in the scenario of known Hilbert space dimensions. These two results were extended to testing of circuits over a real Hilbert space by Magniez et al. [MMMO06]. Most recently, McKague and Mosca [MM11] reproved the Mayers-Yao result and extended it to allow for testing of a larger set of measurements including measurements over the full complex Hilbert space.

In this paper we use proof techniques developed in [MM11] to define self-tests for the graph state for any connected graph. This family of self-tests is efficient in the number of measurement settings, requiring only two or three measurement settings on each vertex, depending on the graph. As well the total number of correlations tested is small, only one per vertex plus an additional 3 at most. We also prove that the self-tests are robust.

1.1 Graph States and Notation

A graph G is composed of two sets: a set V of *vertices*, and a set $E \subset V \times V$ of *edges*. For our purposes we suppose that $(v, v) \notin E$ and $(v, u) \in E$ whenever

$(u, v) \in E$. Two vertices u, v are said to be *adjacent* if $(u, v) \in E$. A cycle is a sequence of vertices in which each vertex occurs at most once, each vertex in the sequence is adjacent to the next vertex in the sequence, and the last vertex is adjacent to the first. A *subgraph* G' of G is a graph (E', V') with $E' \subseteq E, V' \subseteq V$. An *induced subgraph* is a subgraph in which $E' = \{(u, v) \in E \mid u, v \in V'\}$, so the subgraph contains all edges between vertices of V' in the original graph. The *neighbours* $N_v \subseteq V$ of a vertex v are the vertices to which v is connected with an edge, i.e. $N_v = \{u \in V \mid (u, v) \in E\}$. A *bipartite* graph is a graph in which the set of vertices may be partitioned into two sets S and T , each of which has no edges within it. So the induced subgraphs on S and T have no edges. An important property of bipartite graphs is that they are exactly the graphs which contain no cycles with an odd number of vertices. A graph is *connected* if for each pair of vertices u, v there is a sequence of adjacent vertices beginning with u and ending in v . For more detail regarding graph theory see Diestel [Die10].

A graph state consists of a set of qubits indexed by the set of vertices V , each prepared in the state $|+\rangle_v = \frac{1}{\sqrt{2}}(|0\rangle_v + |1\rangle_v)$, followed by $(CTRL - Z)_{uv}$ operations for each adjacent $u, v \in V$. If the graph is not connected then the graph state will be a product state of graph states on the separate components. Hence connected graphs form the interesting case.

Graph states are also characterized by their stabilizer group. Let the operators X_v and Z_v be the Pauli operators X and Z applied to qubit v , tensor product with I on all other qubits. If P is a Pauli and $S \subseteq V$ then

$$P^S = \prod_{v \in S} P_v. \quad (1)$$

The stabilizer group for a graph state on the graph $G = (V, E)$ is generated by

$$S_v = \{X_v Z^{N_v} \mid v \in V\}. \quad (2)$$

That is, for each vertex v there is a stabilizer generator with X operating on v and Z operating on each of v 's neighbours. Note that there are n such generators, they pairwise commute and are independent. Hence there is exactly one state with this stabilizer group. That is to say, the graph state $|\psi\rangle$ is the unique state for which $S_v |\psi\rangle = |\psi\rangle$ for each $v \in V$.

As one additional piece of notation, we will frequently need to deal with products of stabilizers on a subset of vertices. For this case we define

$$Z^{N(S)} = \prod_{v \in S} Z^{N_v} \quad (3)$$

where the factor Z_v appears in $Z^{N(S)}$ if v has an *odd* number of neighbours in S .

1.2 Self-Testing Definitions

Consider the following *black-box* scenario: we are given a set of devices, each with a knob labeled with a number of settings, a pair of lights labeled ± 1 , and a

button. After we select a setting and push the button one of the lights turns on. We are told that the devices jointly share a state which is measured, according to the knob setting, in a specified basis. Our goal is to determine if the black-boxes are operating according to their specification using only the external controls of the boxes. Additionally we may isolate the boxes to ensure that they do not communicate.

We begin with a *reference experiment* consisting of an n -partite system in the state $|\psi\rangle$ together with local measurement observables $M_{j,m}$ on subsystem j with measurement setting $m \in \{0, 1, \dots, k_j\}$. The measurement setting $m = 0$ corresponds to no measurement, which we may represent with the identity. The reference experiment represents the specification for how the black-boxes supposedly operate. In particular, we assume that the state and observables are known.

In addition, we have a *physical experiment* consisting of an n -partite physical system in the state¹ $|\psi'\rangle$ together with local measurement observables $M'_{j,m}$ on subsystem j , with $m \in \{0, 1, \dots, k_j\}$. Again we may take $M'_{j,0} = I$ indicating that we do not measure the subsystem. We place no bound on the dimension of the Hilbert space of each subsystem, but assume that it is finite. The physical experiment represents how the black-boxes *actually* operate.

If a physical and reference experiment have the same number of subsystems and the same number of measurements on each subsystem, then we say that they are *compatible*. Note that we will always deal with the case of two-outcome measurements, so that all observables have eigenvalues ± 1 . In principle, though, the definitions can be extended to other types of measurements.

To be more specific about our task, we introduce two notions, *simulation* and *equivalence*.

Definition 1. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment simulates the reference experiment if for each measurement setting $m = (m_1, \dots, m_n)$, $m_j \in \{0, \dots, k_j\}$ we have*

$$\langle \psi' | \bigotimes_{j=1}^n M'_{j,m_j} | \psi' \rangle = \langle \psi | \bigotimes_{j=1}^n M_{j,m_j} | \psi \rangle. \quad (4)$$

For our purposes it will be sufficient to consider only a subset of possible measurement settings. In this case we include the measurement settings of interest in our description of the reference experiment.

Definition 2. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment is equivalent to the reference experiment if there exists a local isometry*

$$\Phi = \Phi_1 \otimes \dots \otimes \Phi_n \quad (5)$$

¹ We consider only pure states, but since the Hilbert space of the physical system has unbounded dimension we may easily add a purification to mixed states.

and a state $|junk\rangle$ such that, for each j , and $m \in \{1, \dots, k_j\}$

$$\Phi(|\psi'\rangle) = |junk\rangle \otimes |\psi\rangle \quad (6)$$

$$\Phi(M'_{j,m} |\psi'\rangle) = |junk\rangle \otimes M_{j,m} |\psi\rangle \quad (7)$$

where $|junk\rangle$ is in the same Hilbert space as $|\psi'\rangle$.

When describing any physical system we must first fix a reference frame, and decide which components to describe and which to leave out. Thus we may take a description and apply local changes of basis, or add ancillas and arrive at another, perfectly acceptable, description of the system. These two operations are invisible from the perspective of classical interactions with devices so we can never rule them out. This motivates our definition of equivalence, which takes such ambiguities in quantum descriptions into account.

Throughout the remainder of this paper we will use primed ($|\psi'\rangle$, X' , S'_v etc.) to denote physical measurements and states and unprimed for reference measurements and states. Note that $S'_v = X'_v \otimes Z^{N(v)}$ and other derived physical measurements are defined in terms of the local physical measurements. Also, although we use the letters X and Z for the physical measurements, these need not be Pauli matrices, and we assume nothing about them other than what we mention explicitly.

1.3 Main Results

A self-testing theorem specifies a particular reference experiment and states that if a physical experiment simulates the reference experiment, then it is equivalent to it. That is to say, for a particular experiment *simulation implies equivalence*. Our main result is to show that this is the case for the following two reference experiments.

Definition 3 (Reference experiment 1: connected graph with an odd induced cycle). Let $G = (V, E)$ be a connected graph containing an odd induced cycle $C = (V', E')$. Let $|\psi\rangle$ be the corresponding graph state with stabilizers S_v , $v \in V$. The reference experiment consists of the state $|\psi\rangle$, the stabilizer measurements S_v and the measurement $X^{V'} Z^{N(V')}$.

It is easy to show that a graph which contains an odd cycle also contains an induced cycle. Thus reference experiment 1 is applicable to all connected non-bipartite graphs.

Definition 4 (Reference experiment 2: connected graph). Let $G = (V, E)$ be a connected graph with at least two vertices. Let $|\psi\rangle$ be the corresponding graph state with stabilizers S_v , $v \in V$. Choose a fixed edge $(u, v) \in E$ and define

$$D_u = \frac{1}{\sqrt{2}} (X_u + Z_u) \quad (8)$$

The reference experiment consists of the state $|\psi\rangle$, the stabilizer measurements S_v and the measurements

$$Z'_u Z'^{N_u} \quad (9)$$

$$D_u Z^{N_u} \quad (10)$$

$$D_u X_v Z^{N_v \setminus \{u\}} \quad (11)$$

In Appendix C we show that for a bipartite graph all measurements using X and Z alone can be simulated using a classical hidden variable model, hence our addition of the D measurements.

Theorem 1. *If a physical experiment is compatible with reference experiment 1 (2), and simulates it, then the physical experiment is equivalent to reference experiment 1(2).*

2 Proof of Main Result

The proof consists of three sections. First we determine the expected values for the measurements in the reference experiment. Next we show that if the physical experiment simulates the reference experiment then the X' and Z' operators anti-commute. Finally we construct the local isometry and use the anti-commuting property of the X' and Z' operators to show equivalence.

2.1 Probability Distribution from Graph States

We first derive the probability distributions that arise from a graph state with trusted measurements. This establishes the conditions that a physical experiment must meet in order to simulate the reference experiment.

Clearly, the stabilizer measurements all satisfy

$$\langle \psi | S_v | \psi \rangle = 1. \quad (12)$$

For reference experiment 1, we need one additional measurement.

Lemma 1. *Let $G = (V, E)$ be a graph and let $|\psi\rangle$ be the corresponding graph state. Let $V' \subseteq V$ and let $G' = (V', E')$ be the induced subgraph on V' . If each $v \in V'$ has even degree then*

$$(-1)^{|E'|} X^{V'} Z^{N(V')} |\psi\rangle = |\psi\rangle \quad (13)$$

Proof. Consider the product

$$\left(\prod_{v \in V'} S_v \right) |\psi\rangle \quad (14)$$

First note that there will be an X_v factor for each $v \in V'$. As well, there will be a Z_u factor for each $v \in V'$ adjacent to u . Canceling pairs we see that there will be an overall Z_u factor exactly when there are an odd number of neighbours of u in V' . Hence the Z factor will be $Z^{N(V')}$. We only need to determine the sign. Note that the $Z_u, u \notin V'$ factor all commute so we need not consider them any more.

The order of multiplication in Eq. (14) does not matter since the stabilizers all commute. For convenience, then, we may write the product as the product of the rows of a matrix with each column corresponding to a $v \in V'$ and each row a stabilizer. We choose the order of the rows so that the X s appear along the diagonal². For a 5-cycle, for instance, we have

$$\begin{array}{ccccc} X & Z & I & I & Z \\ Z & X & Z & I & I \\ I & Z & X & Z & I \\ I & I & Z & X & Z \\ Z & I & I & Z & X \end{array} \quad (15)$$

The factor on each vertex equals the product of the entries in the corresponding column. In each column there is one X and one Z for each neighbour. The factor will be either $\pm XZ$ or $\pm X$, depending on whether there is an odd or even number of Z s. The sign depends on the number of Z s above the X , since we must use the fact that $XZ = -ZX$ once for each such Z . Combining the signs from all vertices, there is a -1 factor for each Z above the diagonal, and hence one for each edge in G' . The overall sign, then, is $(-1)^{|E'|}$.

For reference experiment 1 we consider an odd cycle, and hence we obtain

$$\langle \psi | X^{V'} Z^{N(V')} | \psi \rangle = -1. \quad (16)$$

Reference experiment 2 has three measurements other than the stabilizer. First we have $Z_u Z^{N_u}$. This is just S_u with X_u replaced by Z_u . Since X and Z anti-commute we have

$$\langle \psi | Z_u Z^{N_u} | \psi \rangle = 0. \quad (17)$$

From this, and linearity, we obtain

$$\langle \psi | D_u Z^{N_u} | \psi \rangle = \frac{1}{\sqrt{2}}. \quad (18)$$

Finally, the operator $D_u X_v Z^{N_v \setminus \{u\}}$ is a linear combination of S_v and S_v with Z_u replaced with X_u . As above, then, we find

$$\langle \psi | D_u X_v Z^{N_v \setminus \{u\}} | \psi \rangle = \frac{1}{\sqrt{2}}. \quad (19)$$

² The matrix may be constructed by taking the adjacency matrix of G' , which has a 1 in the u, v position when $(u, v) \in E'$, replacing the diagonal with X s, the 0s with I s and the 1s with Z .

2.2 Statistics Imply Anti-commuting Observables

We now suppose that the physical experiment simulates either reference experiment 1 or 2 and show that this implies that the X' and Z' measurements on each vertex anti-commute (on the support of $|\psi\rangle$).

First, note that $\langle \psi' | S'_v | \psi' \rangle = 1$ implies $S'_v | \psi' \rangle = |\psi'\rangle$, and similarly for other measurements. This allows us to immediately drop probabilities and deal with states directly.

As a first step towards our goal, we prove a type of induction lemma which says that if the X' and Z' observables anti-commute for some vertex, then the same is true for an adjacent vertex. Thus we need only show anti-commuting observables on one vertex, and apply the lemma repeatedly along paths to all other vertices (since G is connected.)

Lemma 2. *Given a graph G with $(u, v) \in E$. If observables X'_v, Z'_v, X'_u, Z'_u , and $\{Z'_w | w \in N_u \cup N_v\}$ and state $|\psi'\rangle$ satisfy*

$$S'_u | \psi' \rangle = S'_v | \psi' \rangle = |\psi'\rangle \quad (20)$$

$$(X'Z')_v | \psi' \rangle = -(Z'X')_v | \psi' \rangle \quad (21)$$

then

$$(X'Z')_u | \psi' \rangle = -(Z'X')_u | \psi' \rangle \quad (22)$$

Proof. From the fact that $(u, v) \in E$ we obtain

$$(Z'X')_u | \psi' \rangle = (Z'X')_u S'_u S'_v S'_u S'_v | \psi' \rangle \quad (23)$$

$$= (Z'X')_u X'_u Z'_v X'_v Z'_u X'_u Z'_v X'_v Z'_u | \psi' \rangle \quad (24)$$

$$= (X'Z')_u (Z'X')_v (Z'X')_v | \psi' \rangle \quad (25)$$

$$= -(X'Z')_u (Z'X')_v (X'Z')_v | \psi' \rangle \quad (26)$$

$$= -(X'Z')_u | \psi' \rangle \quad (27)$$

For reference experiment 1 we show that the observables X' and Z' anti-commute for each vertex in the induced odd cycle.

Lemma 3. *Let $G = (E, V)$ be a connected graph and let $C = (E', V')$ be an induced odd cycle of G and let $u \in V'$. If observables X'_u, Z'_u for $u \in V'$, $\{Z'_w | w \text{ has a neighbour in } C\}$ and state $|\psi'\rangle$ satisfy*

$$S'_u | \psi' \rangle = |\psi'\rangle \quad (28)$$

$$-X'^{V'} Z'^{N(V')} | \psi' \rangle = |\psi'\rangle \quad (29)$$

Then $(X'Z')_u | \psi' \rangle = -(Z'X')_u | \psi' \rangle$ for each $u \in V'$.

Proof. Number the vertices in the cycle 1 through k so 1 is adjacent to 2, etc.. Without loss of generality we may assume that u is vertex 1. We next consider the following state:

$$-X'^{V'} Z'^{N(V')} \prod_{j=1}^{\frac{k-1}{2}} S'_{2j} \prod_{j=1}^{\frac{k-1}{2}} S'_{2j-1} |\psi'\rangle = |\psi'\rangle \quad (30)$$

Note that the factor $Z'^{N(V')}$ is cancelled by Z operations arising from the products of the S'_v . We may write the product as the product of the rows of the following matrix, where column j corresponds to vertex j in the cycle:

$$\begin{array}{cccccccc} -X' & X' & X' & X' & X' & \dots & X' & X' & X' \\ Z' & X' & Z' & I & I & \dots & I & I & I \\ I & I & Z' & X' & Z' & \dots & I & I & I \\ & & & & & \vdots & & & \\ I & I & I & I & I & \dots & Z' & X' & Z' \\ X' & Z' & I & I & I & \dots & I & I & Z' \\ I & Z' & X' & Z' & I & \dots & I & I & I \\ I & I & I & Z' & X' & \dots & I & I & I \\ & & & & & \vdots & & & \\ Z' & I & I & I & I & \dots & I & Z' & X' \end{array} \quad (31)$$

In each column there are two X' operators and two Z' operators. Also, their arrangement is such that, for every column except the first, the two X' operators are next to one another, so they cancel directly, and similarly for the Z' operators. Hence

$$-(X'Z')_u (X'Z')_u |\psi'\rangle = |\psi'\rangle \quad (32)$$

The desired result follows immediately.

For reference experiment 2, we have one additional measurement on a particular vertex u . We use this extra measurement to establish that the X' and Z' measurements on u anti-commute.

Lemma 4. *Let $G = (V, E)$ be a connected graph with $(u, v) \in E$. If observables $D'_u, X'_v, Z'_v, X'_u, Z'_u, \{Z'_w | w \in N_u \cup N_v\}$ and state $|\psi'\rangle$ satisfy*

$$S'_u |\psi'\rangle = S'_v |\psi'\rangle = |\psi'\rangle \quad (33)$$

$$\langle \psi' | Z'_u Z'^{N_u} | \psi' \rangle = 0 \quad (34)$$

$$\langle \psi' | D'_u Z'^{N_u} | \psi' \rangle = \frac{1}{\sqrt{2}} \quad (35)$$

$$\langle \psi' | D'_u X'_v Z'^{N_v \setminus u} | \psi' \rangle = \frac{1}{\sqrt{2}} \quad (36)$$

then $-(X'Z')_u |\psi'\rangle = (Z'X')_u |\psi'\rangle$

Proof. Since $\langle \psi' | X'_u Z'^{N_u} | \psi \rangle = 1$ we have $X'_u | \psi' \rangle = Z'^{N_u} | \psi \rangle$. Similarly, $Z'_u | \psi' \rangle = X'_v Z'^{N_v \setminus u} | \psi' \rangle$. Along with $\langle \psi' | Z'_u Z'^{N_u} | \psi' \rangle = 0$ we find that $X'_u | \psi' \rangle$ is orthogonal to $Z'_u | \psi' \rangle$. We also obtain $\langle \psi' | D'_u Z'_u | \psi' \rangle = \frac{1}{\sqrt{2}}$ and $\langle \psi' | D'_u X'_u | \psi' \rangle = \frac{1}{\sqrt{2}}$. Since $D'_u | \psi' \rangle$ has norm 1, we find

$$D'_u | \psi' \rangle = \frac{1}{\sqrt{2}} X'_u | \psi' \rangle + Z'_u \frac{1}{\sqrt{2}} | \psi' \rangle \quad (37)$$

Further, since $(D'_u)^2 = I = (Z'_u)^2 = (X'_u)^2$, and

$$| \psi' \rangle = (D'_u)^2 | \psi' \rangle \quad (38)$$

$$= \frac{1}{\sqrt{2}} D'_u \left(Z'^{N_u} + X'_v Z'^{N_v \setminus u} \right) | \psi' \rangle \quad (39)$$

$$= \frac{1}{2} \left(Z'^{N_u} + X'_v Z'^{N_v \setminus u} \right) (X'_u + Z'_u) | \psi' \rangle \quad (40)$$

$$= \frac{1}{2} (2I + (X'Z')_u + (Z'X')_u) | \psi' \rangle \quad (41)$$

In order for this to be true, we must have

$$(X'Z')_u | \psi' \rangle = -(Z'X')_u | \psi' \rangle. \quad (42)$$

We conclude with a technical lemma that allows us to exchange X'_v operations for Z'_v operations.

Lemma 5. *Let $G = (V, E)$ be a connected graph and let X'_v, Z'_v for $v \in V$ and $| \psi' \rangle$ (and D_u for some $u \in V$) be a physical experiment that simulates reference test 1 (or 2). Let $G' = (V', E')$ be an induced subgraph of G . Then*

$$(-1)^{|E'|} X'^{V'} | \psi' \rangle = Z'^{N(V')} | \psi' \rangle \quad (43)$$

Proof. We use the previous lemmas to conclude that $X'_v Z'_v | \psi' \rangle = -Z'_v X'_v | \psi' \rangle$ for each v . Then we repeat the argument used in the proof of Lemma 1. Essentially, we look at the product

$$\prod_v S'_v | \psi' \rangle. \quad (44)$$

Writing this product out as a the product of rows of a symmetric matrix with X' s along the diagonal, we see that in order to get all the X' s together we must use the anti-commuting relation once for each Z' above the diagonal. Since there is one Z' above the diagonal for each edge, we obtain the factor $(-1)^{|E'|}$.

2.3 Constructing the Isometry

The local isometry Φ that we use to show equivalence between the physical experiment and the reference experiment is the tensor product of isometries Φ_v for various $v \in V$, is in the circuit shown in Fig. 1.

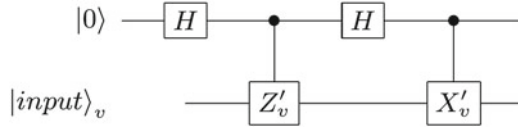


Fig. 1. Circuit for Φ_v

The circuit is based on the argument used by Mayers and Yao in their original EPR test. It may be seen as a type of SWAP gate, decomposed into three CNOT gates. Here the first CNOT gate is omitted since the ancilla is always initialized in the state $|0\rangle$. The Hadamards and Controlled Z operation replace a CNOT targeted on the ancilla. With these points in mind, we see that when Z'_v and X'_v are indeed qubit Pauli operators the circuit defines a SWAP operation.

We will now calculate the result of Φ applied to $|\psi'\rangle$.

$$\Phi(|\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} X_v'^{x_v} (I + (-1)^{x_v} Z'_v) |\psi'\rangle |x\rangle \quad (45)$$

with $x = (x_v)_{v \in V} \in \{0, 1\}^{|V|}$. Applying the anti-commutation relation, this simplifies to

$$\Phi(|\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} (I + Z'_v) X_v'^{x_v} |\psi'\rangle |x\rangle. \quad (46)$$

Using Lemma 5 and the fact that $(I + Z'_v)Z'_v = I + Z'_v$ we finally find

$$\Phi(|\psi'\rangle) = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{e(x)} |x\rangle \right) \quad (47)$$

where $e(x)$ is the number of edges in the induced subgraph on the set $V_x = \{v \in V | x_v = 1\}$.

Set $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{e(x)} |x\rangle$. Consider $S_v |x\rangle$ for some x . This will be $\pm |x \oplus 1_v\rangle$ where 1_v is the binary vector with 1 in position v and 0 everywhere else. The sign may be computed as follows: for each Z_u component of S_v , if $x_u = 1$ a -1 factor will be introduced. This happens when $(u, v) \in E$ and u is in V_x . We may see this as either removing or adding the vertex v and adding a -1 factor for each edge between v and another vertex in V_x . Thus $S_v (-1)^{e(x)} |x\rangle = (-1)^{e(x \oplus 1_v)} |x \oplus 1_v\rangle$. In other words, this exactly produces the correct sign on each $|x\rangle$ so that $S_v |\phi\rangle = |\phi\rangle$ and in fact $|\phi\rangle = |\psi\rangle$.

Now consider $\Phi(X'_v |\psi'\rangle)$ for some v . After anti-commuting the X' operations we have

$$\Phi(X'_v |\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} (I + Z'_v) X_v'^{x_v} X'_v |\psi'\rangle |x\rangle. \quad (48)$$

In this equation, we may simply replace $X_v'^{x_v} X'_v$ with $X_v'^{x_v \oplus 1_u}$, where 1_u is the vector with 0s everywhere, except position u . After applying Lemma 5 we arrive at

$$\Phi(X'_u | \psi') = \left(\frac{1}{2^n} \bigotimes_{v \in V} (I + Z'_v) | \psi' \rangle \right) \sum_x (-1)^{\epsilon(x \oplus 1_u)} | x \rangle. \quad (49)$$

A change of variable, $x \mapsto x \oplus 1_u$, and the fact that $X_u | x \rangle = | x \oplus 1_u \rangle$ gives the final result,

$$\Phi(X'_v | \psi') = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) | \psi' \rangle \right) X_v | \psi \rangle. \quad (50)$$

A similar analysis shows that

$$\Phi(Z'_v | \psi') = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) | \psi' \rangle \right) Z_v | \psi \rangle. \quad (51)$$

Recall from the proof of Lemma 4 that $D'_v | \psi' \rangle$ may be written as $D'_v | \psi' \rangle = \frac{1}{\sqrt{2}} (X'_v + Z'_v) | \psi' \rangle$. By linearity, then

$$\Phi(D'_v | \psi') = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) | \psi' \rangle \right) D_v | \psi \rangle. \quad (52)$$

This concludes the proof of theorem 1.

3 Robustness

In this section we will show that the main theorems are both robust. First, we modify the definitions of simulation and equivalence to allow for small deviations from the reference experiment

Definition 5. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment ϵ -simulates the reference experiment if for each measurement setting $m = (m_2, \dots, m_n)$, $m_j \in \{0, \dots, k_j\}$ we have*

$$\left| \langle \psi' | \bigotimes_{j=1}^n M'_{j,m_j} | \psi' \rangle - \langle \psi | \bigotimes_{j=1}^n M_{j,m_j} | \psi \rangle \right| \leq \epsilon. \quad (53)$$

Definition 6. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment is δ -equivalent to the reference experiment if there exists a local isometry*

$$\Phi = \Phi_2 \otimes \dots \otimes \Phi_n \quad (54)$$

and a state $|junk\rangle$ such that, for each j , and $m \in \{1, \dots, k_j\}$

$$\|\Phi(|\psi'\rangle) - |junk\rangle \otimes |\psi\rangle\|_2 \leq \delta \quad (55)$$

$$\|\Phi(M'_{j,m} | \psi') - |junk\rangle \otimes M_{j,m} | \psi \rangle\|_2 \leq \delta \quad (56)$$

where $|junk\rangle$ is in the same Hilbert space as $|\psi'\rangle$.

Using these definitions we are able to prove the following theorem.

Theorem 2. *Let a graph G be given with $|V| = n$. If a compatible physical experiment ϵ -simulates reference experiment 1 (2) then it is δ -equivalent to it with*

$$\delta = (5n^2 + 11n + 4)n2^{n-2}\sqrt{2\epsilon}(\delta = n2^{n-2} \left((n+2)26\epsilon^{\frac{1}{4}} + (4n^2 + 10n)\sqrt{2\epsilon} \right)).$$

The proof simply follows that of the exact case, applying estimations at each step. Proofs for the two reference experiments are included in Appendix A and B. Note that δ may be improved for particular graphs or by adding additional measurements, such as tests for more odd cycles, or more D type measurements.

4 Discussion

4.1 Estimating Expected Values

The main results concern expected values, rather than experimental outcomes. So in order to make use of these results in any practical implementation we must estimate the expected values using data collected from experimental outcomes. The obvious approach of sampling the devices many times and applying a Chernoff bound is problematic. In particular, we do not wish to assume that separate uses of a device are independent and identically distributed since these assumptions would be untestable and likely false in many practical experiments.

One approach to this problem is that used by Pironio et al. in [PAM⁺10]. There the authors construct a martingale, which is a sequence of random variables with certain properties. In particular, the random variables need not be independent. This allows them to use Azuma's inequality, which gives good bounds for martingales on how far away a sample may lie from the expected value without relying on independence assumptions. A similar approach is viable here and a preliminary analysis suggests that good bounds are achievable.

4.2 Graph State Computation

Graph states are particularly interesting for their role in measurement based quantum computation (MBQC, [RB01]). In this paradigm a graph state is measured, vertex by vertex, in particular bases. Each measurement may be interpreted as performing a unitary on a logical qubit. The composition of these unitaries performs a logical circuit on the logical qubits.

A natural question to ask is whether a self-tested graph state could be used for MBQC to allow for self-tested computation. Unfortunately MBQC depends on measurements in the X - Y plane and the measurements tested here are all in the X - Z plane. However, the techniques used in [MM11] could easily be adapted to allow testing of X - Y plane measurements which would then allow self-tested MBQC. In fact, in the exact case the techniques used in [MM11] can be used with minimal changes. A preliminary analysis of robustness suggests that the errors scale similarly to that of Lemma 4 here.

Acknowledgments. This work is funded by the Centre for Quantum Technologies, which is funded by the Singapore Ministry of Education and the Singapore National Research Foundation.

A Proof of Robustness for Reference Experiment 1

First we note that if $\langle \psi | M | \psi \rangle \geq 1 - \epsilon$ then

$$\| |\psi\rangle - M |\psi\rangle \|_2 \leq \sqrt{2\epsilon}. \quad (57)$$

Next, suppose that we have $\| |\psi\rangle - M |\psi\rangle \|_2 \leq \alpha$ and $\| |\psi\rangle - N |\psi\rangle \|_2 \leq \beta$. Using the triangle inequality and the fact that $\|M\|_\infty = 1$ we have

$$\| |\psi\rangle - MN |\psi\rangle \|_2 \leq \alpha + \beta. \quad (58)$$

The remainder of the proof will use these estimates repeatedly, along with the triangle inequality. We need only count the number of operators multiplied together.

First, for Lemma 3 let c be the size of the induced cycle. We multiply $c + 1$ operators together. Thus we conclude that for a vertex u in the induced cycle

$$\| |X'_u Z'_u |\psi'\rangle + Z'_u X'_u |\psi'\rangle \|_2 \leq (c + 1)\sqrt{2\epsilon}. \quad (59)$$

Next, for Lemma 2 we multiply four operators, then invoke the anti-commuting property on one of the vertices. This gives

$$\| |X'_u Z'_u |\psi'\rangle + Z'_u X'_u |\psi'\rangle \|_2 \leq 4\sqrt{2\epsilon} + \beta \quad (60)$$

where β is $\| |X'_v Z'_v |\psi'\rangle + Z'_v X'_v |\psi'\rangle \|_2$, v being neighbouring vertex. We may apply Lemma 2 along paths from vertices in the induced cycle in G . Let l be the length (number of edges) of the longest path. Then for any vertex u we find, at worst,

$$\| |X'_u Z'_u |\psi'\rangle + Z'_u X'_u |\psi'\rangle \|_2 \leq (4l + c + 1)\sqrt{2\epsilon}. \quad (61)$$

Lastly, for Lemma 5, we multiply $|V'|$ operators, and apply the anti-commuting relation $|E'|$ times. Thus

$$\left\| \left((-1)^{|E'|} |X'^{V'} |\psi'\rangle - Z'^{N(V')} |\psi'\rangle \right) \right\|_2 \leq (|V'| + (4l + c + 1)|E'|)\sqrt{2\epsilon}. \quad (62)$$

We are now ready to analyze the proof of the main theorem for reference experiment 1. To arrive at Eq. 46 we apply the anti-commutation relation. This happens once for each 1 appearing in x , for each possible x , for a total of $n2^{n-1}$ times. We may find this by pairing values x and $x \oplus 111\dots 1$. There are 2^{n-1} such pairs and each pair contains n 1s all together. We find

$$\left\| \Phi(|\psi'\rangle) - \frac{1}{2^n} \sum_x \bigotimes_{v \in V} (I + Z'_v) X'^{x_v} |\psi'\rangle |x\rangle \right\| \leq n2^{n-1}(4l + c + 1)\sqrt{2\epsilon}. \quad (63)$$

For Eq. 47 we use Lemma 5, once for each possible value of x . Again, the estimate depends on the number of 1s in x , summed over all possible x s. As well, it depends on the number of edges in the induced subgraph. An edge (u, v) will be counted only when $x_u = x_v = 1$. This occurs for $1/4$ of all x s. Summed over all possible x s and edges, then, the number of times edges are counted is $2^{n-2}|E|$. This gives our final estimate:

$$\left\| \Phi(|\psi'\rangle) - \left(\frac{1}{2^n} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) \sum_x (-1)^{e(x)} |x\rangle \right\|_2 \quad (64)$$

$$\leq (n2^{n-1}(4l + c + 1) + n2^{n-1} + (4l + c + 1)2^{n-2}|E|) \sqrt{2\epsilon} \quad (65)$$

$$= 2^{n-2} ((4l + c + 1)(2n + |E|) + 2n) \sqrt{2\epsilon} \quad (66)$$

where $e(x)$ is the number of edges in the induced subgraph on the set $V_x = \{v \in V | x_v = 1\}$.

Note that when calculating $\Phi(X'_u |\psi'\rangle)$ etc. we did not use any more estimations, we simply rearrange when Lemma 5 is applied. Thus the same robustness applies. For $\Phi(Z'_v |\psi'\rangle)$ we use $(I + (-1)^{x_v} Z'_v) Z'_v = -(I + (-1)^{x_v} Z'_v)$, which does not involve an estimation, so again the same robustness applies.

As a last estimation, we note that l and c cannot be larger than n , and $|E| \leq n^2$. We may thus set $\delta = (5n^2 + 11n + 4)n2^{n-2}\sqrt{2\epsilon}$.

Note that we may make much better estimates if some properties of the graph are known. For example, if every vertex lies in a triangle and the max degree is 6, as in the case of a lattice of triangles, we may instead set $\delta = 17n2^{n-1}\sqrt{2\epsilon}$.

B Proof of Robustness for Reference Experiment 2

Much of the same analysis may be used for experiment 2. Indeed, since the only difference in the proofs for the non-robust results is how the anti-commuting property is proved, we may simply replace the estimation for Lemma 3 with that of Lemma 4.

We begin, then, with ϵ -simulation and prove a robust version of Lemma 4. First we wish to estimate $\alpha = \left\| D'_u |\psi\rangle - \frac{X'_u + Z'_u}{\sqrt{2}} |\psi\rangle \right\|_2$. Using techniques from the previous section, we have

$$\left\| X'_u |\psi'\rangle - Z'^{N_u} |\psi\rangle \right\|_2 \leq 2\sqrt{\epsilon} \quad (67)$$

$$\left\| Z'_u |\psi'\rangle - X'_v Z'^{N_v \setminus u} |\psi'\rangle \right\|_2 \leq 2\sqrt{\epsilon}. \quad (68)$$

These along with the triangle inequality give an upper bound for α of

$$2\sqrt{2\epsilon} + \left\| D'_u |\psi\rangle - \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} |\psi\rangle \right\|_2 \quad (69)$$

Expanding the second term, we get

$$\sqrt{1 + \left\| \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} | \psi' \rangle \right\|_2^2 - \sqrt{2} (\langle \psi' | D'_u Z'^{N_u} | \psi' \rangle + \langle \psi' | D'_u X'_v Z'^{N_v \setminus u} | \psi' \rangle)}. \quad (70)$$

Since $\|Z'_u | \psi' \rangle - X'_v Z'^{N_v \setminus u} | \psi' \rangle\|_2 \leq 2\sqrt{\epsilon}$ and $\|Z'^{N_u} | \psi' \rangle\|_2 = 1$ we find

$$\left| \langle \psi' | Z'^{N_u} Z'_u | \psi' \rangle - \langle \psi' | Z'^{N_u} X'_v Z'^{N_v \setminus u} | \psi' \rangle \right| \leq 2\sqrt{\epsilon}. \quad (71)$$

By hypothesis, $|\langle \psi' | Z'^{N_u} Z'_u | \psi' \rangle| \leq \epsilon$, so $|\langle \psi' | Z'^{N_u} X'_v Z'^{N_v \setminus u} | \psi' \rangle| \leq 2\sqrt{\epsilon} + \epsilon$.

Meanwhile $\beta^2 = \left\| \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} | \psi' \rangle \right\|_2^2 = 1 + \operatorname{Re} \langle \psi' | Z'^{N_u} X'_v Z'^{N_v \setminus u} | \psi' \rangle$, so $|1 - \beta^2| \leq 2\sqrt{\epsilon} + \epsilon$.

Finally, by hypothesis $|\langle \psi' | D'_u Z'^{N_u} | \psi' \rangle + \langle \psi' | D'_u X'_v Z'^{N_v \setminus u} | \psi' \rangle - \sqrt{2}| \leq 2\epsilon$. Combining these facts we find $\alpha \leq 2\sqrt{2\epsilon} + \sqrt{2\sqrt{\epsilon} + (1 + 2\sqrt{2})\epsilon}$.

Now we wish to estimate

$$\left\| (D'_u)^2 | \psi' \rangle - \frac{(X'_u + Z'_u)^2}{2} | \psi' \rangle \right\|_2 \quad (72)$$

By the fact $\|D'_u\|_\infty = 1$ we have $\left\| (D'_u)^2 | \psi' \rangle - D'_u \frac{X'_u + Z'_u}{\sqrt{2}} | \psi' \rangle \right\|_2 \leq \alpha$. Similarly, since $\|X'_u + Z'_u\|_\infty \leq 2$ we find $\left\| D'_u \frac{X'_u + Z'_u}{\sqrt{2}} | \psi' \rangle - \frac{(X'_u + Z'_u)^2}{2} | \psi' \rangle \right\|_2 \leq \sqrt{2}\alpha$. Using these facts, the triangle inequality, and $(D'_u)^2 = I$, we obtain

$$\begin{aligned} 2 \left\| | \psi' \rangle - \frac{(X'_u + Z'_u)^2}{2} | \psi' \rangle \right\|_2 &= \|X'_u Z'_u | \psi' \rangle + Z'_u X'_u | \psi' \rangle\|_2 \\ &\leq 2(1 + \sqrt{2}) \left(2\sqrt{2\epsilon} + \sqrt{2\sqrt{\epsilon} + (1 + 2\sqrt{2})\epsilon} \right) \leq 26\epsilon^{\frac{1}{4}} \end{aligned} \quad (73)$$

with the last inequality valid for $\epsilon \leq 1$.

Using this estimate, and working through the estimations as in the previous section, we find that we may set

$$\delta = 2^{n-2} \left((2n + |E|)(26\epsilon^{\frac{1}{4}} + 4l\sqrt{2\epsilon}) + 2n\sqrt{2\epsilon} \right). \quad (74)$$

For a simpler expression, we may use $l \leq n$ and $|E| \leq n^2$, obtaining

$$\delta = n2^{n-2} \left((n + 2)26\epsilon^{\frac{1}{4}} + (4n^2 + 10n)\sqrt{2\epsilon} \right) \quad (75)$$

Again, we may find a better estimate with more information about the graph. For cluster states, which have a square lattice graph, we have $|E| \leq 4n$. We may also perform D_u measurements on all vertices and set $l = 0$. In this case we may set $\delta = n2^{n-2} \left(156\epsilon^{\frac{1}{4}} + 2\sqrt{2\epsilon} \right)$.

C Classical Hidden Variable Model for Bipartite Graph States with X and Z Measurements

Let G be a bipartite graph and $|\psi\rangle$ the corresponding graph state. We give a local hidden variable model that is consistent with all measurements which are tensor products of X and Z on this state.

We construct a local hidden variable model by randomly choosing a value ± 1 for Z'_v for each v in the graph. We then set X'_v to be

$$X'_v = \prod_{u \in N_v} Z'_u. \quad (76)$$

Now we show that this is consistent with all possible tensor product X and Z measurements on $|\psi\rangle$. Let $M = X^S Z^T$, $S \cap T = \emptyset$ be such a measurement. First, suppose that $\pm M$ can be written as a product of stabilizers of $|\psi\rangle$. Using Lemma 1 we have

$$M = X^S Z^{N(S)} = (-1)^{|E(S)|} \prod_{x \in S} S_x. \quad (77)$$

Note that, by assumption, M has only X and Z factors, so each $v \in S$ must have an even number of neighbours in S . Then the induced subgraph on S is Eulerian and we can partition the edges of the subgraph into cycles with no common edges (see Diestel [Die10] for a proof). Suppose that $|E(S)|$ is odd. Then there must be at least one odd cycle in this partition and then S has an odd cycle and so does G . Since G is bipartite this must not be the case and in fact $|E(S)|$ is even. Hence $M = \prod_{x \in S} S_x$ and $\langle \psi | M | \psi \rangle = 1$. By construction $M' = X'^S Z'^{N(S)} = \prod_{v \in S} X'_v Z'^{N_v} = 1$ and the expected value of M' matches that of M .

Now suppose that M is not a product of stabilizers of $|\psi\rangle$. Then M must anti-commute with at least one stabilizer and hence $\langle \psi | M | \psi \rangle = 0$. Meanwhile, by construction

$$M' = X'^S Z'^T = Z'^{N(S)} Z'^T. \quad (78)$$

If $N(S) = T$ then M is in fact a product of stabilizers. This is not the case, so there is at least one Z'_v in the above equation which is not cancelled. Since all the Z'_v s are chosen randomly, the product of the Z'_v s not cancelled will also be uniformly random. Thus the expected value of M' is 0.

References

- [Die10] Diestel, R.: Graph theory. In: Graduate Texts in Mathematics, vol. 173, 4th edn. Springer, Heidelberg. <http://diestel-graph-theory.com/> (2010)
- [MM11] McKague, M., Mosca, M.: Generalized self-testing and the security of the 6-state protocol. In: van Dam, W., Kendon, V.M., Severini, S. (eds.) TQC 2010. LNCS, vol. 6519, pp. 113–130. Springer, Heidelberg (2011)

- [MMMO06] Magniez, F., Mayers, D., Mosca, M., Ollivier, H.: Self-testing of quantum circuits. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4051, pp. 72–83. Springer, Heidelberg (2006)
- [MY04] Mayers, D., Yao, A.: Self testing quantum apparatus. *Quantum Inf. Comput.* **4**(4), 273–286 (2004). (<http://arxiv.org/abs/quant-ph/0307205>, <http://www.rintonpress.com/journals/qiconline.html#v4n4>)
- [PAM⁺10] Pironio, S., Acin, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D.N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T.A., Monroe, C.: Random numbers certified by bell’s theorem. *Nature* **464**(7291), 1021–1024 (2010). doi:[10.1038/nature09008](https://doi.org/10.1038/nature09008). (EPRINT [arXiv:0911.3427](https://arxiv.org/abs/0911.3427))
- [RB01] Raussendorf, R., Briegel, H.J.: A one-way quantum computer. *Phys. Rev. Lett.* **86**(22), 5188–5191 (2001). doi:[10.1103/PhysRevLett.86.5188](https://doi.org/10.1103/PhysRevLett.86.5188). (EPRINT [arxiv:quant-ph/0010033](https://arxiv.org/abs/quant-ph/0010033))
- [vMMS00] van Dam, W., Magniez, F., Mosca, M., Santha, M.: Self-testing of universal and fault-tolerant sets of quantum gates. In: *STOC ’00: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pp. 688–696. ACM, New York. (2000). doi:[10.1145/335305.335402](https://doi.org/10.1145/335305.335402). (EPRINT [arxiv:quant-ph/9904108](https://arxiv.org/abs/quant-ph/9904108))

Unconditionally-Secure and Reusable Public-Key Authentication

Lawrence M. Ioannou^{1,2}(✉) and Michele Mosca^{1,2,3}

¹ Institute for Quantum Computing, University of Waterloo, 200 University Avenue,
Waterloo, ON N2L 3G1, Canada

² Department of Combinatorics and Optimization, University of Waterloo, 200
University Avenue, Waterloo, ON N2L 3G1, Canada
lmioannou@gmail.com

³ Perimeter Institute for Theoretical Physics, 31 Caroline Street North,
Waterloo, ON N2L 2Y5, Canada

Abstract. We present a quantum-public-key identification protocol and show that it is secure against a computationally-unbounded adversary. This demonstrates for the first time that unconditionally-secure and reusable public-key authentication is possible in principle with (pure-state) public keys.

1 Introduction

Public-key cryptography has proved to be an indispensable tool in the modern information security infrastructure. Most notably, digital signature schemes form the backbone of Internet commerce, allowing trust to be propagated across the network in an efficient fashion. In turn, public-key encryption allows the private communication of messages (or, more usually, the establishment of symmetric secret keys) among users who are authenticated via digital signatures. The security of these classical public-key cryptosystems relies on assumptions on the difficulty of certain mathematical problems [1]. Gottesman and Chuang [2] initiated the study of quantum-public-key cryptography, where the public keys are quantum systems, with the goal of obtaining the functionality and efficiency of public-key cryptosystems but with information-theoretic security. They presented a secure one-time digital signature scheme for signing classical messages, based on Lamport’s classical scheme [3].

In a public-key framework, Alice chooses a random private key, creates copies of the corresponding public key via some publicly-known algorithm, and distributes the copies in an authenticated fashion to all potential “Bobs”. In principle, this asymmetric setup allows, e.g., any Bob to send encrypted messages to Alice or to verify any signature for a message that Alice digitally signed. By eliminating the need for each Alice-Bob pair to establish a secret key (in large networks where there may be many “Alices” and “Bobs”), the framework vastly simplifies key distribution, which is often the most costly part of any cryptosystem, compared to a framework that uses only symmetric keys.

Some remarks about the quantum-public-key framework are in order. First, we address the issue of *purity* of the quantum public keys. In principle, the quantum public key can be either in a pure or mixed state from Alice’s point of view (a mixed state is a fixed probabilistic distribution of pure states). Gottesman and Chuang [2] assumed pure-state public keys. For digital signature schemes, this purity is crucial; for, otherwise, Alice could cheat by sending different public keys to different “Bobs”. Purity prevents Alice’s cheating in this case because different “Bobs” can compare their copies of the public key via a “distributed SWAP-test” [2] to check they are the same (with high probability), much like can be done in the case of classical public keys. But any scheme can benefit from an equality test, since an adversary who tries to substitute bad keys for legitimate ones could thus be caught. There is no known equality test guaranteed to recognize when two mixed states are equal. Thus, having mixed-state public keys seems to be at odds with what it means to be “public”, i.e., publicly verifiable.¹ Even though the scheme we present in this paper does not make explicit use of the “distributed SWAP-test” (because we assume the public keys have been securely distributed), it can do so in principle. We view this as analogous to how modern public-key protocols do not specify use of an equality test among unsure “Bobs”, but how such a test is supported by the framework to help thwart attempts to distribute fake keys.

Second, we address the issue of *usability* of quantum-public-key systems. The states of two quantum public keys corresponding to two different private keys always have overlap less than $(1 - \delta)$, for some positive and publicly known δ . Thus, a striking aspect of the quantum-public-key framework is that the number of copies of the public key in circulation must be limited (if we want information-theoretic security). If this were not the case, then an adversary could collect an arbitrarily large number of copies, measure them all, and determine the private key. By adjusting protocol parameters, this limit on the number of copies of the quantum public key can be increased in order to accommodate more users (or uses; see next paragraph for a discussion on “reusability”). Thus, in practice, there is no restriction on the usability of a quantum-public-key system as long as an accurate estimate can be made of the maximum number of users/uses.

Presumably, adjusting the protocol parameters (as discussed above) in order to increase the maximum number of copies of the quantum public key in circulation would result in a less efficient protocol instance, and this is one kind of tradeoff between efficiency and usability in the quantum-public-key setting. Another kind concerns *reusability*. The abovementioned digital signature scheme is “one-time” because only one message may be signed under a particular key-value (even though many different users can verify that one signature). If a second message needs to be signed, the signer must choose a new private key and then distribute corresponding new public keys. One open problem is thus whether there exist reusable digital signature schemes, where either the same

¹ Other authors have defined the framework to include mixed public keys, and Ref. [4] proposes an encryption scheme with mixed public keys that is reusable and unconditionally secure [5].

copy of the public key can be used to verify many different message-signature pairs securely, or where just the same key-values can be used to verify many different message-signature pairs securely (but a fresh copy of the public key is needed for each verification). The latter notion of “reusability” is what we adopt here.

In this paper, we consider an identification scheme, which, like a digital signature scheme, is a type of authentication scheme. Authentication schemes seek to ensure the *integrity* of information, rather than its privacy. While digital signature schemes ensure the integrity of origin of messages, identification schemes ensure the integrity of origin of communication *in real time* [1]. Identification protocols are said to ensure “aliveness”—that the entity proving its identity is active at the time the protocol is executed; we describe them in more detail in the next section.

We prove that an identification scheme based on the one in Ref. [6] is secure against a computationally-unbounded adversary (only restricted by finite cheating strategies), demonstrating for the first time that unconditionally-secure and reusable public-key authentication is possible in principle. We regard our result more as a proof of concept than a (potentially) practical scheme. Still, we are confident that an extension of the techniques used here may lead to more efficient protocols.

We now proceed with a description of the protocol (Sect. 2) and the security proof (Sect. 3).

2 Identification Protocol

In the following, Alice and Bob are always assumed to be honest players and Eve is always assumed to be the adversary. Suppose Alice generates a private key and authentically distributes copies of the corresponding public key to any potential users of the scheme, including Bob.

Here is a description (adapted from Sect. 4.7.5.1 in Ref. [7]) of how a secure public-key identification scheme works. When Alice wants to identify herself to Bob (i.e. prove that it is she with whom he is communicating), she invokes the identification protocol by first telling Bob that she is Alice, so that Bob knows he should use the public key corresponding to Alice. The ensuing protocol has the property that the *prover* Alice can convince the *verifier* Bob (except, possibly, with negligible probability) that she is indeed Alice, but an adversary Eve cannot fool Bob (except with negligible probability) into thinking that she is Alice, even after having listened in on the protocol between Alice and Bob or having participated as a (devious) verifier in the protocol with Alice several times. Public-key identification schemes are used in smart-card systems (e.g., inside an automated teller machine (ATM) for access to a bank account, or beside a doorway for access to a building); the smart card “proves” its identity to the card reader.²

² Note that it is not a user’s personal identification number (PIN) that functions as the prover’s private key; the PIN only serves to authenticate the user to the smart card (not the smart card to the card reader).

Note that no identification protocol is secure against an attack where Eve concurrently acts as a verifier with Alice and as a prover with Bob (but note also that, in such a case, the “aliveness” property is still guaranteed). Note also that, by our definition of “reusable,” an identification scheme is considered reusable if Alice can prove her identity many times using the same key-values but the verifier needs a fresh copy of the public key for each instance of the protocol.

Note also that public-key identification can be trivially achieved via a digital signature scheme (Alice signs a random message presented by Bob), but we do not know of an unconditionally-secure and reusable digital signature scheme.³ Similarly, public-key identification can be achieved with a public-key encryption scheme (Bob sends an encrypted random challenge to Alice, who returns it decrypted), but we do not know of an unconditionally-secure and reusable public-key encryption scheme (that uses pure-state public keys; though, see Ref. [9] for a promising candidate).

2.1 Protocol Specification

The identification protocol takes the form of a typical “challenge-response” interactive proof system, consisting of a kernel (or subprotocol) that is repeated several times in order to amplify the security, i.e., reduce the probability that Eve can break the protocol. The following protocol is a simplification of the original protocol from Ref. [6] (but our security proof applies to both protocols, with only minor adjustments). We assume all quantum channels are perfect.

Parameters

- The *security* parameter $s \in \mathbf{Z}^+$
 - \diamond equals the number of kernel iterations.
 - \diamond The probability that Eve can break the protocol is exponentially small in s .
- The *reusability* parameter $r \in \mathbf{Z}^+$
 - \diamond equals the maximum number of copies of the quantum public key in circulation and
 - \diamond equals the maximum number of times the protocol may be executed by Alice, before she needs to pick a new private key.

Keys

- The *private key* is

$$(x_1, x_2, \dots, x_s), \tag{1}$$

where Alice chooses each x_j , $j = 1, 2, \dots, s$, independently and uniformly randomly from $\{1, 2, \dots, 2r + 1\}$.

- \diamond The value x_j is used only in the j th kernel-iteration.

³ Pseudo-signature schemes, such as the one in Ref. [8], are information-theoretically secure but assume broadcast channels.

- One copy of the *public key* is an s -partite system in the state

$$\otimes_{j=1}^s |\psi_{x_j}\rangle, \quad (2)$$

where (omitting normalization factors)

$$|\psi_{x_j}\rangle := |0\rangle + e^{2\pi i x_j / (2r+1)} |1\rangle. \quad (3)$$

- \diamond Alice authentically distributes (e.g. via trusted courier) at most r copies of the public key.
- \diamond The j th subsystem of the public key (which is in the state $|\psi_{x_j}\rangle$) is only used in the j th kernel-iteration.

Actions

- The *kernel* $\mathcal{K}(x)$ of the protocol is the following three steps, where we use the shorthand

$$\phi_x := 2\pi x / (r + 1), \quad (4)$$

and where we have dropped the subscript “ j ” from “ x_j ”:

- (1) Bob secretly chooses a uniformly random bit b and transforms the state of his authentic copy of $|\psi_x\rangle$ into $|0\rangle + (-1)^b e^{i\phi_x} |1\rangle$. Bob sends this qubit to Alice.
- (2) Alice performs the phase shift $|1\rangle \mapsto e^{-i\phi_x} |1\rangle$ on the received qubit and then measures the qubit in the basis $\{|0\rangle \pm |1\rangle\}$ (in order to determine Bob’s secret b above). If Alice gets the outcome corresponding to “+”, she sends 0 to Bob; otherwise, Alice sends 1.
- (3) Bob receives Alice’s bit as b' and tests whether b' equals b .
- When Alice wants to identify herself to Bob, they take the following actions:
 - (i) Alice checks that she has not yet engaged in the protocol r times before with the current value of the private key; if she has, she aborts (and refreshes the private and public keys).
 - (ii) Alice sends Bob her purported identity (“Alice”), so that Bob may retrieve the public keys corresponding to Alice.
 - (iii) The kernel $\mathcal{K}(x)$ is repeated s times, for $x = x_1, x_2, \dots, x_s$. Bob “accepts” if he found that b' equaled b in all the kernel iterations; otherwise, Bob “rejects”.

2.2 Completeness of the Protocol

It is clear that the protocol is correct for honest players: Bob always “accepts” when Alice is the prover. In the Appendix (“Sect. 3”), we prove that the protocol is also secure against any adversary (only restricted by finite cheating strategies): given r and $\epsilon > 0$, there exists a value of $s = s(r, \epsilon)$ such that Bob “accepts” with probability at most ϵ when Eve is the prover.

3 Security

Let us clearly define what Eve is allowed to do in our attack model. Eve can

- passively monitor Alice’s and Bob’s interactions (which means that Eve can read the classical bits sent by Alice, and read the bit that indicates whether Bob “accepts” or “rejects”), and
- participate as the verifier in one or more complete instances of the protocol, and
- participate as the prover, impersonating Alice, in one or more complete instances of the protocol.

Eve is assumed not to be able to actively interfere with Alice’s and Bob’s communications during the protocol, as this would allow Eve to concurrently act as verifier with Alice and as prover with Bob (thus trivially breaking any such scheme⁴).

Evidently, Eve’s passive monitoring only gives her independent and random bits (and the bit corresponding to “accept”), thus giving her no useful information (in that she may as well generate random bits herself). So, we can ignore the effects of her passive monitoring.

With regard to Eve acting as verifier, we will give Eve potentially more power by assuming that Alice, instead of performing both the phase shift and the measurement in Step 2 of the kernel $\mathcal{K}(x)$, only performs the phase shift (Eve could perform Alice’s measurement herself, if she desired). Furthermore, we will assume that the phase shift Alice performs is

$$u_{\phi_x} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi_x} \end{bmatrix}. \quad (5)$$

Even though Alice actually performs the inverse phase shift $u_{-\phi_x}$, note that the two phase shifts are equivalent in the sense that $Zu_{\phi_x}Z$ equals $u_{-\phi_x}$ up to global phase, where

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (6)$$

Thus the protocol is unchanged had we assumed that Alice, instead of performing $u_{-\phi_x}$ in Step 2 of the kernel $\mathcal{K}(x)$, performs $Zu_{\phi_x}Z$. Since Eve can perform

⁴ For password-based identification in a symmetric-key model, as in Ref. [10], where both Alice and Bob know something that Eve does not (i.e. the password), one can define a nontrivial “man-in-the-middle” attack, where Eve’s goal is to learn the password in order to impersonate Alice in a later instance of the protocol. However, in public-key identification, Eve’s goal of learning the private key may, without loss of generality, be accomplished by participating as a dishonest verifier and by obtaining copies of the public key, since Bob does not perform any action that Eve cannot perform herself given a copy of the public key.

Z gates on her qubit immediately before and after she gives it to Alice, our assumption indeed gives Eve at least as much power to cheat. Thus, Eve can effectively extract up to r black boxes for u_{ϕ_x} from Alice (recall Alice only participates in the protocol r times before refreshing her keys).

We will also give Eve potentially more power by giving her a black box for u_{ϕ_x} in place of every copy of $|\psi_x\rangle$ that she obtained legitimately. For each $x \in \{x_1, x_2, \dots, x_s\}$, let t be the total number of black boxes for u_{ϕ_x} that Eve has in her possession; that is, for simplicity, and without loss of generality, we assume she has the same number of black boxes u_{ϕ_x} for each value of x . Note that $t \leq (2r - 1)$, since we always assume that at least one copy of the public key is left for Bob, so that Eve can carry out the protocol with him.

Therefore, to prove security in our setting, it suffices to consider attacks where Eve first uses her st black boxes to create a reference system in some $(\phi_{x_1}, \phi_{x_2}, \dots, \phi_{x_s})$ -dependent state, denoted $|\Psi_R(\phi_{x_1}, \phi_{x_2}, \dots, \phi_{x_s})\rangle$, and then she uses this system while she participates as a prover, impersonating Alice, in one or many instances of the protocol in order to try to cause Bob to “accept”. We use the following definition of “security”:

Definition 1 (Security). *An identification protocol (for honest prover Alice and honest verifier Bob) is secure with error ϵ if the probability that Bob “accepts” when any adversary Eve participates in the protocol as a prover is less than ϵ .*

The only assumption we make on Eve is that her cheating strategy is finite in the sense that her quantum computations are restricted to a finite-dimensional complex vector space; the dimension itself, though, is unbounded.

We will assume that Eve has always extracted the r black boxes for u_{ϕ_x} from Alice (for all $x = x_1, x_2, \dots, x_s$), and we define t' to be the number black boxes that Eve obtained legitimately (via copies of the public key):

$$t = r + t'. \quad (7)$$

Note that Eve can make at most $(r - t')$ attempts at fooling Bob, i.e., causing Bob to “accept”. Let $E(a, b)$ denote the event that Eve fools Bob on her a th attempt using b black boxes for u_{ϕ_x} for all $x = x_1, x_2, \dots, x_s$. Most of the argument, beginning in Sect. 3.1, is devoted to showing that

$$\Pr[E(1, t)] \leq (1 - c/(t + 2)^2)^s, \quad (8)$$

for some positive constant c defined at the end of Sect. 3. In general, Eve learns something from one attempt to the next; however, because Eve can simulate her interaction with Bob at the cost of using one copy of $|\psi_x\rangle$ per simulated iteration of $\mathcal{K}(x)$, we have, for $\ell = 2, 3, \dots, (r - t')$,

$$\Pr[E(\ell, t)] \leq \Pr[E(1, t + \ell - 1)]. \quad (9)$$

Given this, we use the union bound:

$$\Pr[\text{Eve fools Bob at least once, using } t \text{ black boxes for } u_{\phi_x}, \forall x] \quad (10)$$

$$\leq \sum_{\ell=1}^{r-t'} \Pr[E(\ell, t)] \quad (11)$$

$$\leq \sum_{\ell=1}^{r-t'} \Pr[E(1, t + \ell - 1)] \quad (12)$$

$$\leq \sum_{\ell=1}^{r-t'} (1 - c/(t + \ell + 1))^s \quad (13)$$

$$\leq (r - t')(1 - c/(2r + 1))^s, \quad (14)$$

since $t + \ell \leq 2r$. It follows that the probability that Eve can fool Bob at least once, that is, break the protocol, is

$$P_{\text{break}} \leq r(1 - c/(2r + 1))^s, \quad (15)$$

which, for fixed r , is exponentially small in s . Note that this bound is likely not tight, since it ultimately assumes that all of Eve's attempts are equally as powerful. In particular, this bound assumes that Eve's state $|\Psi_R(\phi_{x_1}, \phi_{x_2}, \dots, \phi_{x_s})\rangle$ does not degrade with use. A more detailed analysis using results about degradation of quantum reference frames [11] may be possible.

From Eq. (15) follows our main theorem (see Appendix A.3 for the proof):

Theorem 1 (Security of the protocol). *For any $\epsilon > 0$ and any $r \in \mathbf{Z}^+$, the identification protocol specified in Sect. 2.1 is secure with error ϵ according to Definition 1 if*

$$s > (2r + 1)^2 \log(r/\epsilon)/c, \quad (16)$$

for some positive constant c .

The theorem shows how the efficiency of the protocol scales with its reusability: it suffices to have

$$s \in O(r^2 \log(r/\epsilon)). \quad (17)$$

The remainder of the paper establishes the bound in Line (8).

3.1 Sufficiency of Individual Attacks

At each iteration, we may assume Eve performs some measurement, in order to get an answer to send back to Bob. Generally, Eve can mount a coherent attack, whereby her actions during iteration j may involve systems that she used or will use in previous or future iterations as well as systems created using black boxes for $u_{\phi_{x_k}}$ for any k —not just for $k = j$. Since each x_j is *independently* selected

from the set $\{1, 2, \dots, 2r + 1\}$, intuition suggests that Eve’s measurement at iteration j may be assumed to be independent of her measurement at any other iteration and in particular does not need to involve any black boxes other than ones for $u_{\phi_{x_j}}$. In other words, it seems plausible that the optimal strategy for Eve can consist of the “product” of identical optimal strategies for each iteration individually. This intuition can indeed be shown to be correct by combining a technique from Ref. [12], for expressing the maximum output probability in a multiple-round quantum interactive protocol as a semidefinite program, with a result in Ref. [13], which implies that the semidefinite program satisfies the product rule that we need; see Appendix A.1 for a proof.

The remainder of Sect. 3 establishes the following proposition:

Proposition 2. *The probability that Eve guesses correctly in any particular iteration j , using t black boxes for $u_{\phi_{x_j}}$, is at most $(1 - c/(t + 2)^2)$ for some positive constant c .*

Assuming Proposition 2, the result proved in Appendix A.1 implies that the probability of Eve’s guessing correctly in all s iterations, using t black boxes for u_{ϕ_x} , for $x = x_1, x_2, \dots, x_s$, is at most $(1 - c/(t + 2)^2)^s$, establishing the bound in Line (8).

3.2 Equivalence of Discrete and Continuous Private Phases

To help us prove Proposition 2, we now show that, from Bob’s and Eve’s points of view, Alice’s choosing the private phase angle ϕ_x from the discrete set $\{2\pi x/(2r + 1) : x = 1, 2, \dots, 2r + 1\}$ is equivalent to her choosing the phase angle from the continuous interval $[0, 2\pi)$. We have argued that the only information that Eve or Bob—or anyone but Alice—has about ϕ_x may be assumed to come from a number of black boxes for u_{ϕ_x} that can be no greater than $2r$ (there are r legitimate copies of the public key, and one can extract r more black boxes from Alice); let this number be d , where $1 \leq d \leq 2r$.

In order to access the information from the black boxes, they must, in general, be used in a quantum circuit in order to create some state. Using the d black boxes, the most general (purified) state that can be made is without loss of generality of the form

$$|\psi(\phi_x)\rangle = \sum_{k=0}^{N-1} \left(\sum_{j=0}^d \beta_{j,k} e^{ij\phi_x} \right) |a_k\rangle, \quad (18)$$

where $\{|a_k\rangle : k = 0, 1, \dots, N - 1\}$ is an orthonormal basis of arbitrary but finite size (the assumption of finite N comes from our restricting Eve to using only finite cheating strategies). In general, the numbers N and $\beta_{j,k}$ may depend on d . Here we have followed Ref. [14] by noting that each amplitude is a polynomial in $e^{i\phi_x}$ of degree at most d ; this fact follows from an inductive proof just as in Ref. [15], where the polynomial method is applied to an oracle revealing one of many Boolean variables.

Averaging over Alice’s random choices of x , one would describe the previous state by the density operator

$$\frac{1}{2r+1} \sum_{x=1}^{2r+1} |\psi(\phi_x)\rangle\langle\psi(\phi_x)|, \quad (19)$$

since x is chosen uniformly randomly from $\{1, 2, \dots, 2r+1\}$. Had ϕ_x been chosen uniformly from $\{2\pi x/(2r+1) : x \in [0, 2r+1)\} = [0, 2\pi)$, one would describe the state by

$$\int_0^{2\pi} \frac{d\phi}{2\pi} |\psi(\phi)\rangle\langle\psi(\phi)|. \quad (20)$$

It is straightforward to show⁵ that the above two density operators are both equal to

$$\sum_{k,k'=0}^{N-1} \sum_{j=0}^d \beta_{j,k} \beta_{j,k'}^* |a_k\rangle\langle a_{k'}|. \quad (23)$$

Thus, without loss of generality, we may drop the subscript “ x ” on “ ϕ_x ”, write “ ϕ ” for Alice’s private phase angle, and assume she did (somehow) choose ϕ uniformly randomly from $[0, 2\pi)$.⁶ We are now ready to prove Proposition 2.

3.3 Bound on Relative Phase Shift Estimation

Eve’s task of cheating in one iteration of the kernel may be phrased as follows. Eve is to decide the difference between the relative phases encoded in two subsystems R and S , where S is a given one-qubit system and R is under her control. The given subsystem S is in the state

$$|\psi_S(\phi, \theta)\rangle = |0\rangle + e^{i(\phi+\theta)}|1\rangle, \quad (24)$$

⁵ This requires the following two facts: (1) for any integer a ,

$$\frac{1}{2\pi} \int_0^{2\pi} e^{ia\theta} d\theta = \begin{cases} 0 & \text{if } a \neq 0, \\ 1 & \text{otherwise;} \end{cases} \quad (21)$$

and (2) for any integer $p \geq 2$ and integer a :

$$\frac{1}{p} \sum_{k=1}^p e^{2\pi i ak/p} = \begin{cases} 0 & \text{if } a \text{ is not a multiple of } p, \\ 1 & \text{otherwise,} \end{cases} \quad (22)$$

where the second fact is applied at $p = 2r + 1$.

⁶ One way to interpret this result is that even if Alice encodes infinitely many bits into ϕ , it is no better than if she encoded $\lceil \log_2(2r+1) \rceil$ bits. Note that if Eve performs an optimal phase estimation [16] in order to learn ϕ and then cheat Bob, she can only learn at most $\lfloor \log_2(2r-1) \rfloor$ bits of ϕ (here, we assume Eve has $2r-1$ copies of the public key, having left Bob one copy), whereas Alice actually encoded $\lceil \log_2(2r+1) \rceil$ bits into ϕ .

where θ is unknown and uniformly random in $\{0, \pi\}$, and ϕ is unknown and uniformly random in $[0, 2\pi]$. Eve can make the state $|\psi_R(\phi)\rangle$ of subsystem R by using arbitrary operations interleaved with at most t black boxes for the one-qubit gate u_ϕ . Note that the problem is nontrivial because ϕ is unknown and uniformly random and the qubit S is given to Eve *after* she has used all her black boxes. We seek the optimal success probability for Eve to guess θ correctly.

Eve's estimation problem can be treated within the framework of quantum estimation of group transformations [17]. As such, we regard her problem as finding the optimal measurement (probability) to correctly distinguish the states in the two-element orbit

$$\{V_\theta \rho V_\theta^\dagger : \theta \in \{0, \pi\}\}, \quad (25)$$

where $V_\theta = I_R \otimes (|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|)$ and

$$\rho = \int \frac{d\phi}{2\pi} |\psi_R(\phi)\rangle\langle\psi_R(\phi)| \otimes |\psi_S(\phi, 0)\rangle\langle\psi_S(\phi, 0)|. \quad (26)$$

The probabilities of her estimation procedure can be assumed to be generated by a POVM $\{E_0, E_\pi\}$. In general, it is known how to solve for the POVM that performs optimally on average when the unitarily-generated orbit consists of pure states, but not when the orbit is generated from a mixed state (ρ , in our case). Thus, we now effectively reduce the problem to several instances of an estimation problem where the orbit is pure.

Indeed, suppose that $|\psi_R(\phi)\rangle$ were a state on q qubits that satisfied the property

$$|\psi_R(\phi)\rangle\langle\psi_R(\phi)| = (u_\phi)^{\otimes q} |\psi_R(0)\rangle\langle\psi_R(0)| (u_\phi^\dagger)^{\otimes q} \quad (27)$$

for all $\phi \in [0, 2\pi]$. Then, letting $U_\phi \equiv (u_\phi)^{\otimes(q+1)}$ and $|\psi_{RS}(\phi, \theta)\rangle \equiv |\psi_R(\phi)\rangle|\psi_S(\phi, \theta)\rangle$, we would have that

$$\rho = \int \frac{d\phi}{2\pi} U_\phi |\psi_{RS}(0, 0)\rangle\langle\psi_{RS}(0, 0)| U_\phi^\dagger \quad (28)$$

$$= \sum_w P_w |\psi_{RS}(0, 0)\rangle\langle\psi_{RS}(0, 0)| P_w \quad (29)$$

$$= \sum_w P_w \rho P_w, \quad (30)$$

where P_w is the projection onto the subspace of Hamming weight $w = 0, 1, \dots, q+1$, and we used the formulas $U_\phi = \sum_w P_w e^{iw\phi}$ and $\delta_{w,0} = \int (d\phi/2\pi) e^{iw\phi}$. In other words, the state ρ would be block diagonal with respect to the direct-sum decomposition of the total state space of R into subspaces of constant Hamming weight w . Then we would have that the probability that Eve guesses $\theta = \theta'$ given

that $\theta = \theta''$ is

$$\Pr[\text{Eve guesses } \theta = \theta' | \theta = \theta''] = \text{Tr} \left[E_{\theta'} \left(V_{\theta''} \rho V_{\theta''}^\dagger \right) \right] \quad (31)$$

$$= \text{Tr} \left[E_{\theta'} V_{\theta''} \sum_w P_w \rho P_w V_{\theta''}^\dagger \right] \quad (32)$$

$$= \text{Tr} \left[\left(\bigoplus_w E_{w, \theta'} \right) \left(V_{\theta''} \rho V_{\theta''}^\dagger \right) \right], \quad (33)$$

where $E_{w, \theta'} \equiv P_w E_{\theta'} P_w$, and we used cyclicity of trace and the fact that V_θ and P_w commute. Thus, the elements of Eve's POVM $\{E_0, E_\pi\}$ would without loss of generality have the same block diagonal structure as ρ . In principle, this would allow Eve to measure first (just) the Hamming weight of ρ in order to find w , and then deal with the group transformation estimation problem with respect to the pure orbit

$$\mathcal{O}_w \equiv \{V_\theta |\Psi_w\rangle : \theta \in \{0, \pi\}\}, \quad (34)$$

where $|\Psi_w\rangle$ is the state such that $|\Psi_w\rangle \propto P_w |\psi_{RS}(0, 0)\rangle$; we note that $|\Psi_w\rangle$ is independent of ϕ (and θ). The following lemma shows that, without loss of generality, we may assume that the situation just described is indeed the case:

Lemma 1. *Without loss of generality, Eve's state $|\psi_R(\phi)\rangle$, which she prepares with at most t black boxes for u_ϕ , may be assumed to be on $q = (2t + 1)$ qubits and satisfy*

$$|\psi_R(\phi)\rangle\langle\psi_R(\phi)| = (u_\phi)^{\otimes q} |\psi_R(0)\rangle\langle\psi_R(0)| (u_\phi^\dagger)^{\otimes q} \quad (35)$$

for all $\phi \in [0, 2\pi]$.

Proof. As noted in the previous section, using the t black boxes, the most general (purified) state of R that Eve can make is without loss of generality

$$\sum_{k=0}^{N-1} \left(\sum_{j=0}^t \beta_{j,k} e^{ij\phi} \right) |a_k\rangle_R, \quad (36)$$

where, again, N is a priori unknown but finite (we use subscripts on the kets in this proof to indicate the physical systems). Note that we can rewrite the state in Eq. (36) by changing the order of the summations as

$$\sum_{j=0}^t \beta_j e^{ij\phi} |\tilde{g}_j\rangle_R, \quad (37)$$

where we have defined the numbers β_j and the not-necessarily-orthogonal set of unit vectors $\{|\tilde{g}_j\rangle : j = 0, 1, \dots, t\}$ such that

$$\beta_j |\tilde{g}_j\rangle_R = \sum_{k=0}^{N-1} \beta_{j,k} |a_k\rangle_R. \quad (38)$$

Using the Gram-Schmidt orthonormalization procedure on $\{|\tilde{g}_j\rangle\}_j$ to get the orthonormal set $\{|g_j\rangle\}_j$, we can write

$$|\tilde{g}_j\rangle_R = \sum_{h=0}^t \gamma_{j,h} |g_h\rangle_R. \quad (39)$$

Introduce a new system R' consisting entirely of qubits and define U to be any unitary map acting on $R \otimes R'$ that takes $|0\rangle_R |c_h\rangle_{R'} \mapsto |g_h\rangle_R |0\rangle_{R'}$, where $\{|c_h\rangle_{R'}\}_{h=0,1,\dots,t}$ is an orthonormal set of size $t+1$ with elements that are computational basis states whose labels have constant Hamming weight; note that R' needs only $O(\log(t+1))$ qubits whereas R is of unknown (but finite) size (however, following this proof, we will construct R' using $t+1$ qubits, as this makes things simpler). We first claim that, without loss of generality,

$$|\psi_R(\phi)\rangle = \sum_{j,h} \beta_j \gamma_{j,h} e^{ij\phi} |S_j^t\rangle_A |c_h\rangle_{R'}, \quad (40)$$

where A is a t -qubit ancilla, and $|S_j^t\rangle_A$ is the symmetric state of weight j . To see this, note that Eve's optimal measurement can include the following pre-processing operations (in sequence), so that she recovers the most general state in Eq. (36) (and Eq. (37)) on R but for a different random value of ϕ :

- add an ancillary register R in state $|0\rangle_R$ in between the two registers A and R' and perform U on $R \otimes R'$ to get (after throwing out system R')

$$\sum_j \beta_j \sum_h \gamma_{j,h} e^{ij\phi} |S_j^t\rangle_A |g_h\rangle_R = \sum_j \beta_j e^{ij\phi} |S_j^t\rangle_A |\tilde{g}_j\rangle_R \quad (41)$$

- on A , do the $(t+1)$ -dimensional inverse quantum Fourier transform in the symmetric basis on A , i.e. mapping

$$|S_j^t\rangle_A \mapsto \frac{1}{\sqrt{t+1}} \sum_y e^{-i2\pi yj/(t+1)} |S_y^t\rangle_A, \quad (42)$$

to get

$$\sum_j \sum_y \beta_j e^{ij(\phi - 2\pi y/(t+1))} |S_y^t\rangle_A |\tilde{g}_j\rangle_R \quad (43)$$

and measure the Hamming weight of A to get result y_0 , which leaves the state (after throwing out system A)

$$\sum_j \beta_j e^{ij(\phi - 2\pi y_0/(t+1))} |\tilde{g}_j\rangle_R \quad (44)$$

- correct the relative phase on qubit S by $2\pi y_0/(t+1)$.

Doing these operations does not change the estimation problem, since ϕ is uniformly random anyway; these operations just change the unknown ϕ to $\phi' = \phi - 2\pi y_0/(t+1)$.

Finally, note that Eq. (40) implies that $|\psi_R(\phi)\rangle$ can be made from $|\psi_R(0)\rangle$ with at most t black boxes for u_ϕ , by applying $(u_\phi)^{\otimes t}$ on the t qubits of system A , and note that $|\psi_R(\phi)\rangle$ satisfies Eq. (27), since the states $|c_h\rangle$ are of constant Hamming weight.

Remark 1. (Quantum Fourier transform as analytical tool) Note that Eve's optimal strategy is not necessarily to measure R to get an estimate ϕ' of ϕ first, then apply $u_{-\phi'}$ on S , and then measure S to estimate θ . However, the operation that is optimal for estimating ϕ (see Ref. [14]), i.e. the inverse quantum Fourier transform applied above, is still useful as an analytical tool in order to derive (a convenient form of) an optimal state for her estimation of θ .

Thus, by Lemma 1, we assume Eq. (40) holds, which allows us to derive the following proposition. For convenience, we define

$$\alpha_{j,h} \equiv \beta_j \gamma_{j,h}. \quad (45)$$

Proposition 3. *The elements of the POVM $\{E_0, E_\pi\}$ are without loss of generality defined as*

$$E_0 = |\Xi_0\rangle|0\rangle\langle\Xi_0| \langle 0| + \sum_{w=2}^{t+1} |w, +\rangle\langle w, +| \quad (46)$$

$$E_\pi = \sum_{w=2}^{t+1} |w, -\rangle\langle w, -| + |\Xi_t\rangle|1\rangle\langle\Xi_t| \langle 1|, \quad (47)$$

where

$$|w, \pm\rangle \equiv \frac{1}{\sqrt{2}}(|\Xi_{w-1}\rangle|0\rangle \pm |\Xi_{w-2}\rangle|1\rangle), \quad (48)$$

and $|\Xi_{w-1}\rangle$ and $|\Xi_{w-2}\rangle$ are states such that, for $j = 0, 1, \dots, t$,

$$|\Xi_j\rangle \propto \sum_h \frac{\alpha_{j,h}}{\sqrt{2}} |S_j^t\rangle |c_h\rangle. \quad (49)$$

The proof of Proposition 3 is similar to the argument given in Ref. [11] and is given in Appendix A.2. The total success probability of Eve's strategy can now be computed as

$$\sum_{\theta' \in \{0, \pi\}} \Pr[\text{Eve guesses } \theta = \theta' | \theta = \theta'] \Pr[\theta = \theta'] \quad (50)$$

$$= \frac{1}{2} \sum_{\theta' \in \{0, \pi\}} \text{Tr}(E_{\theta'} V_{\theta'} \rho V_{\theta'}^\dagger) \quad (51)$$

$$= \frac{1}{2} \sum_{\theta' \in \{0, \pi\}} \text{Tr}(E_{\theta'} V_{\theta'} |\psi_{RS}(0, 0)\rangle\langle\psi_{RS}(0, 0)| V_{\theta'}^\dagger) \quad (52)$$

$$= \frac{1}{2} + \frac{1}{4} \langle\psi_R(0)| M_t |\psi_R(0)\rangle, \quad (53)$$

where

$$M_t \equiv \sum_{j=0}^{t-1} |\Xi_{j+1}\rangle \langle \Xi_j| + |\Xi_j\rangle \langle \Xi_{j+1}|. \quad (54)$$

As a last task, we now seek the value of $|\psi_R(0)\rangle$ —i.e. the values of $\alpha_{j,h}$ —such that $\langle \psi_R(0) | M_t | \psi_R(0) \rangle$ is maximal. The proof of the following proposition is in Appendix A.4:

Proposition 4. *The state $|\psi_R(0)\rangle \propto \sum_{j=0}^t \sin\left[\frac{(j+1)\pi}{t+2}\right] |\Xi_j\rangle$ achieves the maximum value in Eq. (53).*

Thus (as in Ref. [11]—see Appendix A.4), we get a maximal success probability of

$$\frac{1}{2} + \frac{1}{2} \cos(\pi/(t+2)) \quad (55)$$

$$\leq \frac{1}{2} + \frac{1}{2} \left(1 - \frac{(\pi/(t+2))^2}{2!} + \frac{(\pi/(t+2))^4}{4!} \right) \quad (56)$$

$$= 1 - \frac{\pi^2}{4} \frac{1}{(t+2)^2} + \frac{\pi^4}{48} \frac{1}{(t+2)^4} \quad (57)$$

$$\leq 1 - \left(\frac{\pi^2}{4} - \frac{\pi^4}{48} \right) \frac{1}{(t+2)^2} \quad (58)$$

$$= 1 - c/(t+2)^2, \quad (59)$$

for the constant $c = (\pi^2/4 - \pi^4/48) \doteq 0.438$ and all $t \geq 1$. This completes the proof of Proposition 2 and thus the proof of Theorem 1.

A Appendices

A.1 Proof of Sufficiency of Individual Attacks

Consider the following non-cryptographic, $(t+1)$ -round interactive protocol (or game) between Evelyn and Bobby (neither of whom is considered adversarial, hence we distinguish these two players from Eve and Bob), denoted $\mathcal{L} = \mathcal{L}(\Phi)$, where

$$\Phi = (\Phi_1, \Phi_2, \dots, \Phi_{t+1}) \quad (60)$$

and the Φ_i are quantum operations (super-operators) that specify Evelyn's actions in the game (the quantities r and t are as defined previously):

- (1') Bobby chooses a uniformly random $x \in \{1, 2, \dots, 2r+1\}$ and sends a qubit in the state $|0\rangle$ to Evelyn (who can ignore this qubit—it carries no significant information).
- (2') For $i = 1, 2, \dots, t$ {
 - ◊ Evelyn performs the quantum operation Φ_i on her system, and then sends one qubit to Bobby.

- ◇ Bobby performs the unitary gate u_{ϕ_x} on the qubit received from Evelyn and sends it back to Evelyn.}
- (3′) Bobby chooses a uniformly random $b \in \{0, 1\}$ and sends a qubit in the state $|0\rangle + (-1)^b e^{i\phi_x} |1\rangle$ to Evelyn.
- (4′) Evelyn performs the quantum operation Φ_{t+1} on her system, and then sends one qubit to Bobby.
- (5′) Bobby measures the received qubit in the computational basis $\{|0\rangle, |1\rangle\}$, getting outcome 0 or 1 (corresponding to $|0\rangle$ and $|1\rangle$ respectively); he tests whether this outcome equals b .

The following proposition is straightforward to prove:

Proposition 5. *The probability that Eve, using t black boxes $u_{\phi_{x_j}}$, causes Bob’s equality test to pass in a particular iteration j of the protocol in Sect. 2.1 is at most*

$$\alpha = \max_{\Phi} \Pr[\text{Bobby’s equality test passes in } \mathcal{L}(\Phi)], \quad (61)$$

where Φ ranges over all $(t + 1)$ -tuples of admissible quantum operations that Evelyn can apply in the game \mathcal{L} .

Now consider the parallel s -fold repetition of \mathcal{L} , which we denote $\mathcal{L}^{\parallel s} = \mathcal{L}^{\parallel s}(\Phi')$, where now Φ' denotes Evelyn’s quantum operation in $\mathcal{L}^{\parallel s}$. The following proposition is also straightforward to prove:

Proposition 6. *The probability that Eve fools Bob on the first attempt using t black boxes per x -value in the protocol in Sect. 2.1 is at most*

$$\alpha' = \max_{\Phi'} \Pr[\text{all of Bobby’s equality tests pass in } \mathcal{L}^{\parallel s}(\Phi')], \quad (62)$$

where Φ' ranges over all $(t + 1)$ -tuples of admissible quantum operations that Evelyn can apply in the game $\mathcal{L}^{\parallel s}$.

Therefore, in order to prove that it is sufficient to consider individual (as opposed to coherent) attacks by Eve, it suffices to show that $\alpha' = \alpha^s$.

In Ref. [12], the above game is viewed as an interaction between a $(t + 1)$ -round (*non-measuring*) strategy and a (*compatible*) measuring co-strategy; Evelyn’s operations Φ form the non-measuring strategy and Bobby’s actions form the measuring co-strategy (technically, Steps (1′), (3′), and (4′) would have to be slightly modified in order to fit the co-strategy formalism: in Steps (1′) and (3′), Bobby should make his random choices in superposition and use the quantum registers storing these choices as a control register whenever requiring these random values subsequently; in Step (4′), Bobby should only make one final measurement whose outcome indicates whether the equality test passes; we assume that these modifications have been made).

For all i , let \mathcal{X}_i and \mathcal{Y}_i be the input and output spaces, respectively, of Evelyn’s quantum operation Φ_i in \mathcal{L} , i.e. $\Phi_i : L(\mathcal{X}_i) \rightarrow L(\mathcal{Y}_i)$, where $L(\mathcal{X}_i)$ is the

space of all linear operators from the complex Euclidean space \mathcal{X}_i to itself (and likewise for $L(\mathcal{Y}_i)$). Let $\text{Pos}(\mathcal{Y} \otimes \mathcal{X})$ denote the set of all positive semidefinite operators in $L(\mathcal{Y} \otimes \mathcal{X})$, where $\mathcal{Y} = \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_{t+1}$ (and similarly for \mathcal{X}). For any Euclidean space \mathcal{Z} , let $\mathbb{I}_{\mathcal{Z}}$ denote the identity operator \mathcal{Z} .

Reference [12] shows that Evelyn's strategy can be equivalently expressed by a single positive semidefinite operator in $\text{Pos}(\mathcal{Y} \otimes \mathcal{X})$ while Bobby's measuring co-strategy can be expressed by the collection $\{B_0, B_1\}$ of two positive semidefinite operators in $\text{Pos}(\mathcal{Y} \otimes \mathcal{X})$, where, without loss of generality, we assume that B_0 corresponds to the measurement outcome indicating that Bobby's test for equality in Step (5') passes. We briefly note that these positive semidefinite operators are the Choi-Jamiołkowski representations of quantum operations corresponding to the players' actions. A more general version of the following theorem is proved in Ref. [12]:

Theorem 7 (Interaction output probabilities [12]). *For any non-measuring strategy $X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X})$ of Evelyn, the probability that Bobby's equality test passes is $\text{Tr}(B_0^\dagger X)$.*

Using Theorem 7, it is shown, in the proof of Theorem 3.3 of Ref. [12], that the maximal probability with which Bobby's measuring co-strategy can be forced to output the outcome corresponding to B_0 by some (compatible) strategy of Evelyn's can be expressed as a semidefinite (optimization) program (see Ref. [18] for a relevant review of semidefinite programming). Thus α and α' can be expressed, respectively, as solutions to the following semidefinite programs π_α and $\pi_{\alpha'}$:

$$\begin{array}{ll} \overline{\pi_\alpha} & \overline{\pi_{\alpha'}} \\ \text{maximize: } \text{Tr}(B_0^\dagger X) & \text{maximize: } \text{Tr}((B_0^{\otimes s})^\dagger X) \\ \text{subject to: } \text{Tr}_{\mathcal{Y}}(X) = \mathbb{I}_{\mathcal{X}}, & \text{subject to: } \text{Tr}_{\mathcal{Y}'}(X) = \mathbb{I}_{\mathcal{X}'}, \\ X \in \text{Pos}(\mathcal{Y} \otimes \mathcal{X}) & X \in \text{Pos}(\mathcal{Y}' \otimes \mathcal{X}'), \end{array}$$

where, for all i , $\mathcal{X}'_i = \mathcal{X}_i^{\otimes s}$ and $\mathcal{X}' = \mathcal{X}'_1 \otimes \mathcal{X}'_2 \otimes \cdots \otimes \mathcal{X}'_{t+1}$ (and similarly for \mathcal{Y}'_i and \mathcal{Y}'). We note that the first constraint in each semidefinite program above codifies the property of trace-preservation for the quantum operation corresponding to X , while the second constraint codifies the property of complete positivity (see Ref. [18] for details). Furthermore, it is shown in Ref. [12] that such semidefinite programs (arising from interactions between strategies and compatible co-strategies) satisfy the condition of strong duality, which means that the solution to each semidefinite program above coincides with that of its dual.

In Ref. [13], the following theorem is proven:

Theorem 8 (Condition for product rule for semidefinite programs [13]). *Suppose that the following two semidefinite programs π_1 and π_2 satisfy strong duality:*

$$\begin{array}{ll} \overline{\pi_1} & \overline{\pi_2} \\ \text{maximize: } \text{Tr}(J_1^\dagger W) & \text{maximize: } \text{Tr}(J_2^\dagger W) \\ \text{subject to: } \Psi_1(W) = C_1, & \text{subject to: } \Psi_2(W) = C_2, \\ W \in \text{Pos}(\mathcal{W}_1) & W \in \text{Pos}(\mathcal{W}_2), \end{array}$$

where $\Psi_1 : \mathbb{L}(\mathcal{W}_1) \rightarrow \mathbb{L}(\mathcal{Z}_1)$ and $\Psi_2 : \mathbb{L}(\mathcal{W}_2) \rightarrow \mathbb{L}(\mathcal{Z}_2)$, for complex Euclidean spaces $\mathcal{W}_1, \mathcal{Z}_1, \mathcal{W}_2, \mathcal{Z}_2$, and $J_1 \in \mathbb{L}(\mathcal{W}_1)$ and $J_2 \in \mathbb{L}(\mathcal{W}_2)$ are Hermitian. Let $\alpha(\pi_1)$ and $\alpha(\pi_2)$ denote the semidefinite programs' solutions. If J_1 and J_2 are positive semidefinite, then the solution to the following semidefinite program, denoted $\pi_1 \otimes \pi_2$, is $\alpha(\pi_1 \otimes \pi_2) = \alpha(\pi_1)\alpha(\pi_2)$:

$$\begin{aligned} & \text{maximize: } \frac{\pi_1 \otimes \pi_2}{\text{Tr}((J_1 \otimes J_2)^\dagger W)} \\ & \text{subject to: } \Psi_1 \otimes \Psi_2(W) = C_1 \otimes C_2, \\ & \quad W \in \text{Pos}(\mathcal{W}_1 \otimes \mathcal{W}_2). \end{aligned}$$

Since B_0 is positive semidefinite and $\pi_{\alpha'} = \pi_{\alpha^s}$ (using the associativity of \otimes), Theorem 8 can be applied $(s-1)$ times in order to prove that $\alpha' = \alpha^s$ as required. See Ref. [12] for a similar approach, based on ideas in Ref. [19]. The idea of expressing the acceptance probability of a quantum interactive proof system as a semidefinite program first appeared in Ref. [20].

Note that this argument, combined with the arguments in the main body of the paper, shows that both the serial and parallel versions of our identification protocol are secure.

A.2 Proof of Proposition 3

Two facts hold without loss of generality:

- the POVMs $\{E_{w,0}, E_{w,\pi}\}$, for all w , may be assumed to be covariant, i.e. $E_{w,\pi} = V_\pi E_{w,0} V_\pi^\dagger$ (to see this, note that any not-necessarily-covariant POVM $\{F_{w,0}, F_{w,\pi}\}$ gives the same average probability of successfully guessing θ , given w , as the covariant POVM $\{E_{w,0}, E_{w,\pi}\}$ defined by $E_{w,0} = (F_{w,0} + V_\pi^\dagger F_{w,\pi} V_\pi)/2$);
- each $E_{w,0}$ has support only on $\text{sp}(\mathcal{O}_w)$ and thus $E_{w,0} + E_{w,\pi} = I_{\text{sp}(\mathcal{O}_w)}$, where $I_{\text{sp}(\mathcal{O}_w)}$ is the identity operator on $\text{sp}(\mathcal{O}_w)$.

To compute a basis of $\text{sp}(\mathcal{O}_w)$, we now further define the system R' in the proof of Lemma 1 to consist of exactly $t+1$ qubits and the states $|c_h\rangle$, $h = 0, 1, \dots, t$, to be all those computational basis states whose labels have Hamming weight 1 (thus $q = 2t+1$, which is larger than necessary, but simplifies the structure of the POVMs). The total subspace

$$S \equiv \text{sp}(\{|S_j^t\rangle\}_{j=0,\dots,t} \otimes \{|c_h\rangle\}_{h=0,1,\dots,t} \otimes \{|0\rangle, |1\rangle\}) \quad (63)$$

supporting $|\psi_{RS}(\phi, \theta)\rangle$ breaks up into mutually orthogonal subspaces S_w of weight w , i.e., spanned by computational basis states whose labels have Hamming weight w :

$$S_1 = \text{sp}(|S_0^t\rangle \otimes \{|c_h\rangle\}_h \otimes |0\rangle) \quad (64)$$

$$S_k = \text{sp}(|S_{k-1}^t\rangle \otimes \{|c_h\rangle\}_h \otimes |0\rangle, |S_{k-2}^t\rangle \otimes \{|c_h\rangle\}_h \otimes |1\rangle), \quad (65)$$

$$S_{t+2} = \text{sp}(|S_t^t\rangle \otimes \{|c_h\rangle\}_h \otimes |1\rangle), \quad (66)$$

for $k = 2, 3, \dots, t+1$. Thus, for each w , we will do the following:

- write P_w in the basis in which S_w is expressed in Eqs. (64), (65), (66),
- derive an expression for $P_w|\psi_{RS}(0, 0)\rangle$ (which is proportional to $|\Psi_w\rangle$) in order to find a basis for $\text{sp}(\mathcal{O}_w) = \text{sp}\{|\Psi_w\rangle, V_\pi|\Psi_w\rangle\}$ (which fully supports $E_{w,0}$), and
- derive the form of $E_{w,0}$ and thus, by covariance, the form of the POVM $\{E_{w,0}, E_{w,\pi}\}$ in each subspace S_w .

Recalling Eq. (40), it will be convenient to let $\alpha_{j,h} \equiv b_j g_{j,h}$ and so

$$|\psi_R(0)\rangle = \sum_{j,h} \alpha_{j,h} |S_j^t\rangle |c_h\rangle. \quad (67)$$

$w=1$:

Writing

$$P_1|\psi_{RS}(0, 0)\rangle \quad (68)$$

$$= \left(\sum_h |S_0^t\rangle \langle S_0^t| \otimes |c_h\rangle \langle c_h| \otimes |0\rangle \langle 0| \right) |\psi_R(0)\rangle (|0\rangle + |1\rangle) / \sqrt{2} \quad (69)$$

$$= |S_0^t\rangle \left(\sum_h [(\langle S_0^t | \langle c_h | |\psi_R(0)\rangle) / \sqrt{2}] |c_h\rangle \right) |0\rangle \quad (70)$$

$$= |S_0^t\rangle \left(\sum_h [\alpha_{0,h} / \sqrt{2}] |c_h\rangle \right) |0\rangle, \quad (71)$$

we see that $V_\pi|\Psi_1\rangle = |\Psi_1\rangle$ so that $E_{1,0} = E_{1,\pi} = |\Xi_0\rangle\langle 0| \langle \Xi_0| \langle 0|$, where $|\Xi_0\rangle$ is a state such that

$$|\Xi_0\rangle \propto |S_0^t\rangle \sum_h [\alpha_{0,h} / \sqrt{2}] |c_h\rangle. \quad (72)$$

We note that getting the outcome corresponding to this POVM element does not give any information about θ ; we arbitrarily assign a guess of “ $\theta = 0$ ” to this outcome, without affecting optimality (since θ is a priori uniformly distributed).

$w \in \{2, 3, \dots, t+1\}$:

Similarly, we can write

$$P_w|\psi_{RS}(0, 0)\rangle \quad (73)$$

$$= |S_{w-1}^t\rangle \left(\sum_h [\alpha_{w-1,h} / \sqrt{2}] |c_h\rangle \right) |0\rangle + \quad (74)$$

$$|S_{w-2}^t\rangle \left(\sum_h [\alpha_{w-2,h} / \sqrt{2}] |c_h\rangle \right) |1\rangle. \quad (75)$$

Chiribella et al. [17] show that $E_{w,0}$ may be assumed to have rank 1 without loss of generality. Thus $E_{w,0}$ may be written $|\eta_w\rangle\langle \eta_w|$, where

$$|\eta_w\rangle = a|\Xi_{w-1}\rangle|0\rangle + b|\Xi_{w-2}\rangle|1\rangle, \quad (76)$$

for some complex coefficients a and b , such that $|a|^2 + |b|^2 = 1$, where $|\Xi_{w-1}\rangle$ and $|\Xi_{w-2}\rangle$ are states such that, for $j = 0, 1, \dots, t$,

$$|\Xi_j\rangle \propto \sum_h \frac{\alpha_{j,h}}{\sqrt{2}} |S_j^t\rangle |c_h\rangle. \quad (77)$$

We have (using covariance to get $E_{w,\pi}$)

$$E_{w,0} + E_{w,\pi} \quad (78)$$

$$= 2(|a|^2 |\Xi_{w-1}\rangle |0\rangle \langle \Xi_{w-1}| \langle 0| + |b|^2 |\Xi_{w-2}\rangle |1\rangle \langle \Xi_{w-2}| \langle 1|). \quad (79)$$

But

$$E_{w,0} + E_{w,\pi} \quad (80)$$

$$= I_{\text{sp}(\mathcal{O}_w)} \quad (81)$$

$$= |\Xi_{w-1}\rangle |0\rangle \langle \Xi_{w-1}| \langle 0| + |\Xi_{w-2}\rangle |1\rangle \langle \Xi_{w-2}| \langle 1|. \quad (82)$$

Equating the two expressions implies that

$$|\eta_w\rangle = \frac{1}{\sqrt{2}} (|\Xi_{w-1}\rangle |0\rangle + e^{i\varphi_w} |\Xi_{w-2}\rangle |1\rangle), \quad (83)$$

for some phase φ_w . But we must have $\varphi_w = 0$ since $E_{w,0}$ corresponds to the guess “ $\theta = 0$ ”.

$w = t + 2$:

Similar to the case $w = 1$ and using the definition from Eq. (77), we have $E_{t+2,0} = E_{t+2,\pi} = |\Xi_t\rangle |1\rangle \langle \Xi_t| \langle 1|$. We assign the guess “ $\theta = \pi$ ” to getting the outcome corresponding to this POVM element.

To summarize, the elements of the overall POVM $\{E_0, E_\pi\}$ describing the measuring-and-guessing strategy may be expressed

$$E_0 = |\Xi_0\rangle |0\rangle \langle \Xi_0| \langle 0| + \sum_{w=2}^{t+1} |w, +\rangle \langle w, +| \quad (84)$$

$$E_\pi = \sum_{w=2}^{t+1} |w, -\rangle \langle w, -| + |\Xi_t\rangle |1\rangle \langle \Xi_t| \langle 1|, \quad (85)$$

where

$$|w, \pm\rangle \equiv \frac{1}{\sqrt{2}} (|\Xi_{w-1}\rangle |0\rangle \pm |\Xi_{w-2}\rangle |1\rangle). \quad (86)$$

A.3 Proof of Theorem 1, Assuming Eq. (15)

For security with error ϵ , we require

$$r(1 - c/(2r + 1)^2)^s < \epsilon, \quad (87)$$

which, by taking the logarithm of both sides, is equivalent to

$$s > \log(\epsilon/r) / \log(1 - c/(2r + 1)^2). \quad (88)$$

Using the series expansion $\log(1-x) = -(x + x^2/2 + x^3/3 + \dots)$, the right-hand side of Eq. (88) is upper-bounded by

$$(2r+1)^2 \log(r/\epsilon)/c, \quad (89)$$

from which the theorem follows.

A.4 Proof of Proposition 4

This maximization problem is very similar to that in Ref. [11], where it was required to maximize $\langle \zeta | M'_t | \zeta \rangle$ over all states $|\zeta\rangle \in \text{sp}\{|j\rangle : j = 0, 1, \dots, t\}$ for

$$M'_t = \sum_{j=0}^{t-1} |j+1\rangle\langle j| + |j\rangle\langle j+1|. \quad (90)$$

In fact, in light of Eq. (40), the phase estimation problem in Ref. [11] may be viewed as the same as the one we consider, but where Eve does not have access to the register R' . (Indeed, our optimal success probability cannot be less than that in Ref. [11], since at the very least Eve can forgo the use of the ancillary register R' .) Finally, below, we show that our optimal success probability is exactly equal to that obtained in Ref. [11].

Let $\alpha_{j,h}^*$ denote the optimal values for our maximization problem, and let M_t^* , $|\psi_R(0)^*\rangle$, and $|\Xi_j^*\rangle$ denote the values of M_t , $|\psi_R(0)\rangle$, and $|\Xi_j\rangle$ at those optimal values. Note that $\{|\Xi_j\rangle : j = 0, 1, \dots, t\}$ is orthonormal for all values of $\alpha_{j,h}$, thus $\{|\Xi_j^*\rangle : j = 0, 1, \dots, t\}$ is orthonormal. Consider now optimizing $\langle \psi | M_t^* | \psi \rangle$ over all unit vectors $|\psi\rangle \in \text{sp}\{|\Xi_j^*\rangle : j = 0, 1, \dots, t\}$ for fixed M_t^* ; denote the optimal $|\psi\rangle$ as $|\psi^*\rangle$. It must be that

$$\langle \psi^* | M_t^* | \psi^* \rangle \geq \langle \psi_R(0)^* | M_t^* | \psi_R(0)^* \rangle, \quad (91)$$

since $|\psi_R(0)^*\rangle \in \text{sp}\{|\Xi_j^*\rangle : j = 0, 1, \dots, t\}$ by inspecting Eqs. (67) and (77). Now note that the coefficients of $|\psi^*\rangle$ with respect to the basis $\{|\Xi_j^*\rangle : j = 0, 1, \dots, t\}$ must be precisely those coefficients of the optimal $|\zeta\rangle$ with respect to the standard orthonormal basis $\{|j\rangle : j = 0, 1, \dots, t\}$ found in Ref. [11]; otherwise, substituting the coefficients of $|\psi^*\rangle$ would give a higher maximum than that in Ref. [11]. (The argument works because, in both cases, the orthonormal basis is fixed for the optimization.) Therefore, we have, as in Ref. [11],

$$|\psi^*\rangle \propto \sum_{j=0}^t \sin \left[\frac{(j+1)\pi}{t+2} \right] |\Xi_j^*\rangle. \quad (92)$$

References

1. Menezes, A.J., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press LLC, Boca Raton (1996)

2. Gottesman, D., Chuang, I.L.: Quantum Digital Signatures (2001). [quant-ph/0105032](http://arxiv.org/abs/quant-ph/0105032)
3. Lamport, L.: Constructing digital signatures from a one-way function. CSL 98, SRI International (1979)
4. Kawachi, A., Koshihara, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 268–284. Springer, Heidelberg (2005). <http://arxiv.org/abs/quant-ph/0403069>
5. Hayashi, M., Kawachi, A., Kobayashi, H.: Quantum measurements for hidden subgroup problems with optimal sample complexity. *Quantum Inf. Comput.* **8**, 0345–0358 (2008)
6. Ioannou, L.M., Mosca, M.: Public-key cryptography based on bounded quantum reference frames. <http://arxiv.org/abs/0903.5156>
7. Goldreich, O.: Foundations of Cryptography (Volume I): Basic Tools. Cambridge University Press, Cambridge (2001)
8. Chaum, D., Roijakkers, S.: Unconditionally secure digital signatures. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 206–214. Springer, Heidelberg (1991)
9. Gottesman, D.: Quantum public key cryptography with information-theoretic security. Workshop on classical and quantum information security, Caltech, 15–18 December 2005. <http://www.cpi.caltech.edu/quantum-security/program.html>; see also <http://www.perimeterinstitute.ca/personal/dgottesman>
10. Damgaard, I., Fehr, S., Salvail, L., Schaffner, C.: Secure identification and QKD in the bounded-quantum-storage model. CRYPTO 2007 **4622**, 342–359 (2007)
11. Bartlett, S.D., Rudolph, T., Spekkens, R.W., Turner, P.S.: Degradation of a quantum reference frame. *New J. Phys.* **8**, 58 (2006)
12. Gutoski, G.: Quantum strategies and local operations. Ph.D. thesis, University of Waterloo (2009)
13. Mittal, R., Szegedy, M.: Product rules in semidefinite programming. In: Csuhaj-Varjú, E., Ésik, Z. (eds.) FCT 2007. LNCS, vol. 4639, pp. 435–445. Springer, Heidelberg (2007)
14. van Dam, W., Mauro D’Ariano, G., Ekert, A., Macchiavello, C., Mosca, M.: Optimal quantum circuits for general phase estimation. *Phys. Rev. Lett.* **98**(9), 090501 (2007)
15. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. In FOCS ’98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science (1998)
16. van Dam, W., Mauro D’Ariano, G., Ekert, A., Macchiavello, C., Mosca, M.: Optimal phase estimation in quantum networks. *J. Phys. A: Math. Theor.* **40**, 7971–7984 (2007)
17. Chiribella, G., D’Ariano, G.M., Sacchi, M.F.: Optimal estimation of group transformations using entanglement. *Phys. Rev. A* **72**(4), 042338 (2005)
18. Watrous, J.: Theory of quantum information. Lecture notes for course CS 789, University of Waterloo, <http://www.cs.uwaterloo.ca/~watrous/> (2008)
19. Cleve, R., Slofstra, W., Unger, F., Upadhyay, S.: Strong parallel repetition theorem for quantum XOR proof systems (2006). [arXiv:quant-ph/0608146v1](http://arxiv.org/abs/quant-ph/0608146v1)
20. Kitaev, A., Watrous, J.: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In STOC ’00: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (2000)

Long Distance Quantum Key Distribution with Continuous Variables

Anthony Leverrier^{1,2}(✉) and Philippe Grangier³

¹ ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels, Barcelona, Spain

² Institut Telecom/Telecom ParisTech, CNRS LTCI, 46, rue Barrault, 75634 Paris Cedex 13, France
`anthony.leverrier@icfo.es`

³ Laboratoire Charles Fabry, Institut d'Optique, CNRS, Univ. Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France

Abstract. We present a continuous-variable quantum key distribution protocol combining a continuous but slightly non-Gaussian modulation together with a efficient reverse reconciliation scheme. We establish the security of this protocol against collective attacks which correspond to a linear quantum channel. In particular, all Gaussian attacks are considered in our framework. We show that this protocol outperforms all known practical protocols, even taking into account finite size effects.

1 Introduction

Quantum key distribution (QKD) is a cryptographic primitive allowing two distant parties, Alice and Bob, to establish a secret key in an untrusted environment controlled by some eavesdropper, Eve [1]. One of the great interests of QKD is that it can be implemented with present day technology, at least for reasonable distances.

Whereas discrete-variable protocols, such as BB84 [2], are quite resistant to losses (experiments over more than 200 km have been achieved [3]), continuous-variable protocols do not seem to display the same quality: the present experimental record is around 25 km [4–7], although recent theoretical results suggest that 100 km should be achievable [8, 9]. On the other hand, continuous-variable (CV) QKD does not require specific equipment such as single-photon counters and can be implemented with off-the-shelf telecom components. For this reason, it is of great importance to find the protocols with the highest resistance to losses. In this paper we introduce such a protocol.

Before describing the new protocol, let us first recall the main ideas of CVQKD, and explain the origin of its sensitivity to losses. The basic idea is to encode information on continuous variables in phase space to perform QKD [10]. This can be achieved with coherent states: the information is simply encoded in their displacement vectors and can be recovered by Bob thanks to homodyne or heterodyne detection (homodyne corresponds to the case where one random quadrature is measured, heterodyne means that both quadratures are

measured). Two main categories of modulation have been considered in the literature: a continuous Gaussian modulation, which maximizes the mutual information I_{AB} between Alice and Bob, and discrete modulations (mainly consisting of either 2 or 4 states) allowing for a simpler reconciliation procedure. In the case where the data are not postselected, both modulation schemes have been proved secure against collective attacks (Refs. [11–13] for a Gaussian modulation, and Refs. [8, 9] for discrete modulations in the case where the quantum channel is linear). Finally, thanks to a de Finetti theorem in infinite-dimensional Hilbert spaces, it is enough to consider collective attacks to prove the general security of a CVQKD scheme [14].

The typical outline of a CV QKD protocol is the following. Alice prepares N coherent states $|q_k + ip_k\rangle$ where q_k and p_k are real random variables following the appropriate probability distribution: q_k, p_k can be either centered normal random variables or Bernoulli random variables depending on the modulation of the protocol. Bob measures each state with a homodyne or a heterodyne detection (in the first case, he needs to inform Alice of his choice of quadrature). At this point, Alice and Bob possess N (or $2N$) couples of correlated data (x_k, y_k) . These data are related through: $y_k = tx_k + z_k$ where t is an unknown constant and z_k is a centered random variable with unknown variance σ^2 . Alice and Bob then proceed with the parameter estimation procedure whose goal is to estimate both t and σ^2 by publicly revealing part of their data [15, 16]. Note that this estimation can never be perfect in practice. The remaining data (x_k, y_k) for $k \in \{1, \dots, n\}$ are used to distill a secret key. This is done by first applying a reverse reconciliation technique [17] where Bob sends some side information to Alice to help her guess the value of (y_1, \dots, y_n) . The side information is typically composed of continuous data, for instance the absolute value $|y_k|$ of Bob's data, as well as of the syndrome of a linear error correcting code (for instance of a Low-density Parity-check (LDPC) code [18, 19]). The reconciliation procedure is characterized by its efficiency β which is the ratio between the length of the bit-string Alice and Bob manage to agree on and the mutual information $I(x; y)$ they initially shared. Finally the privacy amplification allows them to transform this partially unsecure bit-string into a secret key of length $l = nK$ where the asymptotic key rate K is given by:

$$K = \beta I(x; y) - \chi(y; E). \quad (1)$$

Taking into account finite size effects leads to a more complicated expression which can be found elsewhere [15, 16, 20] (see also discussion below). The quantity $\chi(y; E)$ refers to the Holevo information between the eavesdropper and Bob's data. Note that the main contribution to finite size effects comes from the inaccuracy in the parameter estimation: one should indeed consider for $\chi(y; E)$ the maximal value compatible with the estimation except for some small probability ϵ_{PE} , say 10^{-10} .

The main limitation in terms of range for CV QKD stems from the finite reconciliation efficiency, especially for a Gaussian modulation in the low signal-to-noise ratio (SNR) regime. Using a discrete quaternary modulation improves

the performances significantly as one is now able to perform an efficient reconciliation, even for arbitrarily low SNR [8, 9]. On the other hand, upper bounding the Holevo quantity is more challenging in this scenario, and tight bounds are only available when the modulation variance is small. The reason for it is that the bounds are obtained from an optimality property of Gaussian states [11, 21], and that the four-state protocol is close to a Gaussian protocol for low modulation variance only (typically the optimal variance corresponds to sending coherent states with a mean photon number between 0.2 and 0.5). While this is perfectly fine in theory, it certainly makes the experimental implementation more challenging.

In this paper, we introduce a new continuous-variable QKD protocol combining an efficient reconciliation procedure and a much tighter bound on $\chi(y; E)$. This protocol outperforms all known practical CV QKD protocols, both in terms of rate and achievable range. It also allows for larger modulation variances, hence significantly simplifying the experimental implementation for long distances. We will establish the security of this protocol against linear attacks (for instance Gaussian attacks) in the asymptotic regime. By definition, a linear attack corresponds to any action of the eavesdropper compatible with a linear quantum channel between Alice and Bob (see Appendix A for details concerning linear channels). The general case of collective attacks will be treated elsewhere [22]. In order to show the robustness of the protocol, we will also present its performances in a non-asymptotic regime, where the imperfect parameter estimation is taken into account using the techniques described in Refs. [15, 16].

2 A New Modulation Scheme

Let us first say a few words concerning the reconciliation procedure. A necessary condition in order to achieve long distances is to be able to have an efficient reconciliation at low SNR. The main difficulty here lies in the fact that we need a reverse reconciliation. Indeed, the side information sent by Bob must help Alice without giving Eve any relevant information. The only schemes where side information seems to have these properties are the Gaussian modulation where side information describes rotations in \mathbb{R}^8 [23] and the binary and quaternary modulations where side information consists of the absolute value of Bob's measurement result [8].

In order to increase the secret key rate, one needs to find the best possible balance between a large value of $\beta I(x; y)$ and a small value of $\chi(y; E)$. From this perspective, the protocol with a Gaussian modulation and the four-state protocol appear to be at the two ends of the spectrum. A Gaussian modulation, on one hand, insures the lowest possible value for the upper bound on $\chi(y; E)$, but unfortunately, the quantity $\beta I(x; y)$ is also quite small, and one cannot distill secret keys over large distances with this protocol. The 4-state protocol, on the other hand, is designed specifically to maximize the quantity $\beta I(x; y)$ at the cost of increasing the provable upper-bound on $\chi(y; E)$, which is a consequence of the fact that a quaternary modulation only roughly approximates a genuine Gaussian modulation for low modulation variances.

The idea of the protocol presented here is to combine these two solutions to find a better trade-off. The modulation scheme now consists in generating points centered on an 7-dimensional sphere in \mathbb{R}^8 (this is done by considering together 4 successive coherent states in phase space). Then, using the same technique as in Ref. [23], one can reduce the reconciliation problem to the discrete case, which can be efficiently solved as in Ref. [8]. However, because the continuous modulation on a sphere in \mathbb{R}^8 approximates a Gaussian modulation quite accurately, the bound on $\chi(y; E)$ becomes much tighter than for the four-state protocol.

We now give a detailed description of our new protocol. Alice sends $4N$ coherent states to Bob such that the coordinates of all quadruples $\{|\alpha_{4k}\rangle, |\alpha_{4k+1}\rangle, |\alpha_{4k+2}\rangle, |\alpha_{4k+3}\rangle\}$ for $k \in \{1, \dots, N\}$ are drawn with the uniform probability on the seven-dimensional sphere of radius 2α in phase space¹:

$$\mathcal{S}^7 \equiv \{(\alpha_{4k}, \alpha_{4k+1}, \alpha_{4k+2}, \alpha_{4k+3}) \in \mathbb{C}^4 \text{ such that } |\alpha_{4k}|^2 + |\alpha_{4k+1}|^2 + |\alpha_{4k+2}|^2 + |\alpha_{4k+3}|^2 = 4\alpha^2\}. \quad (2)$$

α is related to Alice's modulation variance V_A through $V_A = 2\alpha^2$ (expressed in shot noise units). Then Bob proceeds with an *heterodyne measurement* (as in Ref. [24] for instance). Here, it is crucial that both quadratures are measured in order to use the property of Eq. 2. The parameter estimation procedure now consists in revealing $N - n$ quadruples in order to estimate the parameters t and σ^2 as before. Then, the reconciliation procedure is a mix between the reconciliation using the octonions presented in Ref. [23] and the one described in Ref. [8] using the concatenation of good error correcting codes with a repetition code in order to be able to work at very low SNR. It goes as follows. Bob first puts together his n 8-dimensional real vectors $\mathbf{y}^k = (y_1^k, \dots, y_8^k)$ and chooses randomly n 8-bit strings (u_1^k, \dots, u_8^k) . These 8-bit strings are mapped on points on a hypercube in \mathbb{R}^8 with coordinates $\mathbf{u}^k = ((-1)^{u_1^k} \frac{\|\mathbf{y}^k\|}{2\sqrt{2}}, \dots, (-1)^{u_8^k} \frac{\|\mathbf{y}^k\|}{2\sqrt{2}})$ where $\|\mathbf{y}^k\|^2 = (y_1^k)^2 + \dots + (y_8^k)^2$. He then computes the n rotations in \mathbb{R}^8 mapping \mathbf{y}^k to \mathbf{u}^k as described in Ref. [23] and sends them, together with the value of $\|\mathbf{y}^k\|$ to Alice on the authenticated classical channel. Alice applies the same n rotations to her data. At this point, Bob computes the syndrome of his $8n$ -bit string for a code C he and Alice agreed on beforehand and sends this syndrome to Alice. This syndrome defines a subset of the $8n$ -dimensional hypercube containing the point $(\mathbf{u}^1, \dots, \mathbf{u}^n)$. If the code C is well chosen, with high probability, Alice recovers the value of $(u_1^k, u_2^k, \dots, u_n^k)$. The efficiency of this procedure is the same as the one of the reconciliation of 4-state protocol. Alice and Bob can then proceed with privacy amplification to obtain their secret key.

3 Performance and Security of the Protocol

Our goal here is to evaluate the secret key rate K . The first term $\beta I(x; y)$ is rather easy to estimate. Because of the specific reconciliation procedure, β is the

¹ This can be done quite simply: Alice only needs to draw eight random variable with a normal probability distribution and then to normalize this eight dimensional vector so that it belongs to the sphere \mathcal{S}^7 of radius 2α in \mathbb{R}^8 .

same as for the discrete-modulation protocol, and can be assumed to be at least 0.8 for any SNR lower than 1 [8]. The mutual information between Alice and Bob corresponds to the capacity of a binary input additive white Gaussian noise channel, which is a function of the SNR.

In order to upper bound $\chi(y; E)$, one needs to consider the entanglement-based version of the protocol. Such a “virtual entanglement” does not have to be implemented, but it is formally equivalent to the used prepare-and-measure protocol. In this version, Alice starts by preparing n bipartite states

$$|\Psi\rangle = e^{-2\alpha^2} \sum_{k=0}^{\infty} \frac{(2\alpha)^k}{\sqrt{k!}} |\psi_k^4\rangle, \quad (3)$$

where

$$|\psi_k^4\rangle = \frac{1}{\sqrt{\binom{k+3}{3}}} \sum_{\sum_i k_i=k} |k_1, k_2, k_3, k_4\rangle |k_1, k_2, k_3, k_4\rangle$$

and performs a POVM on the first half of her state which projects the second half on the coherent states with the right modulation. These coherent states are then sent to Bob. The covariance matrices of this state $|\Psi\rangle$ respectively before and after the transmission through a *linear* channel of transmission T and excess noise ξ are noted $\Gamma^0 \otimes \mathbb{1}_4$ and $\Gamma \otimes \mathbb{1}_4$ with

$$\Gamma^0 = \begin{pmatrix} (V_A + 1)\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & (V_A + 1)\mathbb{1}_2 \end{pmatrix}, \Gamma = \begin{pmatrix} (V_A + 1)\mathbb{1}_2 & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & (1 + TV_A + T\xi)\mathbb{1}_2 \end{pmatrix}$$

where $V_A = 2\alpha^2$ is Alice’s modulation variance in the Prepare and Measure version of the protocol. The parameter Z characterizes the level of correlation in phase space between the two halves of the states. The maximal value of Z compatible with quantum mechanics is obtained in the case of a two-mode squeezed state and reads $Z_{\text{TMS}} = \sqrt{V_A^2 + 2V_A}$. This is therefore the relevant value when considering the QKD protocol with a Gaussian modulation. In the case of the continuous-modulation protocol introduced here, one has [16]:

$$Z = \frac{1}{2} e^{-2V_A} \sum_{k=0}^{\infty} \frac{\sqrt{k+4}}{k!} V_A^{k+\frac{1}{2}}. \quad (4)$$

The fact that $Z < Z_{\text{TMS}}$ leads to an increase of the upper bound on $\chi(y; E)$ one can derive from a Gaussian optimality argument. In particular, the value of $\chi(y; E)$ one obtains corresponds to the value one would obtain for a Gaussian modulation protocol with a quantum channel characterized by a transmission $T_G = T/F \approx T$, and an excess noise $\xi_G = F\xi + (F-1)V_A \approx \xi + (F-1)V_A$, where $F \equiv (Z_{\text{TMS}}/Z)^2$. Since one has $F \approx 1$ for reasonable values of V_A , the main effect of the non-Gaussian modulation is the *equivalent excess noise* $\Delta\xi = (F-1)V_A$. Figure 1 displays this equivalent excess noise in the case of the protocol presented here, as well as for the 4-state protocol introduced in [8]. In state-of-the-art implementation, the excess noise is typically less than a few percent of the shot

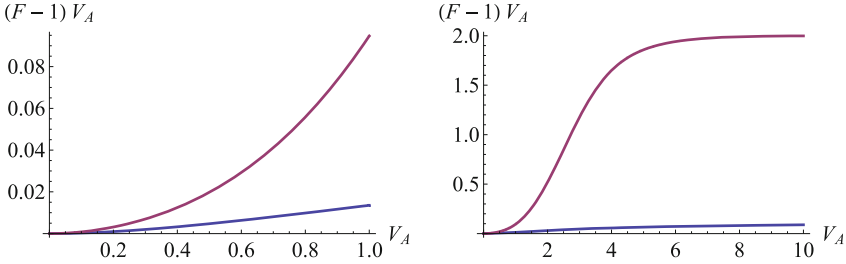


Fig. 1. Equivalent excess noise due to the non-Gaussian modulation. Upper curve refers to the 4-state protocol [8], lower curve to the new continuous-modulation protocol. An excess noise of one unit of shot noise corresponds to an entanglement-breaking channel, therefore no security is possible with such a level of noise.

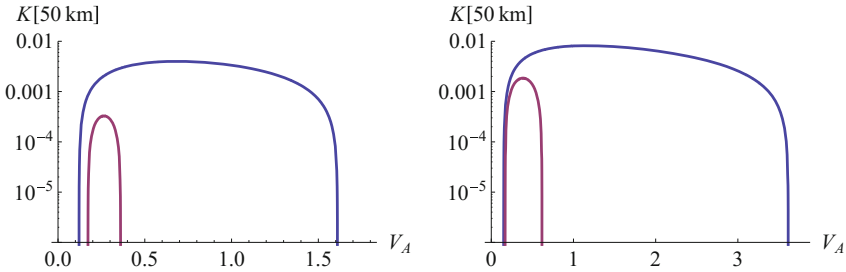


Fig. 2. Asymptotic secret key rate for the new protocol and the four-state protocol (heterodyne detection) for a distance of 50 km, as a function of Alice’s modulation variance. The various parameters are an excess noise of 0.01 and quantum efficiency of the detectors is $\eta = 60\%$. Reconciliation efficiency is supposed to be a conservative 80% on the left figure, and an optimistic 90% on the right figure.

noise. This gives a approximate limit for the value of the equivalent excess noise that is acceptable. In particular, for the 4-state protocol, one needs to work with modulation variances below 0.5 units of shot noise. On the contrary, it becomes possible to work with much higher variances in the case of our new protocol.

This can be seen on Fig. 2 where we display the asymptotic secret key rate for a distance of 50 km for the new protocol as well as for the 4-state protocol as a function of Alice’s modulation variance. The various parameters are chosen conservatively: a quantum efficiency of 60% and an excess noise of 0.01. Both plots correspond respectively to a reconciliation efficiency of 80% and a more optimistic value of 90%. The superiority of the new protocol is quite clear: the secret key rate is higher by nearly an order of magnitude, and one can work with significantly larger modulation variances.

In order to confirm the robustness of the new protocol, we display on Fig. 3 the secret key rate when finite size effects are taken into account. The secret key rate is computed against collective attacks, as detailed in Ref. [15]. Among various finite size effects [20], the most crucial ones for continuous-variable protocols are clearly the imperfect reconciliation efficiency (which prevents the protocol

with a Gaussian modulation to achieve key distribution over large distances) and the parameter estimation. While the reconciliation efficiency is taken care of by the 8-dimensional continuous modulation, the parameter estimation is quite sensitive for continuous-variable protocols. In fact, the real problem lies in the estimation of the excess noise ξ , which is very small compared to the shot noise, and thus hard to evaluate accurately.

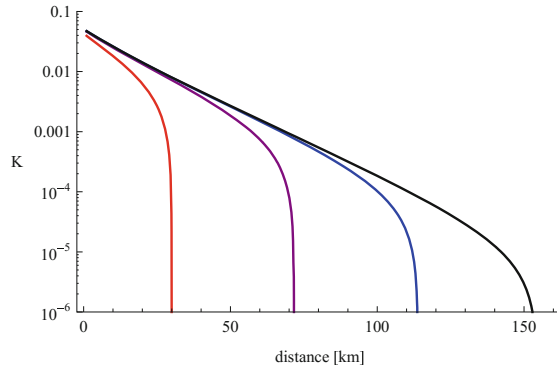


Fig. 3. Non-asymptotic secret key rate for the new protocol, obtained for realistic values: excess noise $\xi = 0.005$, security parameter $\epsilon_{\text{PE}} = 10^{-10}$, quantum efficiency of the detectors $\eta = 60\%$, reconciliation efficiency 80% for the bi-AWGN channel. Half the samples are used for parameter estimation. From left to right, the block length is equal to 10^8 , 10^{10} , 10^{12} and 10^{14} .

In Fig. 3, all such finite size effects are taken into account [15]. The results are rather pessimistic, but remember that this is also true for all discrete-variable protocols [25], and our protocol performs relatively quite well. While exchanging 10^{14} quantum signals is rather unrealistic, exchanging 10^8 or even 10^{10} signals can be done with today's technology. Hence, our new protocol allows for the distribution of secret keys over distances of the order of 50 km, taking into account all finite-size effects.

4 Perspectives

As a conclusion, we presented a new continuous-variable QKD protocol based on a continuous but non-Gaussian modulation and established its security against collective attacks, provided that the quantum channel is linear. The use of a specific reconciliation procedure allows for the distribution of secrets keys over long distances, which was impossible with a Gaussian modulation. Moreover, this protocol clearly outperforms all known practical continuous-variable, with a secret key rate an order of magnitude higher than for the four-state protocol.

An important question at that stage is how to avoid the extra hypothesis that the channel should be linear. As shown in Ref. [22], this can be done by using decoy states, in order to embed the non-Gaussian modulation into an overall gaussian modulation. It is then safe to evaluate the values of T and ξ from a gaussian probe beam, and then to use them as described in the present paper.

Acknowledgments. We acknowledge support from the European Union under project SECOQC (IST-2002-506813) and the ERC Starting grant PERCENT, and from Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05) and SEQUIRE (ANR-07-SESU-011-01).

A Appendix: Linear Quantum Channels

We shall define a linear quantum channel by the input-output relations of the quadrature operators in Heisenberg representation :

$$\begin{aligned} X_{out} &= g_X X_{in} + B_X \\ P_{out} &= g_P P_{in} + B_P \end{aligned} \quad (5)$$

where the added noises B_X , B_P are uncorrelated with the input quadratures X_{in} , P_{in} . Such relations have been extensively used for instance in the context of Quantum Non-Demolition (QND) measurements of continuous variables [26], and they are closely related to the linearized approximation commonly used in quantum optics. Gaussian channels (channels that preserve the Gaussianity of the states) are usual examples of linear quantum channels. However, linear quantum channels may also be non-Gaussian, this will be the case for instance if the added noises B_X , B_P are non-Gaussian.

For our purpose, the main advantage of a linear quantum channel is that it will be characterized by transmission coefficients $T_X = g_X^2$, $T_P = g_P^2$, and by the variances of the added noises B_X and B_P . These quantities can be determined even if the modulation used by Alice is non-Gaussian, with the same measured values as when the modulation is Gaussian (because these values are intrinsic properties of the channel). The relevant covariance matrix can then be easily determined, and Eve's information can be bounded by using the Gaussian optimality theorem.


References

1. Scarani, V., et al.: The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**(3), 1301–1350 (2009)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, vol. 175 (1984)
3. Stucki, D., et al.: High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11**(7), 075003 (2009)

4. Qi, B., Huang, L.L., Qian, L., Lo, H.K.: Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **76**(5), 052323 (2007)
5. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tualle-Brouri, R., McLaughlin, S.W., Grangier, P.: Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**(4), 042305 (2007)
6. Dinh Xuan, Q., Zhang, Z., Voss, P.L.: A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express* **17**(26), 24244–24249 (2009)
7. Chi, Y.M., Qi, B., Zhu, W., Qian, L., Lo, H.K., Youn, S.H., Lvovsky, A.I., Tian, L.: A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution. *New J. Phys.* **13**(1), 013003 (2011)
8. Leverrier, A., Grangier, P.: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **102**(18), 180504 (2009)
9. Leverrier, A., Grangier, P.: Continuous-variable quantum key distribution protocols with a discrete modulation. Arxiv preprint 1002.4083 (2010)
10. Ralph, T.C.: Continuous variable quantum cryptography. *Phys. Rev. A* **61**(1), 010303(R) (1999)
11. García-Patrón, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**(19), 190503 (2006)
12. Navascués, M., Grosshans, F., Acín, A.: Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**(19), 190502 (2006)
13. Leverrier, A., Grangier, P.: Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A* **81**(6), 062314 (2010)
14. Renner, R., De Cirac, J.I.: Fidelity representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**(11), 110504 (2009)
15. Leverrier, A., Grosshans, F., Grangier, P.: Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**(6), 062343 (2010)
16. Leverrier, A.: Theoretical study of continuous-variable quantum key distribution. Ph.D. thesis, Ecole Nationale Supérieure des Télécommunications (2009)
17. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**(5), 057902 (2002)
18. Richardson, T.J., Shokrollahi, M.A., Urbanke, R.L.: Design of capacity-approaching irregular low-density parity-checkcodes. *IEEE Trans. Inf. Theory* **47**(2), 619–637 (2001)
19. Richardson, T., Urbanke, R.: Multi-edge type LDPC codes. In: Workshop Honoring Prof. Bob McEliece on his 60th Birthday, pp. 24–25 (2002)
20. Scarani, V., Renner, R.: Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100**(20), 200501 (2008)
21. Wolf, M.M., Giedke, G., Cirac, J.I.: Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **96**(8), 080502 (2006)
22. Leverrier, A., Grangier, P.: Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A* **83**(4), 042312 (2011)

23. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., Grangier, P.: Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **77**(4), 042325 (2008)
24. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Quantum cryptography without switching. *Phys. Rev. Lett.* **93**(17), 170504 (2004)
25. Cai, R.Y.Q., Scarani, V.: Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11**(4), 045024 (2009)
26. Grangier, P., Levenson, J.A., Poizat, J.P.: Quantum non-demolition measurements in optics. *Nature* **396**(6711), 537–542 (1998)

Multi-query Quantum Sums

David A. Meyer¹ and James Pommersheim^{1,2}

¹ Department of Mathematics, University of California/San Diego,
La Jolla, CA 92093-0112, USA

`dmeyer@math.ucsd.edu`

² Department of Mathematics, Reed College, Portland, OR 97203, USA
`jamie@reed.edu`

Abstract. PARITY is the problem of determining the parity of a string f of n bits given access to an oracle that responds to a query $x \in \{0, 1, \dots, n-1\}$ with the x^{th} bit of the string, $f(x)$. Classically, n queries are required to succeed with probability greater than $1/2$ (assuming equal prior probabilities for all length n bitstrings), but only $\lceil n/2 \rceil$ quantum queries suffice to determine the parity with probability 1. We consider a generalization to strings f of n elements of \mathbb{Z}_k and the problem of determining $\sum f(x)$. By constructing an explicit algorithm, we show that $n-r$ ($n \geq r \in \mathbb{N}$) *entangled* quantum queries suffice to compute the sum correctly with worst case probability $\min\{\lfloor n/r \rfloor/k, 1\}$. This quantum algorithm utilizes the $n-r$ queries sequentially and adaptively, like Grover's algorithm, but in a different way that is not amplitude amplification.

1 Introduction

PARITY is the oracle (or black-box) problem of determining the parity of an n -bit string by querying positions in the string. Since even a single unqueried bit can change the parity, n classical queries are required to solve this problem with probability 1, assuming all n -bit strings are possible.

When $n = 2$, this is Deutsch's problem [1], for which a single quantum query, used properly, suffices [2]. Beals *et al.* show that in general $\lceil n/2 \rceil$ quantum queries suffice by applying the solution to Deutsch's problem to the bits in pairs [3]. In their algorithm the quantum queries are *independent* of one another—they can be asked in parallel since none depends on the responses of the oracle to the others—and they are also *incoherent*—after each query is processed, the state is measured and the resulting information (the parity of a pair of the bits) is combined classically at the end of the algorithm.

This same independence of multiple queries is a feature of existing multi-query quantum algorithms for abelian [4, 5] and non-abelian (*e.g.*, [6–8]) hidden subgroup problems, which range from incoherent [4, 5] through partially [6, 7] to completely [8] coherent. Grover's quantum search algorithm [9, 10], and quantum (random walk) search algorithms on graphs [11–13] more generally, however, utilize coherent sequences of *adapted* queries—the quantum state is modified by each oracle response before it is returned to the oracle for the next query, so the

queries are not independent. These algorithms all use *amplitude amplification* [14] to adapt their sequential queries.

But amplitude amplification, which identifies an element in the preimage of 1 for some bit-valued function, does not apply to PARITY, nor to its generalization:

SUM. Let $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_k$, where f is accessed *via* an oracle that responds with $f(x)$ when queried about $x \in \mathbb{Z}_n$. Find $\sum_{x \in \mathbb{Z}_n} f(x)$ (modulo k).

As they are for PARITY, $n - 1$ classical queries are *useless* for SUM when f is chosen uniformly at random, *i.e.*, the $1/k$ prior probability of each possible sum is unchanged after the oracle responds to the queries [15]. Our Uselessness Theorem: if $2q$ classical queries are useless, then q quantum queries are useless [15], implies that $\lfloor (n - 1)/2 \rfloor$ quantum queries are therefore useless for SUM. This raises the question of how well we can do using more than a useless number of queries; to answer it we construct an $n - r$ quantum query algorithm that computes the sum correctly with worst case probability $\min\{\lfloor n/r \rfloor/k, 1\}$, for each $1 \leq r \in \mathbb{N}$, and that returns a result that is within $\lfloor kr/2n \rfloor$ of the sum with probability at least $4/\pi^2$. This quantum algorithm utilizes the $n - r$ queries sequentially and adaptively, like quantum search algorithms, but in a different way that is not amplitude amplification.

We motivate the development of our algorithm in the next section by considering the simplest new instances of SUM, computing the sum of 2 or 3 trits. In Sect. 3 we state and prove two basic lemmas and combine them to construct the general algorithm in Sect. 4. We conclude in Sect. 5 by recalling the result of van Dam that strings of n bits can be identified with high probability using $n/2 + O(\sqrt{n})$ queries, and hence any function of them can be computed with at least the same probability [16]. We generalize this result to $k > 2$ and show that, unsurprisingly—since it is designed to do more than just compute the sum of the string values, it gives success probabilities less than those of our algorithm.

2 Sums of Trits

The simplest generalization of Deutsch's problem is to add two trits rather than two bits, *i.e.*, the $n = 2$ and $k = 3$ version of SUM. As with Deutsch's problem, if all possible functions $f : \mathbb{Z}_2 \rightarrow \mathbb{Z}_3$ are equally likely, a single classical query is useless—the prior probabilities of $1/3$ for each value of $\sum f(x)$ are unchanged after a single query—while two classical queries suffice to determine the sum with probability 1. Thus the goal of a quantum algorithm for this problem should be to determine the sum with a single quantum query with probability greater than $1/3$.

PROPOSITION 1. *Using a single quantum query the sum of two trits can be determined with worst case probability $2/3$.*

Before giving the proof we recall some standard notation: We will work in the Hilbert space $\mathbb{C}^n \otimes \mathbb{C}^k$, with computational basis $\{|x\rangle|y\rangle \mid x \in \mathbb{Z}_n, y \in \mathbb{Z}_k\}$. The shift operator acts by $X : |z\rangle \mapsto |z + 1\rangle$ and the oracle acts by $\mathcal{O}_f : |x\rangle|y\rangle \mapsto$

$|x\rangle|y + f(x)\rangle = |x\rangle X^{f(x)}|y\rangle$. Finally, $\omega = e^{2\pi i/k}$, and the Fourier transform on \mathbb{C}^k acts by

$$\mathcal{F} : |y\rangle \mapsto \frac{1}{\sqrt{k}} \sum_{\ell=0}^{k-1} \omega^{\ell y} |\ell\rangle =: |\omega^{-y}\rangle, \quad (1)$$

since $X|\omega^{-y}\rangle = \omega^{-y}|\omega^{-y}\rangle$. These ‘‘Fourier’’ (or ‘‘character’’) basis states will be used to implement the widely useful generalization to dimensions greater than 2 [17–19] of the ‘‘phase kickback trick’’ [2].

To use these states in a quantum algorithm for the two trit problem we might expect simply to query the oracle with a state of the form

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\phi\rangle,$$

where $\phi = \omega^{-y}$ for some $y \in \{1, 2\} \subset \mathbb{Z}_3$, as if we were solving Deutsch’s problem. Notice, however, that the relative phase of the two components in the state returned by the oracle would be $\phi^{f(0)-f(1)}$, so it would not encode the sum $f(0) + f(1)$, unlike the two bit case in which $-f(1) \equiv f(1) \pmod{2}$. A different query state is required:

Proof (of Proposition 1). It suffices to exhibit a single query algorithm that succeeds with probability $2/3$.

0. Initialize to the state

$$\frac{1}{\sqrt{2}}(|1\rangle|\omega^1\rangle + |0\rangle|\omega^{-1}\rangle). \quad (2)$$

1. Call the oracle \mathcal{O}_f to obtain the state

$$\frac{1}{\sqrt{2}}(\omega^{f(1)}|1\rangle|\omega^1\rangle + \omega^{-f(0)}|0\rangle|\omega^{-1}\rangle).$$

Notice that the relative phase of the two terms is $\omega^{f(0)+f(1)}$. We could argue at this point that there is a POVM that identifies which of the three possible states we have with probability $2/3$ [20], but as a simple sequence of unitary transformations avoids the necessity for anything beyond a complete von Neumann measurement in the computational basis, we describe it explicitly in the following steps.

2. Act by $X \otimes I$ to obtain the state

$$\frac{1}{\sqrt{2}}(\omega^{f(1)}|0\rangle|\omega^1\rangle + \omega^{-f(0)}|1\rangle|\omega^{-1}\rangle).$$

3. Act by K to obtain the state

$$\frac{1}{\sqrt{2}}|0\rangle(\omega^{f(1)}|\omega^1\rangle + \omega^{-f(0)}|\omega^0\rangle), \quad (3)$$

where K acts on $\mathbb{C}^n \otimes \mathbb{C}^k$ by

$$K : |x\rangle|\omega^y\rangle = \begin{cases} |0\rangle|\omega^0\rangle & \text{if } x = n - 1 \text{ and } y = k - 1; \\ |n - 1\rangle|\omega^{k-1}\rangle & \text{if } x = 0 \text{ and } y = 0; \\ |x\rangle|\omega^y\rangle & \text{otherwise.} \end{cases}$$

Note that while K is a complicated unitary operation, it is independent of f , *i.e.*, it does not call the oracle.

The \mathbb{C}^3 tensor factor in the final state (3) can be rewritten as:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(\omega^{f(1)}|\omega^1\rangle + \omega^{-f(0)}|\omega^0\rangle) \\ &= \omega^{-f(0)} \frac{1}{\sqrt{2}}(\omega^{\Sigma f}|\omega^1\rangle + |\omega^0\rangle) \\ &= \omega^{-f(0)} \frac{1}{\sqrt{6}}\left((1 + \omega^{\Sigma f})|0\rangle + (1 + \omega^{\Sigma f-1})|1\rangle + (1 + \omega^{\Sigma f-2})|2\rangle\right), \end{aligned} \tag{4}$$

using the Definition (1), so now measurement of the \mathbb{C}^3 tensor factor will return $\sum f(x)$ with probability $2/3$. ■

To obtain this probability our initial query (2) was an *entangled* state, rather than the usual tensor product state; this is the first innovation in the algorithm up to which we are building. The next step is to consider adding $n = 3$ trits. In this case two classical queries are useless, so one quantum query is useless [15], and we must consider algorithms with two coherent quantum queries.

PROPOSITION 2. *Two quantum queries suffice to solve SUM with probability 1 when $n = k = 3$.*

Proof. It suffices to exhibit a two query algorithm that succeeds with probability 1.

0. Initialize to the entangled state

$$\frac{1}{\sqrt{3}}(|1\rangle|\omega^1\rangle + |0\rangle|\omega^{-1}\rangle + |0\rangle|\omega^{-2}\rangle).$$

1. Call the oracle \mathcal{O}_f to obtain the state

$$\frac{1}{\sqrt{3}}(\omega^{f(1)}|1\rangle|\omega^1\rangle + \omega^{-f(0)}|0\rangle|\omega^{-1}\rangle + \omega^{-2f(0)}|0\rangle|\omega^{-2}\rangle).$$

2. Act by $X \otimes I$ to obtain the state

$$\frac{1}{\sqrt{3}}(\omega^{f(1)}|2\rangle|\omega^1\rangle + \omega^{-f(0)}|1\rangle|\omega^{-1}\rangle + \omega^{-2f(0)}|1\rangle|\omega^{-2}\rangle).$$

3. Act by J_1 to obtain the state

$$\frac{1}{\sqrt{3}}(\omega^{f(1)}|2\rangle|\omega^2\rangle + \omega^{-f(0)}|2\rangle|\omega^1\rangle + \omega^{-2f(0)}|1\rangle|\omega^{-1}\rangle), \quad (5)$$

where J_r acts on $\mathbb{C}^n \otimes \mathbb{C}^k$ by

$$J_r : |x\rangle|\omega^y\rangle = \begin{cases} |x\rangle|\omega^0\rangle & \text{if } y = 0; \\ |x+r\rangle|\omega^1\rangle & \text{if } y = -1; \\ |x\rangle|\omega^{y+1}\rangle & \text{otherwise.} \end{cases}$$

Note that like K , while J_r is a complicated unitary operation, it is independent of f , *i.e.*, it does not call the oracle.

4. Call the oracle \mathcal{O}_f a second time to obtain the state

$$\frac{1}{\sqrt{3}}(\omega^{f(1)+2f(2)}|2\rangle|\omega^2\rangle + \omega^{-f(0)+f(2)}|2\rangle|\omega^1\rangle + \omega^{-2f(0)-f(1)}|1\rangle|\omega^{-1}\rangle).$$

5. Act by $X \otimes I$ again to obtain the state

$$\frac{1}{\sqrt{3}}(\omega^{f(1)+2f(2)}|0\rangle|\omega^2\rangle + \omega^{-f(0)+f(2)}|0\rangle|\omega^1\rangle + \omega^{-2f(0)-f(1)}|2\rangle|\omega^{-1}\rangle).$$

6. Act by K to obtain the state

$$\frac{1}{\sqrt{3}}|0\rangle(\omega^{f(1)+2f(2)}|\omega^2\rangle + \omega^{-f(0)+f(2)}|\omega^1\rangle + \omega^{-2f(0)-f(1)}|\omega^0\rangle). \quad (6)$$

The \mathbb{C}^3 tensor factor in the final state (6) can be rewritten as:

$$\begin{aligned} & \frac{1}{\sqrt{3}}(\omega^{f(1)+2f(2)}|\omega^2\rangle + \omega^{-f(0)+f(2)}|\omega^1\rangle + \omega^{-2f(0)-f(1)}|\omega^0\rangle) \\ &= \frac{1}{\sqrt{3}}\omega^{f(0)+2f(1)}(\omega^{-\Sigma f}|\omega^2\rangle + \omega^{-2\Sigma f}|\omega^1\rangle + \omega^{-3\Sigma f}|\omega^0\rangle) \\ &= \omega^{f(0)+2f(1)}|\Sigma f\rangle, \end{aligned} \quad (7)$$

using the Definition (1), so now measurement of this tensor factor will return $\sum f(x)$ with probability 1. \blacksquare

The key piece of algebra is that the phases of the terms in (6), each a linear combination of two values of f , are also linear combinations of all *three* values of f , with a coefficient of 0 in front of the third value: $(0, 1, 2) \cdot \mathbf{f}$, $(-1, 0, 1) \cdot \mathbf{f} = (2, 0, 1) \cdot \mathbf{f}$, and $(-2, -1, 0) \cdot \mathbf{f} = (1, 2, 0) \cdot \mathbf{f}$, where $\mathbf{f} = (f(0), f(1), f(2))$. Written this way it is clear that the coefficient vectors are successive cyclic shifts σ of $(0, 1, 2)$, so if we factor out the last phase factor the other two become:

$$\begin{aligned} (0, 1, 2) \cdot \mathbf{f} - \sigma^2(0, 1, 2) \cdot \mathbf{f} &= (2, 2, 2) \cdot \mathbf{f} = -\sum f \\ \sigma(0, 1, 2) \cdot \mathbf{f} - \sigma^2(0, 1, 2) \cdot \mathbf{f} &= \sigma(1, 1, 1) \cdot \mathbf{f} = -2\sum f, \end{aligned}$$

the phases of the first two terms in (7).

This algorithm is optimal since it uses only one more than the useless number of quantum queries. Notice that its two coherent quantum queries are *sequential* rather than parallel, and that the second query is *adapted* in the sense that the state (5) that is passed to the oracle as the second query depends on the response of the oracle to the first query, unitarily transformed by $J(X \otimes I)$. This adaptation differs from amplitude amplification [14] and is the second innovation in our quantum summation algorithm.

3 Two Basic Lemmas

To generalize the quantum algorithms given in the previous section for summing trits, it is convenient first to state two basic lemmas.

LEMMA 3. For $A \in \mathbb{Z}_k$ and $k \geq s \in \mathbb{N}$, let

$$|A_s\rangle = \frac{1}{\sqrt{s}} \sum_{\ell=1}^s \omega^{-\ell A} |\omega^{s-\ell}\rangle \in \mathbb{C}^k. \tag{8}$$

Measurement of $|A_s\rangle$ in the computational basis returns $|y\rangle, y \in \mathbb{Z}_k$, with probability

$$|\langle y|A_s\rangle|^2 = \frac{1}{sk} \left(\frac{\sin \pi s(y-A)/k}{\sin \pi(y-A)/k} \right)^2, \tag{9}$$

defined to be a continuous function of $y - A$. The probability $|\langle y|A_s\rangle|^2$ takes its maximum value, s/k , at $y = A$, and the probability that the measurement is within $\pm[k/2s]$ of A is at least $4/\pi^2$.

Proof. This is an elementary (and familiar from phase estimation; see, e.g., [2]) calculation using the Definition (1):

$$\begin{aligned} \langle y|A_s\rangle &= \frac{1}{\sqrt{sk}} \sum_{\ell=1}^s \omega^{-\ell A - (s-\ell)y} \\ &= \frac{1}{\sqrt{sk}} \omega^{-sy} \sum_{\ell=1}^s \omega^{\ell(y-A)} \\ &= \frac{1}{\sqrt{sk}} \omega^{(1-s)y-A} \frac{1 - \omega^{s(y-A)}}{1 - \omega^{y-A}}. \end{aligned}$$

Taking the norm squared of this expression gives (9), which by continuity takes the value s/k when $y = A$. That this is the maximum follows from the fact that in this case all the terms in the sum above are 1.

Writing $d = y - A$, $|d| \leq k/2s$ implies $|\sin \pi sd/k| \geq |\pi sd/k|/(\pi/2) = 2s|d|/k$, since the argument of \sin has absolute value no more than $\pi/2$. Also, $|\sin \pi d/k| \leq |\pi d/k|$. Using these bounds in (9) gives

$$|\langle A + d|A_s\rangle|^2 \geq \frac{1}{sk} \left(\frac{2s|d|/k}{|\pi d/k|} \right)^2 = \frac{4}{\pi^2} \frac{s}{k},$$

so

$$\sum_{|d| \leq k/2s} \frac{4}{\pi^2} \frac{s}{k} \geq \left\lceil \frac{k}{s} \right\rceil \cdot \frac{4}{\pi^2} \frac{s}{k} \geq \frac{4}{\pi^2}. \quad \blacksquare$$

When $k = 3 = s$ and $A = \sum f(x)$, the state (8) is equal to the \mathbb{C}^3 tensor factor in the final state of the algorithm in Proposition 2, up to an overall phase. Similarly, in the algorithm of Proposition 1, if rather than factoring out the phase $\omega^{-f(0)}$ in (4), we factor out $\omega^{f(0)+2f(1)}$, we obtain (8) with $k = 3$, $s = 2$, and $A = \sum f(x)$. The success probabilities of 1 and $2/3$ in these two algorithms are the values s/k given by Lemma 3.

When $A = \sum_{x \in \mathbb{Z}_n} f(x)$, each component of the state (8) depends on all of the n values of f . The next lemma says that, up to an overall phase, this state is equivalent to one in which each component depends on fewer than n values of f .

LEMMA 4. *Let $1 \leq r \in \mathbb{N}$, let $r|n$, and let $s = n/r$. Then*

$$\begin{aligned} \omega^{\sum_{m=1}^s m[f((m-1)r + \dots + f(mr-1)]} & \frac{1}{\sqrt{s}} \sum_{\ell=1}^s \omega^{-\ell \Sigma f} |\omega^{s-\ell}\rangle \\ & = \frac{1}{\sqrt{s}} \sum_{\ell=1}^s \omega^{\sum_{m=1}^s (m-\ell)[f((m-1)r + \dots + f(mr-1)]} |\omega^{s-\ell}\rangle. \end{aligned}$$

For each value of ℓ , namely for each component, in the sum on the right hand side of this equation, there is a term in the sum in the exponent which vanishes because $m = \ell$. Since each of these terms depends on r values of f , each component depends on $sr - r = n - r$ values of f . In the algorithm of Proposition 1, $n = 2$ and $r = 1$ so $s = n/r = 2$, and each component of the final state (3) depends on $n - r = 2 - 1 = 1$ value of f . In the algorithm of Proposition 2, $n = 3$ and $r = 1$ so $s = n/r = 3$, and each component of the final state (6) depends on $n - r = 3 - 1 = 2$ values of f .

4 The General SUM Problem

Summing two and three trits are special cases of the general SUM problem that motivate the two innovations in our general algorithm. Propositions 1 and 2 are special cases of the following theorem.

THEOREM 5. *Let $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_k$. Using $n - r$ quantum queries the sum $\sum_{x \in \mathbb{Z}_k} f(x)$ can be computed correctly with worst case probability $\min\{\lfloor n/r \rfloor / k, 1\}$, for each $n \geq r \in \mathbb{N}$. Furthermore, the same algorithm outputs a result within $\lfloor kr/2n \rfloor$ of the correct sum with probability at least $4/\pi^2$.*

Proof. First consider the case $r|n$ and let $s = n/r \in \mathbb{N}$. If $s \leq k$ and we can construct the state

$$\frac{1}{\sqrt{s}} \sum_{\ell=1}^s \omega^{-\ell \Sigma f} |\omega^{s-\ell}\rangle,$$

then by Lemma 3 we can find $\sum f(x)$ with probability $s/k = n/(rk)$, and even when the output is wrong, it is likely to be close—within $\lfloor rk/2n \rfloor$ with probability at least $4/\pi^2$. By Lemma 4 we need only construct the state

$$\frac{1}{\sqrt{s}} \sum_{\ell=1}^s \omega^{\sum_{m=1}^s (m-\ell)[f((m-1)r) + \dots + f(mr-1)]} |\omega^{s-\ell}\rangle,$$

in which each component depends on $n - r$ values of f . The following algorithm does so, using $n - r$ quantum queries:

0. Initialize to the entangled state

$$\frac{1}{\sqrt{s}} (|r\rangle|\omega^1\rangle + |0\rangle|\omega^{-1}\rangle + \dots + |0\rangle|\omega^{-(s-1)}\rangle).$$

1. Apply $K(((X \otimes I)\mathcal{O}_f)^r)(J_r((X \otimes I)\mathcal{O}_f)^r)^{s-2}$ to obtain the state

$$\frac{1}{\sqrt{s}} |0\rangle \sum_{\ell=1}^s \omega^{\sum_{m=1}^s (m-\ell)[f((m-1)r) + \dots + f(mr-1)]} |\omega^{s-\ell}\rangle.$$

2. Measure the \mathbb{C}^k tensor factor in the computational basis.

Notice that when $n = k$ and $r = 1$, *i.e.*, using $k - 1$ quantum queries, this algorithm returns $\sum f(x)$ with probability 1.

If $s > k$, or equivalently, if $r < n/k$, then $n = uk + v$ with $u \geq r$ and $0 \leq v < k$, so we can use $k - 1$ queries in this algorithm applied to each block of length k , using a total of $uk - u = n - v - u$ queries, leaving $v + u - r \geq v$ queries to identify the last v values of f . Thus when $s > k$, we can find $\sum f(x)$ with probability 1.

Second, and similarly, if $r \nmid n$, let $s = \lfloor n/r \rfloor$. Then $n = rs + w$ with $0 < w < r$. Using the algorithm applied to the first $n - w$ values of f , we can compute

$$\sum_{x=0}^{rs-1} f(x), \text{ with probability } \min\{1, \lfloor n/r \rfloor/k\},$$

using $n - w - r$ queries, leaving w queries to identify the last w values of f .

Thus in all cases, this algorithm uses $n - r$ quantum queries to return $\sum f(x)$ with probability $\min\{1, \lfloor n/r \rfloor/k\}$, and a value within $\lfloor kr/2n \rfloor$ of the sum with probability at least $4/\pi^2$. ■

We believe this algorithm is optimal, but we have only proved it to be so for $r = n - 1$, *i.e.*, a single query [21].

5 Conclusion

Since the number of queries $n - r \geq 0$, the success probability of our algorithm is always at least $1/k$, as it should be. Furthermore, since $\lfloor n/r \rfloor = 1$ until $r \leq n/2$,

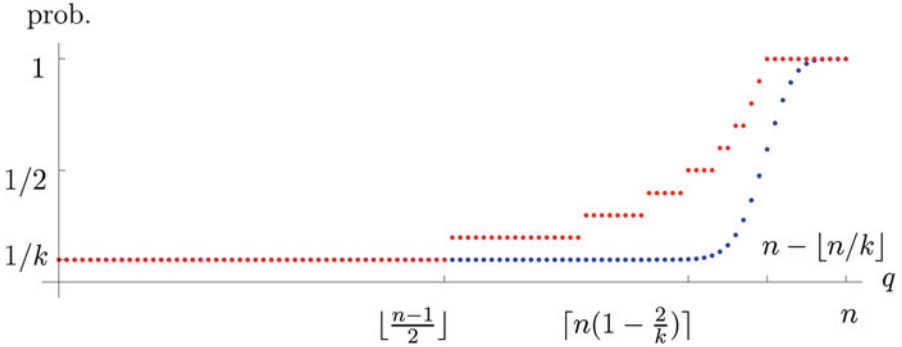


Fig. 1. Success probabilities of the algorithms from Theorems 5 (steps) and 6 (smooth).

fewer than $n/2$ quantum queries in this algorithm are useless, as they must be according to the Uselessness Theorem [15]. When $k = 2$, Theorem 5 says that for $r \leq n/2$ the success probability is 1, as we know from the solution to PARITY [3].

For $k > 2$ we know of no algorithms to which to compare ours. Van Dam’s quantum algorithm for obtaining all the information about a function $\mathbb{Z}_n \rightarrow \mathbb{Z}_2$ with high probability using $n/2 + O(\sqrt{n})$ queries [16], however, can be generalized to functions $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_k$:

THEOREM 6. *Let $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_k$. There is a quantum algorithm using q queries that correctly identifies the function with worst case probability*

$$p_q = \frac{1}{k^n} \sum_{j=0}^q \binom{n}{j} (k - 1)^j. \tag{10}$$

The cumulative distribution function (10) for this binomial probability distribution is greater than 0.95 (almost 0.98) provided $q > n(k-1)/k + 2\sqrt{n(k-1)}/k$, namely the mean plus two standard deviations. Thus with this many queries we can determine the oracle correctly with probability more than 0.95, and thus compute the sum of its values correctly. More precisely, using this algorithm with q queries, we can compute $\sum f(x)$ with probability less than $p_q + (1 - p_q)/k$ (obtained by bounding the probability of computing the sum correctly by $1/k$ when the algorithm fails to output the correct f). Figure 1 plots this upper bound on the success probability as a function of the number of queries, along with the success probability of the algorithm of Theorem 5.

The success probability of the algorithm of Theorem 5 is greater than or equal to that of the generalized van Dam algorithm of Theorem 6, for any number of queries, an unsurprising result since the latter is using those queries to try to determine the whole function, not just its sum. To succeed with probability greater than a constant, the former requires a fraction of n approaching 1 like $1/k$ quantum queries, while the latter requires this many *plus* $O(\sqrt{n})$.

References

1. Deutsch, D.: Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London A* **400**, 97–117 (1985)
2. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. *Proc. Roy. Soc. London A* **454**, 339–354 (1998)
3. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. *J. ACM* **48**, 778–797 (2001)
4. Simon, D.R.: On the power of quantum computation. In: Goldwasser, S. (ed.) *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994, pp. 116–123. IEEE, Los Alamitos, CA (1994)
5. Simon, D.R.: On the power of quantum computation. *SIAM J. Comput.* **26**, 1474–1483 (1997)
6. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.* **35**, 170–188 (2005). [quant-ph/0302112](#)
7. Alagic, G., Moore, C., Russell, A.: Quantum algorithms for Simon’s problem over general groups. In: *Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms*, New Orleans, LA, 7–9 January 2007, pp. 1217–1224. ACM & SIAM, New York & Philadelphia (2007) ([quant-ph/0603251](#))
8. Bacon, D., Childs, A.M., van Dam, W.: From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In: *Proceedings of the 46th Annual Symposium on Foundations of Computer Science*, Pittsburgh, PA, 22–25 October 2005, pp. 469–478. IEEE, Los Alamitos, CA (2005) ([quant-ph/0504083](#))
9. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing*, Philadelphia, PA, 22–24 May 1996, pp. 212–219. ACM, New York (1996)
10. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328 (1997) ([quant-ph/9706033](#))
11. Shenvi, N., Kempe, J., Whaley, K.B.: Quantum random walk search algorithm. *Phys. Rev. A* **67** (2003) 052307/1-11 ([quant-ph/0210064](#))
12. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. In: *Proceedings of the 44th Annual Symposium on Foundations of Computer Science*, Cambridge, MA, 11–14 October 2003, pp. 200–209. IEEE, Los Alamitos, CA (2003) ([quant-ph/0303041](#))
13. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. *Theor. Comput.* **1**, 47–79 (2005)
14. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. In: Lomonaco Jr, S.J., Brandt, H.E. (eds.) *Quantum Computation and Information*, Contemporary Mathematics, vol. 305, pp. 53–74. AMS, Providence, RI (2002) ([quant-ph/0005055](#))
15. Meyer, D.A., Pommersheim, J.: On the uselessness of quantum queries. *Theor. Comput. Sci.* **412**, 7068–7074 (2011) ([arXiv:1004.1434](#), [[quant-ph](#)])
16. van Dam, W.: Quantum oracle interrogation: getting all information for almost half the price. In: *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, Palo Alto, CA, 8–11 November 1998, pp. 362–367. IEEE, Los Alamitos, CA (1998) ([quant-ph/9805006](#))
17. Hunziker, M., Meyer, D.A.: Quantum algorithms for highly structured search problems. *Quantum Inf. Process.* **1**, 145–154 (2002)

18. van Dam, W., Seroussi, G., Efficient quantum algorithms for estimating Gauss sums. *Quantum Inf. Comput.* **14** (2014) 467–492 (quant-ph/0207131)
19. Shakeel, A.: An improved query for the hidden subgroup problem. (arXiv:1101.1053 [quant-ph])
20. Yuen, H.P., Kennedy, R.S., Lax, M.: Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theor.* **IT-21**, 125–134 (1975)
21. Meyer, D.A., Pommersheim, J.: In preparation

Bitwise Quantum Min-Entropy Sampling and New Lower Bounds for Random Access Codes

Jürg Wullschleger^(✉)

DIRO, Université de Montréal, Canada McGill University, Montréal, Canada
juerg@wulli.com

Abstract. *Min-entropy sampling* gives a bound on the min-entropy of a randomly chosen subset of a string, given a bound on the min-entropy of the whole string. König and Renner showed a min-entropy sampling theorem that holds relative to quantum knowledge. Their result achieves the optimal rate, but it can only be applied if the bits are sampled in blocks, and only gives weak bounds for the non-smooth min-entropy.

We give two new quantum min-entropy sampling theorems that do not have the above weaknesses. The first theorem shows that the result by König and Renner also applies to bitwise sampling, and the second theorem gives a strong bound for the non-smooth min-entropy. Our results imply a new lower bound for k -out-of- n random access codes: while previous results by Ben-Aroya, Regev, and de Wolf showed that the decoding probability is exponentially small in k if the storage rate is smaller than 0.7, our results imply that this holds for any storage rate strictly smaller than 1, which is optimal.

1 Introduction

Let two players share a long string $x \in \{0, 1\}^n$, on which an adversary has only partial knowledge. They would like to get a shared key, over which the adversary has almost no knowledge. Since x is long, using a 2-universal hash function or, more generally, a strong extractor would be inefficient and hence impractical. Vadhan showed in [Vad04] that the two players can instead first randomly sample a relatively small substring $x' \in \{0, 1\}^k$ of x , and then apply an extractor to x' . The main part of his proof is a sampling lemma, which shows that with high probability, the string x' will have almost $\frac{t}{n} \cdot k$ bits of min-entropy, if the min-entropy of x is at least t . König and Renner showed in [KR07] that this lemma can be generalized¹ to the setting where the adversary has quantum information about x . Again, with high probability the string x' will have almost $\frac{t}{n} \cdot k$ bits of quantum min-entropy.

Related to these results are lower bounds for *random access codes*. A random access code is an encoding of a message of n classical bits into $m < n$ qubits, such that from these m qubits, k uniformly chosen bits of the message can be guessed with probability at least p . The first lower bound was given for the case

¹ It is however important to note that the results in [KR07] do not converge as fast as in [Vad04]. See also discussion in Sect. 3.

where $k = 1$ by Ambainis, Nayak, Ta-Shma and Vazirani in [ANTSV99]. It was later improved by Nayak in [Nay99] to $m \geq (1 - H(p))n$, where $H(\cdot)$ is the binary entropy function. For the general case where $k \geq 1$, a lower bound was presented by Ben-Aroya, Regev, and de Wolf in [BARdW08]. They showed that for any $\eta > 2 \ln 2$ there exists a constant C_η such that

$$p \leq C_\eta \left(\frac{1}{2} + \frac{1}{2} \sqrt{\frac{\eta m}{n}} \right)^k.$$

This implies that if $m \leq 0.7n$, then $p \leq 2^{-\Omega(k)}$. In the same work they also showed lower bounds for a variant of random access codes called *XOR random access codes*, where the decoder has to guess the XOR of a uniform subset of size k . De and Vidick presented in [DV10] lower bounds for *functional access codes*. They are generalizations of XOR random access codes where the decoder has to guess the output of a function with binary output, where the function is chosen uniformly from a given set.

The result in [Vad04] implies a classical lower bound for k -out-of- n random access codes. In principle, this would also be possible in the quantum setting, as the min-entropy is defined as minus the logarithm of the guessing probability. Unfortunately, the results by König and Renner are not general enough to do that, because they require the sampling to be done in blocks.

1.1 Contributions

In this work we give two new results for quantum min-entropy sampling.

First, we show in Theorems 4 and 5 in Sect. 3 that the bounds given in Corollary 6.19 and Lemma 7.2 in [KR07] also apply to the case where the sample is chosen bitwise, instead of (recursively) in blocks. This result simplifies some protocols² as it eliminates an artificial extra step in which the bits have to be grouped in blocks.

Second, building on previous results given in [BARdW08] and [DV10], in Sect. 4 we prove the following quantum sampling theorem.

Theorem 1. *Let ρ_{XQ} be a state that is classical on $X \in \{0, 1\}^n$. Let T be a uniformly chosen subset of $[n]$ of size k . Then³*

$$H_{\min}(X_T | TQ)_\rho \geq H^{-1} \left(\frac{H_{\min}(X | Q)_\rho}{2n} \right) \frac{k}{6} - 5.$$

Compared with the results in [KR07] and Theorems 4 and 5, Theorem 1 gives stronger bounds for non-smooth min-entropy, but does not achieve the optimal rate⁴. Also note that Theorem 1 only applies to the case where the sample is chosen uniformly, which requires a lot of randomness.

² For example in [KWW09].

³ H_{\min} is defined in Sect. 2.

⁴ Therefore, if we are interested in extracting a key, Theorem 1 only gives better bounds if the sample size is small enough.

Theorem 1 immediately implies the following bound for random access codes.

Corollary 1. *Let $0 < \varepsilon < \frac{1}{2}$. For any k -out-of- n random access code where the code length is bounded by $m \leq (1 - 2H(\varepsilon))n$, the success probability of decoding is at most $2^{-\varepsilon k/6+5}$.*

As the results in [BARdW08], Corollary 1 generalizes the bound given by Nayak to the case where $k \geq 1$. But while the results in [BARdW08] require that $m < 0.7n$, our results imply that the success probability decreases exponentially in k even if m is close to n .

Note that together with Lemma 8 in [BARdW08], Corollary 1 implies a strong lower bound for the one-way communication complexity of k independent instances of the disjointness problem.

2 Preliminaries

The *binary entropy function* is defined as $H(x) := -x \log x - (1-x) \log(1-x)$ for $x \in [0, 1]$, where we use the convention $0 \log 0 = 0$. For $y \in [0, 1]$, let $H^{-1}(y)$ be the value $x \in [0, \frac{1}{2}]$ such that $H(x) = y$. The *Hamming distance* $d_H(\cdot, \cdot)$ between two strings is defined as the number of bits where the two strings disagree. We use the notion $[n] := \{1, \dots, n\}$. The substring of $x \in \{0, 1\}^n$ defined by the set $s \subset [n]$ is denoted by x_s . We call a state ρ_{XQ} a *cq-state* if it is classical on X , which means that it has the form $\rho_{XQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_Q^x$.

The *conditional min-entropy* of a cq-state ρ_{XQ} is defined as

$$H_{\min}(X | Q)_\rho := -\log P_{\text{guess}}(X | Q)_\rho,$$

where

$$P_{\text{guess}}(X | Q)_\rho := \max_{\mathcal{E}} \sum_{x \in \mathcal{X}} P_X(x) \text{tr}(E_x \rho_Q^x).$$

The maximum is taken over all POVMs $\mathcal{E} = \{E_x\}_{x \in \mathcal{X}}$ on \mathcal{Q} . Therefore, $P_{\text{guess}}(X | Q)_\rho$ is the maximal probability to correctly guess X by measuring system Q . The equivalence of this definition of H_{\min} with the definition used in [KR07] has been shown in [KRS09] in Theorem 1.

The *statistical distance* $D(\rho, \phi)$ between two states ρ and ϕ is defined as⁵

$$D(\rho, \phi) := \max_{\mathcal{E}} |\text{tr}(E_1 \rho) - \text{tr}(E_1 \phi)|,$$

where we maximize over all POVMs $\mathcal{E} = \{E_x\}_{x \in \{0,1\}}$. $D(\rho, \phi)$ is therefore the maximal probability to distinguish ρ and ϕ by a measurement. The following lemma shows the connection between the statistical distance and the guessing probability.

Lemma 1. *Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}$ and let τ_X be the fully mixed state. Then $D(\rho_{XQ}, \tau_X \otimes \rho_Q) \leq \varepsilon$ implies that $P_{\text{guess}}(X | Q)_\rho \leq \frac{1}{2} + \varepsilon$.*

⁵ This definition is equivalent to $D(\rho, \phi) := \frac{1}{2} \|\rho - \phi\|_1 = \frac{1}{2} \text{tr}[\sqrt{(\rho - \phi)^\dagger (\rho - \phi)}]$.

Proof. Let us assume that there exists a POVM \mathcal{E} on \mathcal{Q} which can guess X with a probability bigger than $\frac{1}{2} + \varepsilon$. We define a POVM \mathcal{E}' on $\mathcal{X} \otimes \mathcal{Q}$ in the following way: we measure \mathcal{Q} using \mathcal{E} and XOR the output with X . We get $\text{tr}(E'_1 \rho_{XE}) < \frac{1}{2} - \varepsilon$ and $\text{tr}(E'_1(\tau_X \otimes \rho_Q)) = \frac{1}{2}$. It follows that $D(\rho_{XQ}, \tau_X \otimes \rho_Q) > \varepsilon$, which contradicts the assumption. \square

Lemma 2. (Chernoff/Hoeffding). *Let $P_{X_0 \dots X_n} = P_X^n$ be a product distribution with $X_i \in [0, 1]$. Let $X := \frac{1}{n} \sum_{i=0}^{n-1} X_i$, and $\mu = E[X]$. Then, for any $\varepsilon > 0$, $\Pr[X \leq \mu - \varepsilon] \leq e^{-2n\varepsilon^2}$.*

3 Bitwise Sampling from Blockwise Sampling

In this section we show that the min-entropy sampling results from [KR07], which require blockwise sampling, also imply the same bounds for uniform bitwise sampling.

The following theorem is the statement of Corollary 6.19 in [KR07] for uniform blockwise sampling. Here H_{\min}^ε is the *smooth min-entropy*, and H_0 the *Rényi 0-entropy*. The definitions of these entropies and their properties can be found in Sect. 5 in [KR07] or Chap. 3 in [Ren05].

Theorem 2 ([KR07]). *Let ρ_{XQ} be a cq-state where $X = (X_1, \dots, X_n) \in \mathcal{X}^n$. Let $S \subset [n]$ be chosen uniformly at random among all subsets of size r . Assume that $\kappa = \frac{n}{r \log |\mathcal{X}|} \leq 0.15$. Then for any $\xi \in [0, 1]$,*

$$\frac{H_{\min}^\varepsilon(X_S | SQ)}{H_0(X_S)} \geq \frac{H_{\min}(X | Q)}{H_0(X)} - 3\xi - 2\kappa \log 1/\kappa,$$

where $\varepsilon = 2 \cdot 2^{-\xi n \log |\mathcal{X}|} + 3e^{-r\xi^2/8}$.

The statement says that with high probability, the min-entropy rate of a random subset is almost as big as the min-entropy rate of the whole string.

If X is a bit-string, the required condition $n \leq 0.15 \cdot r \log |\mathcal{X}|$ can be achieved by first grouping the bits into blocks. But as pointed out in [BARdW08], even then we need the length of the sampled bit-string to be at least $\Omega(\sqrt{n})$. To overcome this problem, [KR07] proposed a *recursive* application of Theorem 2. The following theorem is Lemma 7.2 in [KR07]. See Section 7 in [KR07] for the definition of the sampling algorithm $\text{ReSamp}(X, f, r, S)$.

Theorem 3 ([KR07]). *Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}^n$. Let n , f and r be such that $n^{(3/4)^f} \geq r^4$. Let S be a string of uniform random bits, and let $Z = \text{ReSamp}(X, f, r, S)$. Then Z is a $n^{(3/4)^f}$ -bit substring of X , with*

$$\frac{H_{\min}^\varepsilon(Z | SQ)}{H_0(Z)} \geq \frac{H_{\min}(X | Q)}{H_0(X)} - 5f \frac{\log r}{r^{1/4}},$$

where $\varepsilon = 5f \cdot 2^{-\sqrt{r}/8}$.

Our results from this section, Theorems 4 and 5, will follow directly from the following lemma.

Lemma 3. *The bounds of Theorems 2 and 3 also apply if the sample is chosen bitwise uniformly.*

Proof. Let $k, n \in \mathbb{N}$, were $k < n$. Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}^n$. Let $S \subset [n]$ be chosen uniformly at random from all subset of size k and let $T \subset [n]$ be a random subset of size k chosen according to a given distribution P_T . Let Π a permutation chosen uniformly at random, but such that it maps all elements in S into T . Strong subadditivity (Theorem 3.2.12 in [Ren05]) implies

$$\begin{aligned} H_{\min}^\varepsilon(X_S | SQ) &\geq H_{\min}^\varepsilon(X_S | S\Pi Q) \\ &= H_{\min}^\varepsilon(\Pi(X)_T | T\Pi Q) . \end{aligned}$$

Note that from (S, Π) it is possible to calculate (T, Π) , and vice-versa. Furthermore, since Π is chosen independent of ρ_{XQ} , we have

$$H_{\min}^\varepsilon(\Pi(X) | \Pi Q) = H_{\min}^\varepsilon(X | \Pi Q) = H_{\min}^\varepsilon(X | Q) .$$

Since S was chosen uniformly and independent of T and ρ_{XQ} , Π is independent of T and ρ_{XQ} . For $Q' := (Q, \Pi)$, we can apply Theorem 2 or 3 to the state $\rho_{\Pi(X)Q'}$. We now choose P_T as the particular sampling required by the theorem and get a bound on $H_{\min}^\varepsilon(\Pi(X)_T | T\Pi Q)$, which then directly implies the same bound for $H_{\min}^\varepsilon(X_S | SQ)$. \square

Theorem 4. *Let $b, r \in \mathbb{N}$. Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}^n$. Let $S \subset [n]$ be chosen uniformly among all subsets of size $k = rb$. Assume that $\kappa = \frac{n}{kb} \leq 0.15$. Then for any constant $\xi \in [0, 1]$,*

$$\frac{H_{\min}^\varepsilon(X_S | SQ)}{H_0(X_S)} \geq \frac{H_{\min}(X | Q)}{H_0(X)} - 3\xi - 2\kappa \log 1/\kappa ,$$

where $\varepsilon = 2 \cdot 2^{-\xi n} + 3e^{-k\xi^2/(8b)}$.

Note that even though we sample bitwise in Theorem 4, the block-size parameter b is still present. It can be chosen depending on the required result: a bigger value b gives a better rate, but results in a slower convergence of the error ε . The best convergence of ε is achieved by choosing $b = \frac{n}{0.15k}$, where we get

$$\varepsilon = 2 \cdot 2^{-\xi n} + 3e^{-k\xi^2/(8b)} = 2 \cdot 2^{-\xi n} + 3e^{-0.15k^2\xi^2/(8n)} .$$

Hence, as mentioned before, we need $k = \Omega(\sqrt{n})$.

Theorem 5. *Let n, f and $r \in \mathbb{N}$ be such that $n^{(3/4)^f} \geq r^4$. Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}^n$. Let $S \subset [n]$ be chosen uniformly among all subsets of size $k = n^{(3/4)^f}$. Then*

$$\frac{H_{\min}^\varepsilon(X_S | SQ)}{H_0(X_S)} \geq \frac{H_{\min}(X | Q)}{H_0(X)} - 5f \frac{\log r}{r^{1/4}} ,$$

where $\varepsilon = 5f \cdot 2^{-\sqrt{r}/8}$.

Theorem 5 can be applied even if $k = o(\sqrt{n})$, but the error converges rather slow: since $k \geq r^4$, we have

$$\varepsilon = 5f \cdot 2^{-\sqrt{r}/8} \geq 5f \cdot 2^{-\sqrt[8]{k}/8}.$$

4 A Sampling Theorem from Quantum Bit Extractors

In this section we give a new min-entropy sampling theorem (Theorem 1) using a completely different approach than [KR07]. Our proof has two steps. First, we show a bound on the guessing probability of the XOR of a randomly chosen substring of X using the same approach as [DV10], which is based on a result by König and Terhal [KT08] on strong bit-extractors against quantum adversaries. Second, we will show that this implies a bound on the guessing probability of a randomly chosen substring of X . To show this we use a result from [BARdW08].

A function $\text{ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is a (ℓ, ε) -strong extractor against quantum adversaries, if for all cq-states ρ_{XQ} with $H_{\min}(X | Q)_\rho \geq \ell$ and for a uniform seed R , we have $D(\rho_{\text{ext}(X,R)RQ}, \tau_U \otimes \rho_R \otimes \rho_Q) \leq \varepsilon$, where τ_U is the fully mixed state. A strong classical extractor is the same, but with a trivial system Q . If $m = 1$, we call it a *bit-extractor*. König and Terhal showed in [KT08] that any classical bit-extractor is also a quantum bit-extractor.

Theorem 6 (Theorem III.1 in [KT08]). *Any (ℓ, ε) -strong bit-extractor is a $(\ell + \log 1/\varepsilon, 3\sqrt{\varepsilon})$ -strong bit-extractor against quantum adversaries.*

One way to construct a strong bit-extractor is to use a (ε, δ, L) -approximately list-decodable code. This is a code $C : \{0, 1\}^n \rightarrow \{0, 1\}^m$ where for every $c \in \{0, 1\}^m$ there exist L strings $x_1, \dots, x_L \in \{0, 1\}^n$, such that for any string $x \in \{0, 1\}^n$ satisfying $d_H(c, C(x)) < (\frac{1}{2} - \varepsilon)m$, there exists an $i \in \{1, \dots, L\}$ such that $d_H(x_i, x) \leq \delta m$. From a code $C : \{0, 1\}^n \rightarrow \{0, 1\}^{2^t}$, we can build a bit-extractor $\text{ext} : \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}$ as $\text{ext}(x, y) := C(x)_y$, where $C(x)_y$ is the y th position of the codeword $C(x)$.

Lemma 4 (Claim 3.7 in [DV10]). *Let $\delta \in [0, \frac{1}{2}]$. An extractor build from a (ε, δ, L) -approximately list-decodable code $C : \{0, 1\}^n \rightarrow \{0, 1\}^{2^t}$ is a (ℓ, ε) -strong classical bit-extractor for $\ell > H(\delta)n + \log L + \log 2/\varepsilon$.*

The (n, k) -XOR-code over strings of length n is the code where the string x gets encoded into a string of size $\binom{n}{k}$ where each bit is the XOR of a subset of x of size k .

Lemma 5 (Lemma 42 in [JK06], adapted to Lemma 3.11 in [DV10]). *For $\varepsilon > 2k^2/2^n$, the (n, k) -XOR-code is a $(\varepsilon, \frac{1}{k} \ln \frac{2}{\varepsilon}, 4/\varepsilon^2)$ -approximately list-decodable code.*

Combining Lemmas 4 and 5 with Theorem 6, we get the following lemma.

Lemma 6. *Let $\varepsilon > 2k^2/2^n$ and $k \geq 2 \ln \frac{2}{\varepsilon}$. The extractor build from the (n, k) -XOR-code implies a $(\ell, 3\sqrt{\varepsilon})$ -strong bit-extractor against quantum adversaries for*

$$\ell > H\left(\frac{1}{k} \ln \frac{2}{\varepsilon}\right)n + 4 \log \frac{1}{\varepsilon} + 3.$$

Proof. Using Lemmas 4 and 5, the (n, k) -XOR-code implies a (ℓ, ε) -strong classical bit-extractor for

$$\ell > H\left(\frac{1}{k} \ln \frac{2}{\varepsilon}\right)n + \log \frac{4}{\varepsilon^2} + \log \frac{2}{\varepsilon} = H\left(\frac{1}{k} \ln \frac{2}{\varepsilon}\right)n + 3 \log \frac{1}{\varepsilon} + 3.$$

The statement follows from Theorem 6. \square

From Lemmas 1 and 6 follows that if a string X can only be guessed from Q with probability at most $2^{-\ell}$, i.e., $H_{\min}(X | Q) \geq \ell$, then the XOR of a random subset of size k can be guessed with probability at most $1/2 + 3\sqrt{\varepsilon}$. The following lemma gives a bound on the probability to guess a whole substring, given bounds on the probability to guess the XOR of substrings. It has been proven as a part of Theorem 2 in [BARdW08].

Lemma 7 (part of Theorem 2 in [BARdW08]). *Let ρ_{XQ} be a cq-state where $X \in \{0, 1\}^n$ and let $p_j > 0$ for $j \in \{0, \dots, k\}$ be upper bounds on the probability to guess the XOR of a random subset of X of size j given Q and the subset. Then the probability to guess a random subset of X of size k from Q and the subset is at most*

$$\frac{1}{2^k} \sum_{j=0}^k \binom{k}{j} (2p_j - 1).$$

We can now use Lemmas 6 and 7 to proof the following sampling lemma.

Lemma 8. *Let a cq-state ρ_{XQ} be given, where $X \in \{0, 1\}^n$. Let T be a uniformly chosen subset of $[n]$ of size k . If $\log \frac{1}{p} \leq k/12 - 5$ and*

$$H_{\min}(X | Q)_\rho \geq H\left(\frac{6}{k} \log \frac{17}{p}\right)n + 8 \log \frac{12}{p} + 3,$$

then $H_{\min}(X_T | TQ)_\rho \geq \log \frac{1}{p}$.

Proof. From $\log \frac{1}{p} \leq k/12 - 5$ follows that

$$k \geq 12 \log \frac{17}{p} \geq 17 \ln \frac{17}{p}. \quad (1)$$

Since $k \leq n$ and $5k/12 + 5 \geq \log(17k)$, it follows also that

$$\log \frac{1}{p} \leq \frac{k}{12} - 5 = \frac{k}{2} - \frac{5k}{12} - 5 \leq \frac{k}{2} - \log(17k) \leq \frac{n}{2} - \log(17k)$$

and hence $p^2 \geq 288 \cdot k^2 / 2^n$. For $j \in \{0, \dots, k\}$, let p_j be the guessing probability of the XOR for random subsets of size j . From Lemma 7 follows that

$$\begin{aligned} P_{\text{guess}}(X_T | TQ)_\rho &\leq \frac{1}{2^k} \sum_{j=0}^k \binom{k}{j} (2p_j - 1) \\ &\leq \frac{1}{2^k} \sum_{j=0}^{k/4} \binom{k}{j} + \max_{j' \in [k/4+1, k]} (2p_{j'} - 1) \cdot \frac{1}{2^k} \sum_{j=k/4+1}^k \binom{k}{j} \\ &\leq \frac{1}{2^k} \sum_{j=0}^{k/4} \binom{k}{j} + \max_{j' \in [k/4+1, k]} (2p_{j'} - 1). \end{aligned}$$

We have

$$\sum_{j=0}^{k/4} \frac{1}{2^k} \binom{k}{j} = \Pr [J \leq k/4],$$

where $J = \sum_{i \in [k]} J_i$ and the random variables J_i are independent and uniform on $\{0, 1\}$. From Lemma 2 follows that

$$\Pr[J \leq k/4] \leq \exp(-k/8) \leq p/2,$$

since $k \geq 17 \ln \frac{17}{p} > 8 \ln \frac{2}{p}$. Let $\varepsilon := p^2/144$. From Eq. (1) follows that

$$\frac{1}{2} \geq \frac{6}{k} \log \frac{17}{p} \geq \frac{17}{2k} \ln \frac{17}{p} \geq \frac{4}{k} \ln \frac{288}{p^2} = \frac{4}{k} \ln \frac{2}{\varepsilon} \geq \frac{1}{j'} \ln \frac{2}{\varepsilon},$$

for any $j' \in [k/4 + 1, k]$. Since $8 \log(12/p) = 4 \log(1/\varepsilon)$, we have

$$H_{\min}(X | Q)_\rho \geq H\left(\frac{1}{j'} \ln \frac{2}{\varepsilon}\right)n + 4 \log \frac{1}{\varepsilon} + 3.$$

From $p^2 \geq 288 \cdot k^2 / 2^n$ follows that $\varepsilon \geq 2k^2 / 2^n \geq 2j'^2 / 2^n$. Lemmas 1 and 6 imply that $p_{j'} \leq 1/2 + 3\sqrt{\varepsilon}$, and hence

$$\max_{j' \in [k/4+1, k]} (2p_{j'} - 1) \leq 6\sqrt{\varepsilon} = p/2.$$

So $P_{\text{guess}}(X_T | TQ)_\rho \leq p$. The statement follows from the definition of H_{\min} . \square

Proof. (Theorem 1). Let $m := H_{\min}(X | Q)_\rho$ and $p := 2^{-H^{-1}(m/2n)k/6+5}$. We have

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5,$$

which implies

$$\frac{m}{2} = H\left(\frac{6}{k} \log \frac{32}{p}\right)n \geq H\left(\frac{6}{k} \log \frac{17}{p}\right)n \quad (2)$$

and, since $H^{-1}(m/2n) \leq \frac{1}{2}$,

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5 \leq \frac{k}{12} - 5. \quad (3)$$

From $n \geq k$ and $\frac{1}{2} \geq x/2 \geq H^{-1}(x)$ for any $x \in [0, 1]$ follows

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5 \leq H^{-1}\left(\frac{m}{2n}\right) \cdot \frac{n}{6} - 5 \leq \frac{m}{4n} \cdot \frac{n}{6} - 5 = \frac{m}{24} - 5,$$

which implies

$$8 \log \frac{12}{p} + 3 = 8 \log \frac{1}{p} + 8 \log(12) + 3 \leq \frac{m}{3} - 40 + 32 + 3 \leq \frac{m}{2}.$$

Together with Eq. (2), we get

$$m \geq H\left(\frac{6}{k} \log \frac{17}{p}\right) n + 8 \log \frac{12}{p} + 3. \quad (4)$$

The statement follows from Lemma 8 and Eqs. (3) and (4). \square

5 Lower Bounds for Random Access Codes

Corollary 1 directly implies a lower bound for k -out-of- n random access codes: if we choose the string $X \in \{0, 1\}^n$ uniformly at random and the quantum system Q has at most $m \leq (1 - 2H(\varepsilon))n$ qubits, then by Proposition 2' in [KT08], we have $H_{\min}(X | Q) \geq 2H(\varepsilon)n$. Corollary 1 follows.

Note that in the same way Theorems 4 or 5 could be used to give a bound for random access codes, since $H_{\min}^{\varepsilon}(X | Q) \geq \ell$ implies $P_{\text{guess}}(X | Q) \geq 2^{-\ell} + \varepsilon$. But since the error ε converges slowly, we would only get a weak bound on the guessing probability.

6 Open Problems

Our sampling results only apply to the case where the sample is chosen uniformly. It would be interesting to know if they can be generalized to other sampling strategies.

Acknowledgements. I thank Robert König, Thomas Vidick and Stephanie Wehner for helpful discussions and the anonymous reviewers for useful comments. This work was funded by the U.K. EPSRC grant EP/E04297X/1 and the Canada-France NSERC-ANR project FREQUENCY. Most of this work was done while I was at the University of Bristol.

References

- ANTSV99. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and a lower bound for 1-way quantum automata. In: Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing (STOC '99). ACM (1999)
- BARdW08. Ben-Aroya, A., Regev, O., de Wolf, R.: A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In: Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08) (2008)
- DV10. De, A., Vidick, T.: Near-optimal extractors against quantum storage. In: Proceedings of the Fourty-Second Annual ACM Symposium on Theory of Computing (STOC '10). ACM (2010)
- IJK06. Impagliazzo, I., Jaiswal, R., Kabanets, V.: Approximately list-decoding direct product codes and uniform hardness amplification. In: Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science (FOCS '06), pp. 187–196 (2006)
- KR07. König, R., Renner, R.: Sampling of min-entropy relative to quantum knowledge. arXiv:0712.4291 (2007)
- KRS09. König, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**(9), 4337–4347 (2009)
- KT08. König, R., Terhal, B.M.: The bounded storage model in the presence of a quantum adversary. *IEEE Trans. Inf. Theory* **54**(2), 749–762 (2008)
- KWW09. König, R., Wehner, S., Wullschleger, J.: Unconditional security from noisy quantum storage. arXiv:0906.1030 (2009)
- Nay99. Nayak, A.: Optimal lower bounds for quantum automata and random access codes. In: Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS '99), pp. 369–376 (1999)
- Ren05. Renner, R.: Security of quantum key distribution. Ph.D thesis, ETH Zürich, Switzerland. arXiv:quant-ph/0512258 (2005)
- Vad04. Vadhan, S.: Constructing locally computable extractors and cryptosystems in the bounded-storage model. *J. Cryptol.* **17**, 2004 (2004)

Which Graph States are Useful for Quantum Information Processing?

Mehdi Mhalla¹(✉), Mio Murao^{2,3}, Simon Perdrix¹, Masato Someya²,
and Peter S. Turner²

¹ CNRS, LIG, Université de Grenoble, Grenoble, France
mehdi.mhalla@gmail.com

² Graduate School of Science, The University of Tokyo, Tokyo, Japan

³ NanoQuine, The University of Tokyo, Tokyo, Japan

Abstract. Graph states [5] are an elegant and powerful quantum resource for measurement based quantum computation (MBQC). They are also used for many quantum protocols (error correction, secret sharing, etc.). The main focus of this paper is to provide a structural characterisation of the graph states that can be used for quantum information processing. The existence of a gflow (generalized flow) [8] is known to be a requirement for open graphs (graph, input set and output set) to perform uniformly and strongly deterministic computations. We weaken the gflow conditions to define two new more general kinds of MBQC: uniform equiprobability and constant probability. These classes can be useful from a cryptographic and information point of view because even though we cannot do a deterministic computation in general we can preserve the information and transfer it perfectly from the inputs to the outputs. We derive simple graph characterisations for these classes and prove that the deterministic and uniform equiprobability classes collapse when the cardinalities of inputs and outputs are the same. We also prove the reversibility of gflow in that case. The new graphical characterisations allow us to go from open graphs to graphs in general and to consider this question: given a graph with no inputs or outputs fixed, which vertices can be chosen as input and output for quantum information processing? We present a characterisation of the sets of possible inputs and outputs for the equiprobability class, which is also valid for deterministic computations with inputs and outputs of the same cardinality.

1 Introduction

The graph state formalism [5] is an elegant and powerful formalism for quantum information processing. Graph states form a subfamily of the stabiliser states [4]. They provide a graphical description of entangled states and they have multiple applications in quantum information processing, in particular in measurement-based quantum computation (MBQC) [9], but also in quantum error correcting codes [4] and in quantum protocols like secret sharing [6, 7]. They offer a combinatorial approach to the characterisation of the fundamental properties

of entangled states in quantum information processing. The invariance of the entanglement by local complementation of a graph [10]; the use of measure of entanglement based on the rank-width of a graph [11]; and the combinatorial *flow* characterisation [1] of deterministic evolutions in measurement-based quantum computation witness the import role of the graph state formalism in quantum information processing.

In this paper, we focus on the application of graph states in MBQC and in particular on the characterisation of graphs that can be used to perform quantum information processing in this context. The existence of a graphical condition which guarantees that a deterministic MBQC evolution can be driven despite of the probabilistic behaviour of the measurements is a central point in MBQC. It has already been proven that the existence of a certain kind of flow called *gflow* characterises uniformly stepwise determinism [1]. In Sect. 3, we introduce a simpler but equivalent combinatorial characterisation using *focused gflow* and we provide a simple condition of existence of such a flow as the existence of a right inverse to the adjacency matrix of the graph. We also prove additional properties in the case where the number of input and output qubits of the computation are the same: the *gflow* is then reversible and the stepwise condition [1] on determinism is not required to guarantee the existence of a *gflow*.

The main contribution of this paper is the weakening of the determinism condition in order to consider the more general class of *information preserving* evolutions. Being information preserving is one of the most fundamental property that can be required for an MBQC computation. Indeed, some non-deterministic evolutions can be information preserving when one knows the classical outcomes of the measurements produced by the computation. Such evolutions are called *equi-probabilistic* – when each classical outcome occurs with probability $1/2$ – or *constant-probabilistic* in the general case. In Sect. 4, we introduce simple combinatorial conditions for equi-probabilistic and constant-probabilistic MBQC by means of excluded violating sets of vertices. We show, in the particular case where the number of input and output qubits are the same, that graphs guaranteeing equi-probabilism and determinism are the same. In Sect. 6, using this graphical characterisation, we address the fundamental question of finding input and output vertices in an arbitrary graph for guaranteeing an equi-probabilistic (or deterministic) evolution. To this end, we show that the input and output vertices of a graph must form transversals of the violating sets induced by the equi-probabilistic characterisation. Finally, in the last section, we investigate several properties of the most general and less understood class of constant probabilistic evolutions.

2 Measurement-Based Quantum Computation

In this section, the main ingredients of measurement based quantum computation (MBQC) are described. More detailed introductions can be found in [2,3]. An MBQC is described by:

- (i) an open graph (G, I, O) (G is a simple undirected graph, $I, O \subseteq V(G)$ are called resp. input and output vertices);
- (ii) a map $\alpha : O^C \rightarrow [0, 2\pi)$, where $O^C := V(G) \setminus O$, which associates with every non output vertex an angle; and
- (iii) two maps $\mathbf{x}, \mathbf{z} : O^C \rightarrow \{0, 1\}^{V(G)}$ called *corrective maps*. A vertex $v \in \text{supp}(\mathbf{x}(u)) \cup \text{supp}(\mathbf{z}(u))$ is called a *corrector* of u , where $\text{supp}(y) = \{u \mid y_u = 1\}$.

The maps \mathbf{x}, \mathbf{z} should be *extensive* in the sense that there exists a (strict) partial order \prec over the vertices of the graph s.t. any corrector v of a vertex u is larger than u , i.e. $v \in \text{supp}(\mathbf{x}(u)) \cup \text{supp}(\mathbf{z}(u))$ implies $u \prec v$.

In the following the semantics of a given MBQC is described. The evolution can be decomposed into two steps: first the preparation of a large entangled state described by the open graph (G, I, O) ; then a sequence of one-qubit measurements (which basis are characterised by the map α) and Pauli operations (described by the maps \mathbf{x} and \mathbf{z}).

Let $N : \mathbb{C}^{\{0,1\}^I} \rightarrow \mathbb{C}^{\{0,1\}^{V(G)}}$ be the preparation map which associates with any arbitrary input state located on the input qubits the initial entangled state of the MBQC:

$$N = \frac{1}{\sqrt{2^{|I^C|}}} \sum_{x \in \{0,1\}^I, y \in \{0,1\}^{I^C}} (-1)^{q(xy)} |xy\rangle \langle x|$$

where xy denotes the concatenation of x and y , and $q : \{0, 1\}^{V(G)} \rightarrow \mathbb{N}::x \mapsto |E(G) \cap (\text{supp}(x) \times \text{supp}(x))|$ associates with every x the number of edges of the subgraph $G_x = (V(G) \cap \text{supp}(x), E(G) \cap (\text{supp}(x) \times \text{supp}(x)))$ induced by x .

The one-qubit measurements, parametrized by an angle α_u , of every non-output qubit u are inducing the following projection $P_s(\alpha) : \mathbb{C}^{\{0,1\}^{V(G)}} \rightarrow \mathbb{C}^{\{0,1\}^{O^C}}$ of the entangled state onto the subspace of the output qubits, where $s \in \{0, 1\}^{O^C}$ stands for the classical outcomes of the one-qubit measurements:

$$P_s(\alpha) = \frac{1}{\sqrt{2^{|I^C|}}} \sum_{x \in \{0,1\}^{O^C}, y \in \{0,1\}^O} e^{\alpha_{x \cdot s}} |y\rangle \langle xy|$$

with $\alpha_x = \sum_{u \in \text{supp}(x)} \alpha(u)$ and $x \cdot s$ is the bitwise conjunction of x and s .

Moreover, adaptative Pauli corrections depending on the classical outcomes of the measurements and on the corrective maps, are applied during the computation leading, for any possible classical outcomes $s \in \{0, 1\}^{O^C}$, to the following overall (postselected) evolution $\chi_s : \mathbb{C}^{\{0,1\}^I} \rightarrow \mathbb{C}^{\{0,1\}^O}$:

$$\chi_s = P_s(\alpha) \left(\prod_{u \in V(G)} X_{s \cdot \mathbf{x}(u)} Z_{s \cdot \mathbf{z}(u)} \right) N$$

where X_s and Z_s are Pauli operators: $X_s = \bigotimes_{u \in \text{supp}(s)} X_u$ and $Z_s = \bigotimes_{u \in \text{supp}(s)} Z_u$.

An MBQC is implementing the quantum operation $\{\chi_s\}_{s \in \{0,1\}^{O^C}}$. The evolution is as follows: a classical outcome (also called branch) $s \in \{0,1\}^{O^C}$ is produced and the input state $|\phi\rangle \in \mathbb{C}^{\{0,1\}^I}$ is mapped to the state $\chi_s |\phi\rangle \in \mathbb{C}^{\{0,1\}^{O^C}}$ (up to a normalisation). The probability for an outcome $s \in \{0,1\}^{O^C}$ to occur is $p_s = \|\chi_s |\phi\rangle\|^2$.

The overall evolution can be decomposed into several steps, corresponding to a possible implementation of the MBQC model: first the input state $|\phi\rangle$ is encoded into the open graph state $|\phi_G\rangle = N |\phi\rangle$, then the local measurements (qubit u is measured according the observable $\cos(\alpha(u))X + \sin(\alpha(u))Y$) and the local Pauli corrections are performed. This sequence of local operations is done according to the partial order induced by the correction maps \mathbf{x}, \mathbf{z} .

3 Determinism

Definition 1. An MBQC $(G, I, O, \alpha, \mathbf{x}, \mathbf{z})$ is strongly deterministic if all the branches are implementing the same map, i.e. $\exists U$ s.t. $\forall s \in \{0,1\}^{O^C}$, $\chi_s = \frac{1}{\sqrt{2^{|O^C|}}} U$.

Lemma 1. If an MBQC is strongly deterministic then it implements an isometry.

Proof. Since $\sum_{s \in \{0,1\}^{O^C}} \chi_s^\dagger \chi_s = I$, $U^\dagger U = I$ so U is an isometry and the MBQC implements the super operator $\rho \mapsto U \rho U^\dagger$. \square

In order to point out the combinatorial properties of MBQC, the angles of measurements and the corrective maps can be abstracted away in the following way, keeping only the influence of the initial open graph.

Definition 2. An open graph (G, I, O) guarantees uniformly strong determinism if $\exists \mathbf{x}, \mathbf{z}$ s.t. $\forall \alpha$, $(G, I, O, \alpha, \mathbf{x}, \mathbf{z})$ is strongly deterministic.

An open graph is said to guarantee uniform *stepwise* strong determinism if any partial computation is also strongly deterministic:

Definition 3. An open graph (G, I, O) guarantees uniformly stepwise strong determinism if $\exists \mathbf{x}, \mathbf{z}$ s.t. for any upward closed set $O' \supseteq O$ and for any α , $(G, I, O', \alpha, \mathbf{x}, \mathbf{z})$ is strongly deterministic, where O' is upward closed if $\forall u \in O'$, $u \prec v \Rightarrow v \in O'$ with \prec the partial order induced by \mathbf{x} and \mathbf{z} .

The gflow of an open graph is defined as follows, based on the use of the odd neighborhood of a set of vertices: for a given subset S of vertices in a graph G , $Odd(S) := \{v \in V(G) \text{ s.t. } |\mathcal{N}_G(v) \cap S| = 1 \pmod{2}\}$.

Definition 4. (g, \prec) is a gflow of (G, I, O) , where $g : O^C \rightarrow 2^{I^c}$, if for any u ,

- if $v \in g(u)$, then $u \prec v$;
- $u \in Odd(g(u))$;
- if $v \in Odd(g(u))$ and $u \neq v$ then $u \prec v$.

Theorem 1. An open graph (G, I, O) guarantees uniform stepwise strong determinism iff (G, I, O) has a gflow.

3.1 Focused Gflow

Since the gflow is not unique we introduce a stronger version called focused gflow, which is unique if the number of inputs and outputs are the same. The focused gflow gives rise to a simpler characterisation of uniform stepwise strong determinism. The focused gflow is based on the use of *extensive* maps.

Definition 5. $g : O^C \rightarrow 2^{I^C}$ is a focused gflow of (G, I, O) if g is extensive – i.e. the transitive closure of the relation $\{(u, v) \text{ s.t. } v \in g(u)\}$ is a partial order over $V(G)$ – and $\forall u \in O^C, \text{Odd}(g(u)) \cap O^C = \{u\}$

Theorem 2. An open graph (G, I, O) guarantees uniform stepwise strong determinism iff (G, I, O) has a focused gflow.

Proof. We prove that (G, I, O) has a gflow iff it has a focused gflow. First, assume g is a focused gflow, and let \prec be the transitive closure of $\{(u, v) \text{ s.t. } v \in g(u)\}$. \prec is a partial order and by definition, if $v \in g(u)$ then $u \prec v$. Moreover $u \in \text{Odd}(g(u)) = \{u\}$. Finally, if $v \in \text{Odd}(g(u))$ and $v \neq u$ then $v \in O$, so there is no element larger than v by definition of \prec . Thus (g, \prec) is a gflow. Now, assume (g, \prec) is a gflow. We call the co-depth of a vertex u its distance to the output, i.e. the length k of longest strictly increasing sequence $u \prec u_1 \prec \dots \prec u_k$ s.t. $u_k \in O$. We construct a focus gflow g_f by induction on the co-depth of the vertices. If u is of co-depth 1 then $g_f(u) := g(u)$. If u is of co-depth larger than 2, let $g_f(u) := g(u) \Delta (\Delta_{v \in \text{Odd}(g(u)) \cap O^C, v \neq u} g_f(v))$, where Δ is the symmetric difference: $A \Delta B = (A \cup B) \setminus (A \cap B)$. Since $\text{Odd}(A \Delta B) = \text{Odd}(A) \Delta \text{Odd}(B)$, $\text{Odd}(g_f(u)) \cap O^C = (\text{Odd}(g(u)) \Delta (\Delta_{v \in \text{Odd}(g(u)) \cap O^C, v \neq u} \text{Odd}(g_f(v)))) \cap O^C = (\text{Odd}(g(u)) \cap O^C) \Delta (\text{Odd}(g(u)) \setminus \{u\}) \cap O^C = \{u\}$. Moreover g_f is extensive since the relation R induced by g_f is s.t. $uRv \implies u \prec v$ so the transitive closure of R is a partial order. \square

3.2 Induced Adjacency Matrix and Reversibility

We introduce the notion of induced adjacency matrix of an open graph and show that an open graph has a gflow if and only if its induced matrix has a DAG (Directed Acyclic Graph) as right inverse.

Definition 6. The induced adjacency matrix of an open graph (G, I, O) is the submatrix $A_G|_{I^C}^{O^C}$ of the adjacency matrix $A_G = \{m_{u,v}, (u, v) \in V(G)\}$ of G removing the rows of O and column of I , i.e. $A_G|_{I^C}^{O^C} = \{m_{u,v}, (u, v) \in O^C \times I^C\}$.

The induced matrix $A_G|_{I^C}^{O^C}$ is the matrix representation of the linear map $W \mapsto \text{Odd}(W) \cap O^C$ which domain is 2^{I^C} and codomain is 2^{O^C} .

Theorem 3. (G, I, O) has a gflow iff there exists a DAG $F = (V(G), E)$ s.t.

$$A_G|_{I^C}^{O^C} . A_F|_{O^C}^{I^C} = I$$

Proof. (only if) Assume (G, I, O) has a gflow. Thanks to lemma 2 w.l.o.g. (G, I, O) has a focused gflow g_f . Let $F = (V(G), E)$ be a directed graph s.t. $(u, v) \in E(F) \iff v \in g_f(u)$. Notice that $\forall u \in O^C, A_F|_{O^C}^I 1_{\{u\}} = 1_{g_f(u)}$ where 1_X is a binary vector s.t. $(1_X)_u = 1 \iff u \in X$. Moreover, since g_f is extensive, F is a DAG. Thus $A_G|_{O^C}^I A_F|_{O^C}^I 1_{\{u\}} = A_G|_{O^C}^I 1_{g(u)} = 1_{\text{Odd}(g_f(u)) \cap O^C} = 1_{\{u\}}$.

(if) Assume $F = (V(G), E)$ be a DAG s.t. $A_G|_{O^C}^I A_F|_{O^C}^I = I$, then let $g : O^C \rightarrow 2^{I^C} = u \mapsto \mathcal{N}_F^+(u)$. Since F is a DAG, g is extensive, and $1_{\text{Odd}(g(u)) \cap O^C} = A_F|_{O^C}^I (1_{g(u)}) = A_G|_{O^C}^I A_F|_{O^C}^I 1_{\{u\}} = 1_{\{u\}}$, so $\text{Odd}(g(u)) \cap O^C = \{u\}$. \square

Thus, according to Theorem 3, an open graph has a gflow if and only if it has a DAG as right inverse. Notice that this DAG is nothing but the graphical description of the focused gflow function: the set of successors of a vertex u is the image of u by the focused gflow function.

As a corollary of Theorem 3, (G, I, O) has no gflow if $|I| > |O|$. Indeed, for dimension reasons, if $|I| > |O|$ the matrix $A_G|_{O^C}^I$ has no right inverse. When $|I| = |O|$ the focused gflow is *reversible* in the following sense:

Theorem 4. *When $|I| = |O|$, (G, I, O) has a gflow iff (G, O, I) has a gflow.*

Proof. Assume (G, I, O) has a gflow. So it exists a DAG F s.t. $A_F|_{O^C}^I$ is the right inverse of $A_G|_{O^C}^I$. Notice that the induced adjacency matrix of (G, O, I) is the transpose ${}^t A_G|_{O^C}^I$ of the one of (G, I, O) . Moreover, since $A_G|_{O^C}^I$ is squared, $A_F|_{O^C}^I$ is both right and left inverse of $A_G|_{O^C}^I$. Thus, $A_G|_{O^C}^I \cdot {}^t A_F|_{O^C}^I = {}^t (A_F|_{O^C}^I \cdot A_G|_{O^C}^I) = I$. As a consequence $A_G|_{O^C}^I$ has a right inverse which is a DAG since the transpose of a DAG is a DAG. \square

4 Relaxing Uniform Determinism

Focused gflow guarantees uniformly stepwise strong determinism. We consider here two more general classes of MBQC evolutions: the *equi-probabilistic* case where all the branches occur with the same probability, independent of the input state; and the *constant probability* case where all the branches occur with a probability independent of the input state. We show that both equi-probabilistic and constant probabilistic evolutions are information preserving and admit a simple graphical characterisation by means of violating sets.

Definition 7. *An MBQC $(G, I, O, \alpha, \mathbf{x}, \mathbf{z})$ is:*

- equi-probabilistic if for any input state $|\phi\rangle \in \mathbb{C}^{2^I}$ and any branch $s \in \{0, 1\}^{O^C}$, $p_s = \|\chi_s |\phi\rangle\|^2 = \frac{1}{2^{|O^C|}}$.
- constant-probabilistic if for any branch $s \in \{0, 1\}^{O^C}$ the probability $p_s = \|\chi_s |\phi\rangle\|$ that the branch s occurs does not depend on the input state $|\phi\rangle$.

Constant probabilistic (and hence equi-probabilistic) evolutions are *information preserving* in the sense that if one knows the branch s of the computation (i.e. the classical outcome) then he can recover the initial input state of

the computation. Indeed, if an MBQC is constant probabilistic then the map $|\phi\rangle \mapsto \|\chi_s|\phi\rangle\|$ is constant, thus $\chi_s^\dagger\chi_s = p_s.I$. If $p_s = 0$ then the branch never occurs, otherwise the branch s is implementing an isometry.

Remark: Notice that the knowledge of the branch s , which is necessary the case in the MBQC model because of the corrective strategy, is essential to make an equi-probabilistic evolution information preserving. Indeed, consider the quantum one-time pad example with $\forall s \in \{0, 1\}^2$, $\chi_s = \sigma_s/2$ where σ_s is a Pauli operator ($\sigma_{00} = I, \sigma_{01} = X, \sigma_{10} = Y, \sigma_{11} = Z$). This evolution is equi-probabilistic but if the information of the branch is not taken into account, the corresponding super operator is $\rho \mapsto \sum_{s \in \{0,1\}^2} \sigma_s \rho \sigma_s^\dagger = I/2$ which is clearly not information preserving.

We prove that uniform equi- and constant probabilities have simple graph characterisations by violating sets, where uniformity is defined similarly to the determinism case:

Definition 8. *An open graph (G, I, O) guarantees uniform constant (resp. equi-) probabilisty if $\exists \mathbf{x}, \mathbf{z}$ s.t. $\forall \alpha, (G, I, O, \alpha, \mathbf{x}, \mathbf{z})$ has a constant (resp. equi-) probabilistic evolution.*

Theorem 5. *An open graph (G, I, O) guarantees uniform equiprobability iff*

$$\forall W \subseteq O^C, \text{Odd}(W) \subseteq W \cup I \implies W = \emptyset$$

A nonempty set $W \subseteq O^C$ such that $\text{Odd}(W) \subseteq W \cup I$ is called an *internal set*. Theorem 5 says that an open graph (G, I, O) guarantees uniform equi-probability if and only if it has no internal set.

Proof. (if) First we assume that there is no internal set and we show that every branch occurs with the same probability $1/2^{|O^C|}$, independently of the input state and the set of measurement angles. For a given open graph (G, I, O) , a given input state $|\phi\rangle$ and a given set of measurement angles $\{\alpha_v\}_{v \in O^C}$, we consider w.l.o.g. the 0-branch, i.e. the branch where all outcomes are 0¹. The probability of this branch is $p = \|\prod_{v \in O^C} \langle +\alpha_v | \phi_G \rangle\|^2 = \frac{1}{2^{|O^C|}} \|\sum_{x \in \{0,1\}^{O^C}} e^{i\alpha_x} \langle x | \phi_G \rangle\|^2$ where $\alpha_x = \sum_{v \in O^C} \alpha_v \cdot x_v$ and $|\phi_G\rangle = E_G |+\rangle_{IC} |\phi\rangle_I$. As a consequence,

$$\begin{aligned} p &= \frac{1}{2^{|O^C|}} \sum_{x, y \in \{0,1\}^{O^C}} e^{i(\alpha_y - \alpha_x)} \langle \phi_G | x \rangle \langle y | \phi_G \rangle \\ &= \frac{1}{2^{|O^C|}} \sum_{u \in \{-1,0,1\}^{O^C}} e^{i\alpha_u} \sum_{x, y \in \{0,1\}^{O^C}} \text{s.t. } x-y=u \langle \phi_G | x \rangle \langle y | \phi_G \rangle \\ &= \frac{1}{2^{|O^C|}} \sum_{u \in \{-1,0,1\}^{O^C}} e^{i\alpha_u} \sum_{x \in \{0,1\}^{V_u^C}} \langle \phi_G | x \rangle_{V_u^C} \left| \frac{1+u}{2} \right\rangle_{V_u} \langle x |_{V_u^C} \left\langle \frac{1-u}{2} \right\rangle_{V_u} | \phi_G \rangle \\ &= \frac{1}{2^{|O^C|}} \sum_{u \in \{-1,0,1\}^{O^C}} e^{i\alpha_u} \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \left(\sum_{x \in \{0,1\}^{V_u^C}} |x\rangle \langle x| \right) \left\langle \frac{1-u}{2} \right\rangle_{V_u} | \phi_G \rangle \\ &= \frac{1}{2^{|O^C|}} \sum_{u \in \{-1,0,1\}^{O^C}} e^{i\alpha_u} \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \left\langle \frac{1-u}{2} \right\rangle_{V_u} | \phi_G \rangle \\ &= \frac{1}{2^{|O^C|}} \sum_{u \in \{-1,0,1\}^{O^C}} e^{i\alpha_u} p_u \end{aligned}$$

¹ The other branches are taken into account by considering a different set of measurement angles e.g. the branch where all outcomes are 1 corresponds to the 0-branch when the set of measurements is $\{\alpha_v + \pi\}_{v \in O^C}$.

where $V_u = \{i \in O^C \mid u_i \neq 0\}$, $|\frac{1+u}{2}\rangle_{V_u} = \bigotimes_{i \in V_u} |\frac{1+u_i}{2}\rangle_i$, and $p_u = \langle \phi_G | |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1-u}{2} |_{V_u} | \phi_G \rangle$. Notice that for any $v \in I^C$, $|\phi_G\rangle = \frac{1}{\sqrt{2}} \sum_{a \in \{0,1\}} Z_{\mathcal{N}_G(v)}^a |\phi_{G \setminus v}\rangle \otimes |a\rangle_v$. Thus for any $u \in \{-1, 0, 1\}^{O^C}$ s.t. $V_u \neq \emptyset$, there exists $v \in I^C \cap V_u^C \cap \text{Odd}(V_u)$ (which is not empty by hypothesis) such that:

$$\begin{aligned} p_u &= \langle \phi_G | |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} X_{V_u} | \phi_G \rangle \\ &= \frac{1}{2} \sum_{a,b \in \{0,1\}} \langle \phi_{G \setminus v} | \langle a |_v Z_{\mathcal{N}_G(v)}^a |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} X_{V_u} Z_{\mathcal{N}_G(v)}^b |\phi_{G \setminus v}\rangle |b\rangle_v \\ &= \frac{1}{2} \sum_{a \in \{0,1\}} \langle \phi_{G \setminus v} | Z_{\mathcal{N}_G(v)}^a |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} X_{V_u} Z_{\mathcal{N}_G(v)}^a |\phi_{G \setminus v}\rangle \\ &= \frac{1}{2} \sum_{a \in \{0,1\}} (-1)^a \langle \phi_{G \setminus v} | Z_{\mathcal{N}_G(v)}^a |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} Z_{\mathcal{N}_G(v)}^a X_{V_u} |\phi_{G \setminus v}\rangle \\ &= \frac{1}{2} \sum_{a \in \{0,1\}} (-1)^a \langle \phi_{G \setminus v} | |\frac{1+u}{2}\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} X_{V_u} |\phi_{G \setminus v}\rangle = 0 \end{aligned}$$

where the factor $(-1)^a$ comes from the fact that X_{V_u} and $Z_{\mathcal{N}_G(v)}^a$ are commuting when $a = 0$ and anticommuting when $a = 1$ since $v \in \text{Odd}(V_u)$. As a consequence, it remains in p only the case where $V_u = \emptyset$, so $p = \frac{1}{2^{|\mathcal{O}^C|}} \langle \phi_G | \phi_G \rangle = \frac{1}{2^{|\mathcal{O}^C|}}$.

(only if) Now we prove that the existence of an internal set implies that there exists a particular input state and a particular set of measurement angles such that some branches occur with probability 0. Let $W_0 \subseteq O^C$ s.t. $\text{Odd}(W_0) \cap W_0^C \cap I^C = \emptyset$ and $P = \bigotimes_{v \in V(G)} P_v$ be a Pauli operator defined as follows:

$$\forall v \in V(G), P_v = \begin{cases} X & \text{if } v \in W_0 \text{ and } v \notin \text{Odd}(W_0) \\ Y & \text{if } v \in W_0 \cap \text{Odd}(W_0) \\ I & \text{otherwise} \end{cases}$$

Let $|\phi_0\rangle = |+\rangle_{W_0 \cap I} \otimes |0\rangle_{W_0^C \cap I}$ be an input state. Notice that

$$\begin{aligned} P E_G |+\rangle_{I^C} |\phi_0\rangle &= (-1)^{|E(W_0)|} E_G X_{W_0} Z_{\text{Odd}(W_0) \cap W_0^C} |+\rangle_{I^C} |\phi_0\rangle \\ &= (-1)^{|E(W_0)|} E_G X_{W_0} |+\rangle_{I^C \cup W_0} Z_{\text{Odd}(W_0) \cap W_0^C} |0\rangle_{W_0^C \cap I} \\ &= (-1)^{|E(W_0)|} E_G |+\rangle_{I^C} |\phi_0\rangle, \end{aligned}$$

where $E(W) = E \cap (W \times W)$ is the set of the internal edges of W . Thus $E_G |+\rangle_{I^C} |\phi_0\rangle$ is an the eigenvector of P associated with the eigenvalue $(-1)^{|E(W_0)|}$, implying that if each qubit $v \in W_0$ is individually measured according to the observable P_v producing the classical outcome $s_v \in \{0, 1\}$, then $\sum_{v \in W_0} s_v = |E(W_0)| \pmod{2}$. As a consequence, for the input $|\phi_0\rangle$ and any set of measurements $\{\alpha_v\}_{v \in O^C}$ s.t. $\alpha_v = 0$ if $v \in W_0 \cap \text{Odd}(W_0)^C$ and $\alpha_v = \pi/2$ if $v \in W_0 \cap \text{Odd}(W_0)$, all the branches \mathbf{s} s.t. $\sum_{v \in W_0} \mathbf{s}_v = 1 + |E(W_0)| \pmod{2}$ occur with probability 0. \square

Theorem 6. *An open graph (G, I, O) guarantees uniform constant probability iff*

$$\forall W \subseteq O^C, \text{Odd}(W) \subseteq W \cup I \implies L(W) \cap I = \emptyset$$

where $L(W) := \text{Odd}(W) \cup W$.

A nonempty set $W \subseteq O^C$ such that $\text{Odd}(W) \subseteq W \cup I$ and $L(W) \cap I \neq \emptyset$ is called a strongly internal set. Theorem 6 says that an open graph (G, I, O)

guarantees uniform constant probability if and only if it has no strongly internal set, or equivalently if and only if all internal sets are ‘far enough’ from the inputs.

Proof. (if) First we assume that there is no strongly internal set and we show that every branch occurs with a probability independent of the input. Using the notations of the proof of Theorem 5, it only remains to prove that p_u is independent of the input for any $u \neq 0$ such that $I^C \cap V_u^C \cap \text{Odd}(V_u) = \emptyset$ and $L(V_u) \cap I = \emptyset$. Note that $\text{Odd}(V_u) \subseteq V_u \subseteq I^C$ so

$$\begin{aligned} p_u &= \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} X_{V_u} | \phi_G \rangle \\ &= (-1)^{|E(V_u)|} \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} E_G Z_{\text{Odd}(V_u)} X_{V_u} | + \rangle_{I^C} | \phi \rangle_I \\ &= (-1)^{|E(V_u)|} \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} E_G Z_{\text{Odd}(V_u)} | + \rangle_{I^C} | \phi \rangle_I \\ &= (-1)^{|E(V_u)| + |V_u \cap \text{Odd}(V_u)|} \langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} | \phi_G \rangle \end{aligned}$$

Moreover, for any $v \in V_u$, since $v \in I^C$, $\langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} | \phi_G \rangle$

$$\begin{aligned} &= \frac{1}{2} \sum_{a,b \in \{0,1\}} \langle \phi_{G \setminus v} | \langle a |_v Z_{\mathcal{N}_G(v)}^a | \frac{1+u}{2} \rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} Z_{\mathcal{N}_G(v)}^b | b \rangle_v | \phi_{G \setminus v} \rangle \\ &= \frac{1}{2} \langle \phi_{G \setminus v} | Z_{\mathcal{N}_G(v)}^{\frac{1+u+v}{2}} | \frac{1+u}{2} \rangle_{V_u \setminus v} \langle \frac{1+u}{2} |_{V_u \setminus v} Z_{\mathcal{N}_G(v)}^{\frac{1+u+v}{2}} | \phi_{G \setminus v} \rangle \\ &= \frac{1}{2} \langle \phi_{G \setminus v} | \left| \frac{1+u}{2} \right\rangle_{V_u \setminus v} \langle \frac{1+u}{2} |_{V_u \setminus v} | \phi_{G \setminus v} \rangle \end{aligned}$$

So, by induction, $\langle \phi_G | \left| \frac{1+u}{2} \right\rangle_{V_u} \langle \frac{1+u}{2} |_{V_u} | \phi_G \rangle = \frac{1}{2^{|V_u|}} \langle \phi_{G \setminus V_u} | | \phi_{G \setminus V_u} \rangle = \frac{1}{2^{|V_u|}}$. This shows that p_u does not depend on the input state.

(only if) Now we prove that the existence of a strongly internal set implies that there exists a particular set of measurement angles such that some branches occur with probability zero for some input state and with nonzero probability for other inputs. Let $W_0 \subseteq O^C$ s.t. $\text{Odd}(W_0) \cap W_0^C \cap I^C = \emptyset$, $u_0 \in L(W_0) \cap I$, and $P = \bigotimes_{v \in V} P_v$ be a Pauli operator defined like in the proof of Theorem 5. We consider the following input states: $|\phi_a\rangle = |+\rangle_{W_0 \cap I} \otimes |0\rangle_{W_0^C \cap I \setminus u_0} \otimes |a\rangle_u$ for $a \in \{0, 1\}$. Notice that $PE_G |+\rangle_{I^C} | \phi_a \rangle_I = (-1)^{a+|E(W_0)|} E_G |+\rangle_{I^C} | \phi_a \rangle_I$. Let $\alpha_v = \pi/2$ if $v \in W_0 \cap \text{Odd}(W_0)$ and $\alpha_v = 0$ otherwise. We consider a branch \mathbf{s} of measurement which occurs with a nonzero probability if the input state is $|\phi_0\rangle$. Notice that this branch satisfies $\sum_{v \in W_0} \mathbf{s}_v = (-1)^{|E(W_0)|}$. As a consequence, if the input state is $|\phi_1\rangle$, this branch \mathbf{s} occurs with probability 0. \square

5 Uniform Equiprobability Versus Gflow Existence

Since the existence of a gflow implies uniform strong determinism it also implies uniform equiprobability. In general uniform equiprobability does not imply gflow:

Lemma 2. *When $|I| \neq |O|$, there exists an open graph that satisfies uniform equiprobability but that has no gflow.*

Proof. Consider the graph depicted in Fig. 1. It is easy to see that it has no gflow, as no subset of the outputs has a single vertex as its odd neighborhood. On the other hand, all the subsets of O^C have a nonempty external odd neighborhood in I^C . \square

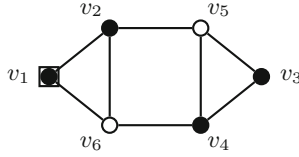


Fig. 1. Open graph (G, I, O) with $I = \{v_1\}$ and $O = \{v_5, v_6\}$ satisfying the uniform equiprobability condition but having no gflow.

However, in the particular case where $|I| = |O|$, the existence of a gflow implies uniform equiprobability.

Theorem 7. *When $|I| = |O|$, (G, I, O) guarantees uniform equiprobability iff it has a gflow.*

Proof. We only have to prove that uniform equiprobability implies the existence of gflow (the other direction is obvious). We prove the existence of a gflow for (G, O, I) which, according to Theorem 4, implies the existence of a gflow for (G, I, O) . Since (G, I, O) is uniformly equiprobable, the matrix $A_G|_{O^C}^{I^C}$ is injective, so reversible. Indeed, for any $W \subseteq O^C$, $A_G|_{O^C}^{I^C} \cdot 1_W = \emptyset \iff 1_{Odd(W) \cap I^C} = 0 \implies Odd(W) \subseteq I \subseteq W \cup I$ so $W = \emptyset$. The matrix $(A_G|_{O^C}^{I^C})^{-1}$ is the induced matrix of a directed open graph (H, O, I) , where H is chosen s.t. vertices in O have no successor. In the following we show that H is a DAG. By contradiction, let $S \subseteq V(H)$ be the shortest cycle in H . Notice that $S \subseteq O^C$ since vertices in O have no successor. $A_G|_{O^C}^{I^C} \cdot (A_G|_{O^C}^{I^C})^{-1} \cdot 1_S = 1_S \iff A_G|_{O^C}^{I^C} \cdot 1_{Odd_H(S) \cap O^C} = 1_S \iff Odd_G(Odd_H(S) \cap O^C) \cap I^C = S$. Let $W := Odd_H(S) \cap O^C$. Since S is the shortest cycle, $S \subseteq Odd_H(S)$. Moreover $S \subseteq O^C$ so $S \subseteq W$. Thus $Odd_G(W) \subseteq W \cup I^C$ which implies $W = \emptyset$, so $S = \emptyset$. Thus H is a DAG. \square

Notice that thanks to Theorem 7 the stepwise condition in the characterisation of gflow can be removed, improving Theorem 1:

Corollary 1. *When $|I| = |O|$, (G, I, O) guarantees uniform strong determinism iff it has a gflow.*

Proof. Uniform strong determinism implies equiprobability which ensures the existence of gflow when $|I| = |O|$. \square

6 Choosing Inputs and Outputs

The fact that the characterisation of uniform equiprobability is by excluded internal sets allows us to have a better view of the following general problem: given a graph, which vertices can be chosen as outputs and inputs for measurement based quantum information processing.

Definition 9. Given a graph G , for any $A \subseteq V(G)$, let \mathcal{E}_A be the collection of internal sets outside A : $\mathcal{E}_A := \{S \subseteq V(G), S \neq \emptyset \wedge \text{Odd}(S) \cap S^C \cap A^C = \emptyset\}$

A transversal of a collection C of sets is a set that intersects all the elements of C . The set of all transversals of \mathcal{E}_A is $T(\mathcal{E}_A) := \{S' \subseteq V(G), \forall S \in \mathcal{E}_A \ S' \cap S \neq \emptyset\}$.

Lemma 3. If an open graph (G, I, O) guarantees uniform equiprobability then $O \in T(\mathcal{E}_\emptyset)$.

Proof. By contradiction if $W \in \mathcal{E}_\emptyset$ and $W \cap O = \emptyset$, then $\text{Odd}(W) \cap W^C = \emptyset$, so $\text{Odd}(W) \subseteq W \cup I^C$ which implies $W = \emptyset$. It contradicts the fact that $W \in \mathcal{E}_\emptyset$. \square

Theorem 8. An open graph (G, I, O) guarantees uniform equiprobability if and only if $O \in T(\mathcal{E}_I)$.

Proof. $O \in T(\mathcal{E}_I) \iff \forall W \in \mathcal{E}_I, W \cap O \neq \emptyset \iff \forall W \subseteq O^C, W \notin \mathcal{E}_I \iff \forall W \subseteq O^C, \neg(\text{Odd}(W) \cap W^C \cap I^C \wedge W \neq \emptyset) \iff \forall W \subseteq O^C, (\text{Odd}(W) \subseteq W \cup I \Rightarrow W = \emptyset)$. \square

Theorem 9. Given a graph G and two subsets of vertices I and O with $|I| = |O|$, the open graph (G, I, O) guarantees equiprobability iff $I \in T(\mathcal{E}_\emptyset)$ and $O \in T(\mathcal{E}_I)$.

Proof. When $|I| = |O|$, if (G, I, O) guarantees equiprobability then (G, I, O) has a gflow (Theorem 7) and thus (G, O, I) has a gflow (Theorem 4) as well. As a consequence (G, I, O) guarantees uniform equiprobability so $I \in T(\mathcal{E}_\emptyset)$. \square

This observation allows a characterisation of the possible deterministic computations for small graphs. The main question is, given a graph G , how to find $I \subseteq V(G)$ and $O \subseteq V(G)$ with $|I| = |O|$ such that (G, I, O) has gflow.

Furthermore it is straightforward to see that :

Lemma 4. If an open graph (G, I, O) guarantees uniform equi-probability then (G, I', O') with $I' \subseteq I$ and $O \subseteq O'$ also guarantees uniform equi-probability.

Notice that gflow and constant probability classes are also stable by adding new outputs or removing inputs. Thus the interesting problem when choosing inputs and outputs consists of minimizing $|O|$ and maximizing $|I|$.

Thus one can take minimal elements in $T(\mathcal{E}_\emptyset)$ as inputs I and then look for minimal elements in $T(\mathcal{E}_I)$. If they have the same size then we can conclude that they are a proper input/output pair for deterministic computation. This allows one to characterise the possible deterministic computations for small graphs (as it is not polynomial to compute the big transversal sets). For instance in the case of the 2×3 grid, the test shows that the minimal number of outputs is 2 and that there are only 3 solutions up to symmetry (see Fig. 2).

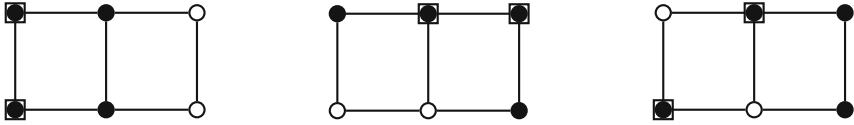


Fig. 2. Uniform deterministic choice of inputs for the 2×3 grid – input (resp. output) vertices are represented by squared (resp. white) vertices.

7 Uniform Constant Probability

The constant probability case is at the same time the most general case where information is not lost during the measurement and the less understood case. In this last section, we investigate some properties of the graph states that guarantee constant probability. We show a decomposition theorem into a gflow part and an internal set and we characterise open graphs with constant probability in the particular case of one input and one output. We also prove a reversibility property in the considered cases.

Lemma 5. *If an open graph (G, I, O) with $|I| = |O|$ guarantees uniform constant probability then there exists a subgraph G' of G such that (G', I, O) has a gflow and $V(G) \setminus V(G')$ is an internal set.*

Proof. Inductively removing the empty neighborhood subsets (W such that $Odd(W) \cap W^C = \emptyset$) leaves an open graph with gflow. □

Theorem 10. *An open graph (G, I, O) with $|I| = |O| = 1$ guarantees uniformly constant probability if and only if $\forall u \in V(G)$,*

$$d(u) \equiv 1 \pmod{2} \iff u \in I \Delta O$$

where $d(u) = |\mathcal{N}_G(u)|$ is the degree of u .

Proof. Consider a constant probability open graph $(G, \{i\}, \{o\})$, by definition there is no strongly internal set. We prove by contradiction that if $i = o$ then all the vertices have even degree and that if $i \neq o$ the input and output vertices have odd degree and all the other vertices have an even degree. Indeed:

- if $i = o$ then
 - if $d(i) \equiv 1 \pmod{2}$ then $V(G) \setminus \{i\}$ is a strongly internal set.
 - if $d(i) \equiv 0 \pmod{2}$ and there exists $u \neq i, d(u) \equiv 1 \pmod{2}$. Consider the shortest path P between the output and a vertex of odd degree. $Odd(G \setminus P) \cap (G \setminus P)^C = \{i\}$ thus $V(G) \setminus P$ is a strongly internal set.
- if $i \neq o$ then
 - if $d(o) \equiv 0 \pmod{2}$ then $V(G) \setminus \{o\}$ is a strongly internal set.
 - if $d(o) \equiv 1 \pmod{2}$, then if there exists $u \notin \{i, o\}$ with $d(u) \equiv 1 \pmod{2}$.

Consider the shortest path P between the output and a non input vertex of odd degree. If $i \notin P$ then $Odd(G \setminus P) \cap (G \setminus P)^C = \emptyset$ thus $V(G) \setminus P$ is a strongly internal set. Otherwise, if $d(i) = 1 \pmod 2$ then $Odd(G \setminus P) \cap (G \setminus P)^C = \{i\}$ thus $V(G) \setminus P$ is a strongly internal set. Otherwise consider $P' \subset P$ the part of the path from o to i , $Odd(G \setminus P') \cap (G \setminus P')^C = \{i\}$ thus $V(G) \setminus P'$ is a strongly internal set. If $d(i) = 0 \pmod 2$, then, as the sum of the degrees is even, there exists $u \notin \{i, o\}$ with $d(u) = 1 \pmod 2$ and thus a strongly internal set.

For the other direction, suppose that $(G, \{i\}, \{o\})$ satisfies that $\forall u \in V(G)$, $d(u) = 1 \pmod 2$ iff $u \in \{i\} \Delta \{o\}$. For any subset S of $V(G) \setminus \{i, o\}$ as $\sum_{v \in S} d(v) = 0 \pmod 2$, $|Odd(S) \cap S^C| = 0 \pmod 2$ and thus there is no strongly internal set if $i = o$. Furthermore, if $i \neq o$, for any set S of $V(G) \setminus \{o\}$ containing i , S contains one vertex of odd degree thus $|Odd(S) \cap S^C| = 1 \pmod 2$ and therefore there is no strongly internal set. \square

8 Open Questions

This work raises several open questions, from the structural point of view. For example, it is not known whether the uniform constant probability case is reversible when $|I| = |O|$. From a complexity perspective: is it possible to derive a polynomial algorithm to characterise the uniform equiprobability class and the uniform constant probability class? Is it possible to derive an efficient algorithm for finding inputs and outputs?

Acknowledgements. The authors want to thank E. Kashefi for discussions. This work is supported by CNRS-JST Strategic French-Japanese Cooperative Program, and Special Coordination Funds for Promoting Science and Technology in Japan.

References

1. Browne, D.E., Kashefi, E., Mhalla, M., Perdrix, S.: Generalized flow and determinism in measurement-based quantum computation. *New J. Phys.* **9**, 250 (2007)
2. Danos, V., Kashefi, E., Panangaden, P.: The measurement calculus. *J. ACM* **54**, 2 (2007)
3. Danos, V., Kashefi, E., Panangaden, P., Perdrix, S.: Extended measurement calculus. In: Gay, S., Mackie, I. (eds.) *Semantic Techniques in Quantum Computation*. Cambridge University Press, Cambridge (2010)
4. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology, Pasadena (1997)
5. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. *Phys. Rev. A* **69**, 062311 (2004)
6. Kashefi, E., Markham, D., Mhalla, M., Perdrix, S.: Information flow in secret sharing protocols. In: *Developments in Computational Models (DCM'09)*, EPTCS **9**, pp. 87–97 (2009)
7. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. *Phys. Rev. A* **78**, 042309 (2008)

8. Mhalla, M., Perdrix, S.: Finding optimal flows efficiently. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M., Ingólfssdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part I. LNCS, vol. 5125, pp. 857–868. Springer, Heidelberg (2008)
9. Raussendorf, R., Briegel, H.: A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188 (2001)
10. Van den Nest, M., Dehaene, J., De Moor, B.: Graphical description of the action of local Clifford transformations on graph states. *Phys. Rev. A* **69**, 22316 (2004)
11. Van den Nest, M., Miyake, A., Dür, W., Briegel, H.J.: Universal resources for measurement-based quantum computation. *Phys. Rev. Lett.* **97**, 150504 (2006)

Quantum Discord in Quantum Information Theory – From Strong Subadditivity to the Mother Protocol

Vaibhav Madhok¹ and Animesh Datta²(✉)

¹ Center for Quantum Information and Control, University of New Mexico, Albuquerque, NM 87131-0001, USA

² Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU Oxford, UK

animesh.datta@physics.ox.ac.uk

Abstract. Positivity of quantum discord is shown to be equivalent to the strong sub additivity of the von Neumann entropy. This leads to a connection between the mother protocol of quantum information theory [17] and quantum discord. We exploit this to show that discord is a measure coherence in the performance of the mother protocol. Since the mother protocol is a unification of an important class of problems (those that are bipartite, unidirectional and memoryless), we show discord to be a measure of coherence in these protocols. Our work generalizes an earlier operational interpretation of discord provided in terms of quantum state merging [10].

1 Introduction

Why quantum mechanics provides enhancements and speedups over best known classical procedures forms one of the most fundamental questions in quantum information science. This has canonically been answered in terms of quantum entanglement [1, 2]. This is however far from complete. There are quantum processes which provide an exponential advantage in the presence of little or no entanglement [3, 4]. In the realm of mixed-state quantum computation, quantum discord [5, 6] has been proposed as resource [8] and there are already some formal proofs in that direction [9]. The role of quantum discord in quantum information theory, however, still remains unclear. Recently, operational interpretations for quantum discord have been provided in terms of the quantum state merging protocol [10, 11]. In this paper, we go beyond this by exhibiting the role of quantum discord in essentially *all* quantum information processing protocols.

Quantum discord aims at capturing all quantum correlations in a quantum state, including entanglement [5–7]. Quantum mutual information is generally taken to be the measure of total correlations, classical and quantum, in a quantum state. For two systems, A and B , it is defined as $I(A : B) = S(A) + S(B) - S(A, B)$, where $S(\cdot)$ stands for the von Neumann entropy, $S(\rho) \equiv -\text{Tr}(\rho \log \rho)$. In our paper, all logarithms are taken to base 2. For a classical probability distribution, Bayes' rule leads to an equivalent definition of the mutual

information as $I(A : B) = S(A) - S(A|B)$, where the conditional entropy $S(A|B)$ is an average of the Shannon entropies of A , conditioned on the alternatives of B . It captures the ignorance in A once the state of B has been determined. For a quantum system, this depends on the measurements that are made on B . For a POVM given by the set $\{\Pi_i\}$, the state of A after the measurement corresponding to the outcome i is given by

$$\rho_{A|i} = \text{Tr}_B(\Pi_i \rho_{AB}) / p_i, \quad p_i = \text{Tr}_{A,B}(\Pi_i \rho_{AB}). \quad (1)$$

A quantum analogue of the conditional entropy can then be defined as $\tilde{S}_{\{\Pi_i\}}(A|B) \equiv \sum_i p_i S(\rho_{A|i})$, and an alternative version of the quantum mutual information can now be defined as $\mathcal{J}_{\{\Pi_i\}}(A : B) = S(A) - \tilde{S}_{\{\Pi_i\}}(A|B)$. The above quantity depends on the chosen set of measurements $\{\Pi_i\}$. To capture all the classical correlations present in ρ_{AB} , we maximize $\mathcal{J}_{\{\Pi_i\}}(A : B)$ over all $\{\Pi_i\}$, arriving at a measurement independent quantity $\mathcal{J}(A : B) = \max_{\{\Pi_i\}}(S(A) - \tilde{S}_{\{\Pi_i\}}(A|B)) \equiv S(A) - \tilde{S}(A|B)$, where $\tilde{S}(A|B) = \min_{\{\Pi_i\}} \tilde{S}_{\{\Pi_i\}}(A|B)$. Since the conditional entropy is concave over the set of POVMs, which is convex, the minimum is attained on the extreme points of the set of POVMs, which are rank 1 [12]. Then, quantum discord is finally defined as

$$\begin{aligned} \mathcal{D}(A : B) &= I(A : B) - \mathcal{J}(A : B) \\ &= S(A) - S(A : B) + \min_{\{\Pi_i\}} \tilde{S}_{\{\Pi_i\}}(A|B), \end{aligned} \quad (2)$$

where $\{\Pi_i\}$ are now, and henceforth in the paper, rank 1 POVMs. It is well known that the quantum discord is non-negative for all quantum states [6, 12].

Our endeavour in this paper shall be to clarify the role of quantum discord in quantum information theory. We shall show how discord quantifies the coherence in a large class of quantum resource inequalities, beginning with the so-called ‘mother protocol’. Our way into the heart of quantum information theory will be through strong sub-additivity (SSA) of von Neumann entropy. SSA is one of the most fundamental inequalities in information theory, quantum and classical. We shall use a simple proof of SSA provided by quantum state merging protocol [15, 16], to lead us onto the mother protocol of quantum information theory [17]. The mother protocol which can be thought of as the fully quantum Slepian-Wolf protocol, achieving quantum communication-assisted entanglement distillation, and state transfer from the sender to the receiver. It also has as its children several important and common protocols like quantum teleportation and entanglement distillation. We shall discuss the role of quantum discord in the performance of the noisy versions these protocols in the final section of our paper.

2 Quantum Discord and Strong Subadditivity

We begin by providing a new proof of the positivity of quantum discord [6] by casting it in terms of the SSA of von Neumann entropy.

Theorem 1. *Strong subadditivity of the von Neumann entropy implies nonnegativity of the quantum discord.*

Proof: Consider the joint state ρ_{AB} subject to one dimensional orthogonal measurements $\Pi_j = |e_j\rangle\langle e_j|$ on B , extended to arbitrary (at most $\dim(B)^2$) dimensions. Then

$$p_j \rho_{A|j} = \text{Tr}_B(\rho_{AB}\Pi_j) = \langle e_j|\rho_{AB}|e_j\rangle, \quad p_j = \text{Tr}_B(\rho_B\Pi_j) = \langle e_j|\rho_B|e_j\rangle.$$

Note that the measurement is made on the system B , while in the definition of discord, it was on A . Discord is not symmetric under the exchange of the subsystems, but this is not a concern as we just as well have proved the result for $\mathcal{D}(B, A)$.

Suppose now that a system C interacts with B so as to make the desired measurement ($U|e_j\rangle \otimes |0\rangle = |e_j\rangle \otimes |f_j\rangle$), leaving the state

$$\rho'_{ABC} = \sum_{j,k} \langle e_j|\rho_{AB}|e_k\rangle \otimes |e_j\rangle\langle e_k| \otimes |f_j\rangle\langle f_k|. \tag{3}$$

If the eigendecomposition of $\rho_{AB} = \sum_l \lambda_l |r_l\rangle\langle r_l|$, then

$$\rho'_{ABC} = \sum_{j,k,l} \lambda_l \langle \mathbb{I}_A, e_j|r_l\rangle\langle r_l|\mathbb{I}_A, e_k\rangle \otimes |e_j\rangle\langle e_k| \otimes |f_j\rangle\langle f_k| = \sum_l \lambda_l |e_l, r_l, f_l\rangle\langle e_l, r_l, f_l|$$

whereby

$$S(\rho'_{ABC}) = S(\rho_{AB}).$$

Also, from Eq. (3),

$$\rho'_{AB} = \sum_j p_j \rho_{A|j} \otimes |e_j\rangle\langle e_j|, \quad \text{so } S(\rho'_{AB}) = S(\mathbf{p}) + \sum_j p_j S(A|j), \tag{4a}$$

$$\rho'_{BC} = \sum_{j,k} |e_j\rangle\langle e_k| \rho_B |e_k\rangle\langle e_k| \otimes |f_j\rangle\langle f_k|, \quad \text{so } S(\rho'_{BC}) = S(\rho_B), \tag{4b}$$

$$\rho'_B = \sum_j p_j |e_j\rangle\langle e_j|, \quad \text{so } S(\rho'_B) = S(\mathbf{p}). \tag{4c}$$

Now use the strong subadditivity of the von Neumann entropy [13] which is

$$S(\rho'_{ABC}) + S(\rho'_B) \leq S(\rho'_{AB}) + S(\rho'_{BC}). \tag{5}$$

Equations (4a–4c) reduce this to

$$S(\rho_{AB}) + S(\mathbf{p}) \leq S(\mathbf{p}) + \sum_j p_j S(A|j) + S(\rho_B), \tag{6}$$

whereby

$$\tilde{S}_{\{\Pi_j\}}(A|B) \equiv \sum_j p_j S(A|j) \geq S(\rho_{AB}) - S(\rho_B) \equiv S(A|B). \tag{7}$$

This, being true for all measurements, also holds for the minimum. So

$$\mathcal{D}(A, B) = \min_{\{\Pi_j\}} \tilde{S}_{\{\Pi_j\}}(A|B) - S(A|B) \geq 0.$$

□

This theorem shows that quantum discord and SSA are intimately connected, in that the existence of the former is guaranteed by the validity of the latter, and the nullity of the former is guaranteed by the saturation of the latter. We have shown that for any bipartite state, we can introduce a third system that executes a measurement on one of the subsystems, and the resulting tripartite system allows us to investigate the role of quantum discord in quantum information theory.

3 Interpreting Quantum Discord Through Quantum State Merging via SSA

Quantum state merging protocol is the extension of the classical Slepian-Wolf protocol [14] into the quantum domain where Alice and Bob share the quantum state $\rho_{AB}^{\otimes n}$, with each party having the marginal density operators $\rho_A^{\otimes n}$ and $\rho_B^{\otimes n}$ respectively. Let $|\Psi_{ABC}\rangle$ be a purification of ρ_{AB} . Assume, without loss of generality, that Bob holds C . The quantum state merging protocol quantifies the minimum amount of quantum information which Alice must send to Bob so that he ends up with a state arbitrarily close to $|\Psi\rangle_{B'BC}^{\otimes n}$, B' being a register at Bob's end to store the qubits received from Alice. It was shown that in the limit of $n \rightarrow \infty$, and asymptotically vanishing errors, the answer is given by the quantum conditional entropy [15, 16]: $S(A|B) = S(A, B) - S(B)$. When $S(A|B)$ is negative, Bob obtains the full state with just local operations and classical communication, and distill $-S(A|B)$ ebits with Alice, which can be used to transfer additional quantum information in the future.

That quantum discord has an operational interpretation in terms of quantum state merging was shown in [10, 11]. In [10], it was shown that discord is the markup in the cost of quantum communication in the process of quantum state merging, if one discards relevant prior information. SSA served as a crucial link in this exercise. An intuitive argument for the above interpretation of quantum discord can be made through strong subadditivity, which can also be written as [15, 16]

$$S(A|B, C) \leq S(A|B). \quad (8)$$

From the point of view of the state merging protocol, the above has a very clear interpretation: having more prior information makes state merging cheaper. Or in other words, throwing away information will make state merging more expensive. Thus, if Bob discards system C , it will increase the cost of quantum communication needed by Alice in order to merge her state with Bob. Our goal now is to take these results a step further. In particular, we show that we can interpret discord in terms of the mother protocol [17] and thus elucidate its connection to all the children protocols that can be derived from the mother.

4 The Mother Protocol

We begin by briefly describing the Mother protocol and its generalization to the fully quantum Slepian Wolf (FQSW) protocol. The mother protocol [17] is a transformation of a quantum state $(|\Psi^{ABR}\rangle)^{\otimes n}$. At the start, Alice holds the A shares and Bob the B shares. The reference system R is purifying the AB system and does not actively participate in the protocol. The Mother protocol can be viewed as an entanglement distillation between A and B when the only type of communication permitted is the ability to send qubits from Alice to Bob. The transformation can be expressed concisely in the resource inequality formalism as [18]

$$\langle \Psi^{AB} \rangle + \frac{1}{2}I(A : R)[q \rightarrow q] \geq \frac{1}{2}I(A : B)[qq]. \quad (9)$$

The above inequality means that n copies of the state Ψ can be converted to $\frac{1}{2}I(A : B)$ EPR pairs ($[qq]$) per copy, provided Alice is allowed to communicate with Bob by sending him qubits at the rate $\frac{1}{2}I(A : R)$ ($[q \rightarrow q]$) per copy.

One can generalize the mother protocol to a stronger inequality known as the FQSW protocol. This inequality states that starting from the state $(|\Psi^{ABR}\rangle)^{\otimes n}$, and using $\frac{1}{2}I(A : R)$ bits of quantum communication from Alice to Bob, they can distill $\frac{1}{2}I(A : B)$ EPR pairs per copy, and in addition Alice can accomplish merging her state with Bob. In the process of accomplishing state merging, they create the state $(|\Phi^{\hat{B}R}\rangle)^{\otimes n}$, where \hat{B} is a register held with B and $\Psi^R = \Phi^R$. Since all purifications are equivalent up to local unitaries, Bob can convert $\Phi^{\hat{B}}$ to Ψ^{AB} at his end and thus complete the state merging with Alice. Hence in the state merging task, as described above, Alice is able to successfully transfer her entanglement with the reference system R to Bob. Writing the FQSW in terms of a resource inequality

$$\langle \mathcal{W}^{S \rightarrow AB} : \Psi^S \rangle + \frac{1}{2}I(A : R)[q \rightarrow q] \geq \frac{1}{2}I(A : B)[qq] + \langle id^{S \rightarrow \hat{B}} : \Psi^S \rangle. \quad (10)$$

The above inequality is another way of expressing the FQSW protocol, where we accomplish state merging as well as entanglement distillation. The state S on the left-hand side of the inequality, is distributed to Alice and Bob, while on the right-hand side, that same state is given to Bob alone. $\mathcal{W}^{S \rightarrow AB}$ is an isometry taking the system S to AB [17]. The FQSW protocol is valid asymptotically in the limit of a large number of copies and this is denoted by the symbol \geq .

4.1 Quantum State Merging Primitive from FQSW

We start by expressing the quantum state merging protocol [15, 16] as a resource inequality

$$\langle \Psi^{AB} \rangle + S(A|B)[q \rightarrow q] + I(A : B)_\psi[c \rightarrow c] \geq \langle id^{S \rightarrow \hat{B}} : \Psi^S \rangle. \quad (11)$$

This accomplishes state merging from Alice to Bob at the cost of $S(A|B)$ bits of quantum communication. In the case when $S(A|B)$ is negative, Alice and Bob can distill this amount of entanglement in the form of Bell pairs. Quantum state merging thus provides an operational interpretation of $S(A|B)$, assuming we ignore the amount of classical communication needed to accomplish the required state merging.

We can derive quantum state merging from the FQSW if the entanglement produced at the end of the FQSW protocol, can be used to perform teleportation. We can see this through simple manipulation of the resource inequalities described above. We start by describing quantum teleportation as

$$[qq] + 2[c \rightarrow c] \succeq [q \rightarrow q]. \quad (12)$$

It means that one requires a shared ebit and two bits of classical communication to accomplish teleportation of a quantum state. The symbol \succeq is used to denote exact attainability as compared to \geq which is to denote asymptotic attainability. From the FQSW protocol (Eq. 2.3), using the entanglement produced at the end for quantum communication (Eq. 2.5), one gets the quantum state merging primitive (Eq. 2.4).

5 Discord as a Measure of the Coherence of the Mother Protocol

In this section we present our main result, that quantum discord is a measure of how coherently the mother protocol is performed between two parties, Alice and Bob. More specifically, we will study the loss of information and coherence at Bob's end. To that end, we consider arbitrary quantum operations to model decoherence. We also consider a quantum operation where quantum measurements are made at Bob's end and the results are discarded. In practice, such a pre-measurement state can be due to the environment assisted decoherence.

To begin, expand the size of the Hilbert space so that an arbitrary pre-measurement (or any other quantum operation) can be modeled by coupling to the auxiliary subsystem and then discarding it. We assume C to initially be in a pure state $|\mathbf{0}\rangle$, and a unitary interaction U between B and C . Letting primes denote the state of the system after U has acted, we have $S(A, B) = S(A, BC)$ as C starts out in a product state with AB . We also have $I(A : BC) = I(A' : B'C')$. As discarding quantum systems cannot increase the mutual information, we get $I(A' : B') \leq I(A' : B'C')$. Now consider the FQSW protocol between A and B in the presence of C . We have $S(A|B) = S(A) - I(A : B) = S(A) - I(A : BC) = S(A|BC)$. After the application of the unitary U , but before discarding the subsystem C , the cost of merging is still given by $S(A'|B'C') = S(A|B)$. This implies that one can always view the cost of merging the state of system A with B , as the cost of merging A with the system BC , where C is some ancilla (initially in a pure state) with which B interacts coherently through a unitary U . Such a scheme does not change the cost of state merging, as shown, but helps

us in counting resources. Discarding system C yields

$$I(A' : B') \leq I(A' : B'C') = I(A : BC) = I(A : B), \tag{13}$$

or alternatively,

$$S(A'|B') \geq S(A'|B'C') = S(A|B). \tag{14}$$

Now consider a protocol which we call as $FQSWD_B$, (Fully Quantum Slepian Wolf after decoherence) where the subscript refers to the decoherence at B. The resource inequality for $FQSWD_B$ is

$$\langle \mathcal{U}^{S \rightarrow A'B'} : \Psi^S \rangle + \frac{1}{2}I(A' : R')[q \rightarrow q] \geq \frac{1}{2}I(A' : B')[qq] + \langle id^{S \rightarrow \hat{B}} : \Psi^S \rangle. \tag{15}$$

As in the fully coherent version, Alice is able to transfer her entanglement with the reference system R' , and is able to distill $\frac{1}{2}I(A' : B')$ EPR pairs ($[qq]$) with Bob. The net gain, G , for the fully coherent protocol is $\frac{1}{2}I(A : B) - \frac{1}{2}I(A : R) = -S(A|B)$. This is the difference between the yield obtained and the cost of quantum communication incurred. Likewise, the net gain, G_D , for the protocol suffering from decoherence at B is $\frac{1}{2}I(A' : B') - \frac{1}{2}I(A' : R') = -S(A'|B')$. Therefore, the net advantage, $G - G_D$, of the coherent protocol over the decohered one is given by $D = S(A'|B') - S(A|B)$.

We now show that the minimum of D over all possible measurements is the quantum discord \mathcal{D} . The state ρ_{AB} , under measurement of subsystem B , changes to $\rho'_{AB} = \sum_j p_j \rho_{A|j} \otimes \pi_j$, where $\{\pi_j\}$ are orthogonal projectors resulting from a Neumark extension of the POVM elements. The unconditioned post measurement states of A and B are

$$\rho'_A = \sum_j p_j \rho_{A|j} = \rho_A, \quad \rho'_B = \sum_j p_j \pi_j.$$

Computing the value of $I(A' : B')$, we get

$$\begin{aligned} I(A' : B') &= S(A') + S(B') - S(A', B'), \\ &= S(A') + H(p) - \left\{ H(p) + \sum_j p_j S(\rho_{A|j}) \right\}, \\ &= S(A) - \sum_j p_j S(\rho_{A|j}). \end{aligned} \tag{16}$$

After maximization, it reduces to $\mathcal{J}(\rho_{AB})$, as defined earlier as is the reduction to rank 1 POVMs. One might consider reverting to Zurek's original definition of quantum discord, which incidentally first appeared in [5]. Then one does not have to throw in the maximization; discord quantifies the increase in quantum state merging due to environmental projection, and hence the quantity \mathcal{D} serves as a valid measure for the net loss in the number of EPR pairs in the mother protocol due to the environment. The above connection between discord and the mother protocol suggests that discord can also serve as a measure of coherence in accomplishing any of the children protocols that can be derived from the mother. We illustrate this in the next section.

6 Role of Discord in the Children Protocols

In this section we see that by connecting quantum discord with the FQSW protocol, we can interpret discord as the advantage of quantum coherence in various scenarios. There in lies the power of our approach.

6.1 Discord as the Mark Up in the Cost of Quantum Communication to State Merging

We can easily derive the results of [10] from the previous section. In particular, consider the $QSMD_B$ (Quantum state merging protocol with decoherence at party B). One can get $QSMD_B$ from $FQSWD_B$ if one recycles the entanglement produced at the end of the $FQSWD_B$ protocol to perform quantum teleportation. We start by expressing $QSMD_B$ in the form of a resource inequality,

$$\langle \Psi^{A'B'} \rangle + S(A'|B')[q \rightarrow q] + I(A' : B')_\psi [c \rightarrow c] \geq \langle id^{S \rightarrow \hat{B}} : \Psi^S \rangle. \tag{17}$$

The optimal cost of quantum communication in this case is $S(A'|B')$. Thus the mark up in this cost is $S(A'B') - S(A|B)$, which is equal to the quantum discord of the original state. It is to be noted that we will always have this mark up, regardless of the cost of classical communication incurred.

6.2 Quantum Discord and Noisy Super-Dense Coding

The noisy super-dense coding can be derived by combining the mother with super-dense coding [19]. It can be expressed in the form of the resource inequality as,

$$\langle \Psi^{AB} \rangle + S(A)[q \rightarrow q] \geq I(A : B)[c \rightarrow c]. \tag{18}$$

When the party B is undergoing decoherence, the noisy superdense coding can be expressed as,

$$\langle \Psi^{A'B'} \rangle + S(A')[q \rightarrow q] \geq I(A' : B')[c \rightarrow c]. \tag{19}$$

We note that $S(A) = S(A')$. Thus, due to decoherence, the number of classical bits communicated through this protocol gets reduced by the amount $I(A : B) - I(A' : B')$, which is equal to the discord of the original state.

6.3 Quantum Discord and Entanglement Distillation

The one way entanglement distillation can be expressed as [20,21],

$$\langle \Psi^{AB} \rangle + I(A : R)[c \rightarrow c] \geq I(A)B[qq]. \tag{20}$$

In the above equation, $I(A|B)[qq] = -S(A|B)$, and is also known as the coherent information [22,23]. When the party B is undergoing decoherence we get,

$$\langle \Psi^{A'B'} \rangle + I(A' : R')[c \rightarrow c] \geq I(A')B'[qq]. \quad (21)$$

The net loss in entanglement distillation is equal to $S(A'|B') - S(A|B)$ which again is the quantum discord of the original state. As is well known, classical communication between parties cannot enhance entanglement, and we can neglect the difference in $I(A : R) - I(A' : R')$ classical bits required.

7 Conclusion

Our work elucidates the role non classical correlations, those captured by quantum discord, play in quantum information processing tasks. For an important class of problems described above, quantum discord is shown to be a measure of how coherently the protocol was performed. We have quantified the cost due to decoherence we suffer in quantum communication protocols and this is aptly captured by discord. We hope that this work places quantum discord at the heart of quantum information theory, and demonstrates the vital role it plays in quantifying the cost of decoherence in almost all quantum information processing protocols.

Acknowledgments. This work was supported in part by the EPSRC (EP/H03031X/1), the EC integrated project Q-ESSENCE, US European Office of Aerospace Research (FA8655-09-1-3020), and the Center for Quantum Information and Control (CQuIC) where this work was done, and NSF Grant Nos. 0903953 and 0903692.

References

1. Plenio, M.B., Virmani, S.: *Quant. Inf. Comp.* **7**, 1 (2007)
2. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: *Rev. Mod. Phys.* **81**, 865 (2009)
3. Datta, A., Flammia, S.T., Caves, C.M.: *Phys. Rev. A* **72**, 042316 (2005)
4. Datta, A., Vidal, G.: *Phys. Rev. A* **75**, 042310 (2007)
5. Zurek, W.H.: *Ann. Phys. (Leipzig)* **9**, 855 (2000)
6. Ollivier, H., Zurek, W.H.: *Phys. Rev. Lett.* **88**, 017901 (2002)
7. Henderson, L., Vedral, V.: *J. Phys. A: Math. Gen.* **34**, 6899 (2001)
8. Datta, A., Shaji, A., Caves, C.M.: *Phys. Rev. Lett.* **100**, 050502 (2008)
9. Eastin, B.: arxiv:1006.4402 (2010)
10. Madhok, V., Datta, A.: *Phys. Rev. A* **83**, 032323 (2011)
11. Cavalcanti, D., Aolita, L., Boixo, S., Modi, K., Piani, M., Winter, A.: *Phys. Rev. A* **83**, 032324 (2011)
12. Datta, A.: Studies on the role of entanglement in mixed-state quantum computation, Ph.D thesis, University of New Mexico, arxiv:0807.4490 (2008)
13. Lieb, E.H., Ruskai, M.B.: *J. Math. Phys.* **12**, 1938 (1973)
14. Cover, T., Thomas, J.: *Elements of Information Theory*. Wiley & Sons, New York (2006)

15. Horodecki, M., Oppenheim, J., Winter, A.: *Nature* **436**, 673 (2005)
16. Horodecki, M., Oppenheim, J., Winter, A.: *Comm. Math. Phys.* **268**, 107 (2007)
17. Abeyesinghe, A., Devetak, I., Hayden, P., Winter, A.: *Proc. R. Soc. A* **465**, 2537 (2009)
18. Devetak, I., Harrow, A.W., Winter, A.: *IEEE Trans. Inf. Theory* **54**, 4587 (2008)
19. Horodecki, M., Horodecki, P., Horodecki, R., Leung, D.W., Terhal, B.M.: *Quantum Inf. Comput.* **1**, 70 (2001)
20. Devetak, I., Winter, A.: *Proc. R. Soc. Lond. A* **461**, 207 (2005)
21. Devetak, I., Winter, A.: *Phys. Rev. Lett.* **93**, 080501 (2004)
22. Schumacher, B.: *Phys. Rev. A* **54**, 2614 (1996)
23. Schumacher, B., Nielsen, M.A.: *Phys. Rev. A* **54**, 2629 (1996)

Local Unitary Group Stabilizers and Entanglement for Multiqubit Symmetric States

Curt D. Cenci¹, David W. Lyons¹(✉), and Scott N. Walck²

¹ Mathematical Sciences, Lebanon Valley College, Annville, PA, USA
lyons@lvc.edu

² Physics, Lebanon Valley College, Annville, PA, USA

Abstract. We refine recent local unitary entanglement classification for symmetric pure states of n qubits (that is, states invariant under permutations of qubits) using local unitary stabilizer subgroups and Majorana configurations.

1 Introduction

The question of when a given multipartite state can be converted to another by local operations and measurements of subsystems is crucial in quantum information science [1]. The fact that entangled states play a role as resources in computation and communication protocols motivates problems of measurement and classification of entanglement. In general, these are difficult problems, already rich for the case of pure states of n -qubits, where the number of real parameters necessary for classifying entanglement types grows exponentially in n .

A promising special case for the general problem of entanglement measurement and classification is that of the symmetric states, that is, states of composite systems that are invariant under permutation of the subsystems. Symmetric states admit simplified analyses, and they are of interest in their own right. Examples of recent work in which permutation invariance has made possible results where the general case remains intractable include: geometric measure of entanglement [2–4], efficient tomography [5], classification of states equivalent under stochastic local operations and classical communication (SLOCC) [6, 7], and our own work on classification of states equivalent under local unitary (LU) transformations [8].

The main result of this paper (Theorem 3 below) is a classification of LU equivalence classes of n -qubit symmetric states that refines our own previous work [8], which is based on the following idea. Suppose states ρ, ρ' are local unitary equivalent via some LU transformation U , that is, we have $\rho' = U\rho U^\dagger$. If a local unitary operator V stabilizes ρ , then UVU^\dagger stabilizes ρ' . The consequence is that stabilizer subgroups of locally equivalent states are isomorphic via conjugation. Thus the isomorphism class of the stabilizer is an LU invariant. This inspires a two-stage classification program.

1. Classify LU stabilizer subgroup conjugacy classes.
2. Classify LU classes of states, that is, distinct entanglement types of states, for each of the stabilizer classes from stage 1.

Analysis of both stages 1 and 2 for symmetric states makes use of the Majorana representation for pure symmetric states: Given a collection $|\psi_1\rangle, \dots, |\psi_n\rangle$ of 1-qubit states, we can symmetrize to form the state

$$|\psi\rangle = \alpha \sum_{\pi} |\psi_{\pi(1)}\rangle |\psi_{\pi(2)}\rangle \cdots |\psi_{\pi(n)}\rangle$$

where π ranges over all $n!$ permutations of the n -qubits, and α is a normalization factor. It is a fact (see [6]) that *any* symmetric pure state can be written as such a symmetrization, and further, that the set of n 1-qubit states whose symmetrization is $|\psi\rangle$ is unique up to phase factors. Thus the set of symmetric pure states is in one-to-one correspondence with configurations of multisets (one or more of the 1-qubit states may be repeated) of n of points on the Bloch sphere.

Using the fact that a rotation of the Bloch sphere corresponds to unitary operation on 1-qubit states, it is a simple observation that a rotation of the Majorana configuration of points representing a state $|\psi\rangle$ results in an LU equivalent state $|\psi'\rangle = V^{\otimes n} |\psi\rangle$, where V is the 2×2 unitary operator corresponding to the given rotation of the sphere. Not obvious, but true nonetheless, is that given *any* LU operation $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$ that transforms a symmetric state $|\psi\rangle$ to another symmetric state $|\psi'\rangle$, there is a 1-qubit operation V such that $|\psi'\rangle = V^{\otimes n} |\psi\rangle$. This was proved by Mathonet et al. [14] for SLOCC operations on pure symmetric states. We show in Theorem 1 below that this holds more generally for LU operations on *mixed* symmetric states. A consequence (Theorem 2) is that ρ, ρ' are LU equivalent if and only if their Majorana configurations can be interchanged by a rotation of the Bloch sphere.

In previous work [8–13], we have exploited the Lie algebra structure of the tangent space of infinitesimal LU transformations, which is a linearization of the stabilizer subgroup, to achieve results in both of these stages for various classes of states. A strength of this method is that linear Lie algebra computations are more tractable than the corresponding nonlinear Lie group computations. The drawback is that a Lie algebra detects only the connected component at the identity element of the corresponding Lie group. A stabilizer subalgebra does not “see” the discrete part of the stabilizer subgroup. For example, the Lie stabilizer subalgebra is the zero vector space for most stabilizer states, that is, states stabilized by the full n -qubit Pauli group. Group level information is necessary to capture the local unitary stabilizer properties of such states.

In Theorems 1 and 2 of [8], we classify four infinite families and 1 discrete family (that is, the zero vector space) of stabilizer subalgebras for pure symmetric states, and identify LU classes of pure symmetric states that have those stabilizers. The main result of this paper, Theorem 3 below, advances this previous subalgebra classification to the group level. We show there are six classes of infinite LU stabilizer groups, inequivalent under isomorphism by local unitary conjugation, and classify their corresponding LU-inequivalent states. Discrete

LU stabilizer subgroups are isomorphic to finite subgroups of $SO(3)$. These are the cyclic groups, the dihedral groups, and the symmetry groups of the five Platonic solids.

2 Preliminaries

We take n -qubit state space to be the set of $2^n \times 2^n$ density matrices (positive semidefinite matrices with trace 1). Pure states are represented by density matrices of rank 1. We write $|D_n^{(k)}\rangle$ to denote the Dicke state with k excitations.

We take the local unitary group to be $PU(2)^n$, where $PU(2) = U(2)/\{\lambda \text{ Id} : \lambda \in \mathbb{C}|\lambda| = 1\}$, called the projective unitary group, is the set of projective equivalence classes of matrices in $U(2)$. That is, matrices g, h in $U(2)$ represent the same element in $PU(2)$ if and only if $g = \lambda h$ for complex number λ . The projective unitary group $PU(2)$ is isomorphic to the group $SO(3)$ of rotations of 3-dimensional Euclidean space via

$$\lambda \exp(-i\theta/2v \cdot \sigma) \leftrightarrow \text{rotation by } \theta \text{ radians about axis } v$$

where λ is a norm 1 complex number, θ is a real number, $v = (v_1, v_2, v_3)$ is a unit vector in \mathbb{R}^3 , and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices (see [1] Ex. 4.5.).

We will denote elements of $PU(2)$ and the local unitary group $PU(2)^n$ by their representatives g in $U(2)$ and $U = (g_1, \dots, g_n)$ in $U(2)^n$, and will write $g \equiv h$ or $U \equiv V$ to denote equality in $PU(2)$ and $PU(2)^n$, and will use the equals sign to indicate equality in $U(2)$ and $U(2)^n$. Similarly, we will write $|\psi\rangle \equiv |\phi\rangle$ to indicate that two state vectors are equal up to phase.

The local unitary group element $U = (g_1, \dots, g_n)$ acts on the density matrix ρ by

$$\rho \rightarrow U\rho U^\dagger = (g_1 \otimes \dots \otimes g_n) \rho (g_1 \otimes \dots \otimes g_n)^\dagger.$$

We denote by Stab_ρ the local unitary stabilizer subgroup for ρ

$$\text{Stab}_\rho = \{U \in PU(2)^n : U\rho U^\dagger = \rho\}.$$

3 Main Results

Theorem 1. *Let ρ, ρ' be n -qubit symmetric states, pure or mixed, with $n \geq 3$. Then ρ, ρ' are LU equivalent if and only if there exists an element g in $U(2)$ such that*

$$\rho' = (g^{\otimes n})\rho(g^{\otimes n})^\dagger.$$

Proof of Theorem 1. We only need to prove the “only if” direction. Let $\rho' = U\rho U^\dagger$, where

$$U = (g_1, g_2, \dots, g_n) = \prod_{j=1}^n g_j^{(j)}$$

is an LU transformation. Suppose there exist k, ℓ with $g_k \neq g_\ell$. Transposing the k -th and ℓ -th coordinates of U , let

$$V = g_\ell^{(k)} g_k^{(\ell)} \prod_{j \neq k, \ell} g_j^{(j)}$$

By symmetry, we have $\rho' = V\rho V^\dagger$, and therefore we have $\rho = (V^\dagger U)\rho(U^\dagger V)$.

Let $h = g_\ell^\dagger g_k$ so that we have

$$V^\dagger U = h^{(k)}(h^\dagger)^{(\ell)},$$

and choose u in $U(2)$ to diagonalize h , so that we have

$$uhu^\dagger \equiv \begin{bmatrix} e^{it} & \\ & e^{-it} \end{bmatrix}$$

for some t . Let us call this diagonal matrix d , and let $\tau = (u^{\otimes n})\rho(u^{\otimes n})^\dagger$, so that we have

$$\tau = d^{(k)}(d^\dagger)^{(\ell)} \tau (d^\dagger)^{(k)}d^{(\ell)}.$$

Let $\tau = \sum_{IJ} c_{IJ} |I\rangle \langle J|$ be the expansion of τ in the computational basis, where $I = i_1 \dots i_n, J = j_1 \dots j_n$ denote binary strings of length n and the c_{IJ} are complex coefficients. We claim that if $c_{IJ} \neq 0$, then $J = I$ or $J = I^c$, where I^c denotes the bit string obtained by taking the mod 2 complement of each bit in the string I . Suppose, on the other hand, that there exists a pair I, J such that $c_{IJ} \neq 0$ and $J \neq I$ and $J \neq I^c$. Then there exist two qubit labels k, ℓ such that $j_k j_\ell \neq i_k i_\ell$ and $j_k j_\ell \neq (i_k i_\ell)^c$. Without loss of generality, suppose $(i_k i_\ell) = 00$ and $(j_k j_\ell) = 01$. Since

$$d^{(k)}(d^\dagger)^{(\ell)} |00\rangle \langle 01| (d^\dagger)^{(k)}d^{(\ell)} = e^{-2it} |00\rangle \langle 01|$$

we must have $t = m\pi$ for some integer m . Then $d \equiv \text{Id}$, and so $h \equiv \text{Id}$, and therefore $g_k \equiv g_\ell$, contradicting our assumption. We conclude that

$$\tau = a |I\rangle \langle I| + b |I\rangle \langle I^c| + \bar{b} |I^c\rangle \langle I| + (1 - a) |I^c\rangle \langle I^c| \tag{1}$$

for some coefficients a, b and some bit string I .

Next we claim that we may assume $I = 0 \dots 0$ or $I = 1 \dots 1$. Suppose contrary that there are two qubit positions k, ℓ such that $i_k \neq i_\ell$. Choose any third qubit position r (this is where we use the hypothesis that $n \geq 3$). We must have $i_r = i_k$ or $i_r = i_\ell$. Without loss of generality, suppose $i_r = i_k$. Now transpose qubits ℓ, r . This produces a state $\tilde{\tau}$ with nonzero coefficient for the term $|I'\rangle \langle I'|$, where $i'_k = i'_\ell$. But this contradicts the fact that $\tilde{\tau} = \tau$ because τ is symmetric. This establishes the claim.

Next we claim that we may take b to be real and nonnegative in (1). If b is not real, let $\phi = \arg(b)/n$ if $I = 0 \dots 0$ and let $\phi = -\arg(b)/n$ if $I = 1 \dots 1$. Replacing τ by $(\text{diag}(1, e^{i\phi}))^{\otimes n} \tau (\text{diag}(1, e^{-i\phi}))^{\otimes n}$ establishes the claim.

Now apply the preceding argument to ρ' to construct a sequence of LU transformations that are the same in each qubit to obtain

$$\tau' = a' |I'\rangle \langle I'| + b' |I'\rangle \langle (I')^c| + \bar{b}' |(I')^c\rangle \langle I'| + (1 - a') |(I')^c\rangle \langle (I')^c|$$

for some real and nonnegative coefficients a', b' and some bit string $I' = 0 \cdots 0$ or $I' = 1 \cdots 1$. Comparing 1-qubit reduced density matrices for τ, τ' yields $a = a'$ or $a = 1 - a'$. If the latter, replace τ' by $(X, \dots, X) \tau' (X, \dots, X)$. Finally, comparing eigenvalues of τ, τ' , we conclude that $b = b'$. Thus we have constructed a chain of symmetric local unitary operations that transform ρ to ρ' , as desired. This concludes the proof of Theorem 1. \square

Theorem 2. *Let $|\psi\rangle, |\psi'\rangle$ be n -qubit symmetric states with Majorana configurations $\mathcal{C}_\psi, \mathcal{C}_{\psi'}$. Then $|\psi\rangle, |\psi'\rangle$ are local unitary equivalent if and only if there exists an element g in $U(2)$ such that*

$$\mathcal{C}_{\psi'} = g\mathcal{C}_\psi.$$

Proof of Theorem 2. Let $|\psi\rangle, |\psi'\rangle$ be symmetric states with Majorana configurations $\mathcal{C}_\psi = \{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ and $\mathcal{C}_{\psi'} = \{|\psi'_1\rangle, \dots, |\psi'_n\rangle\}$. If there is a rotation of the Bloch sphere given by g in $U(2)$ that takes \mathcal{C}_ψ to $\mathcal{C}_{\psi'}$, then (possibly after renumbering) we have $g|\psi_j\rangle \equiv |\psi'_j\rangle$ for $1 \leq j \leq n$, and hence $|\psi'\rangle \equiv g^{\otimes n} |\psi\rangle$. Conversely, if $|\psi'\rangle = U|\psi\rangle$ for some local unitary U , then by Theorem 1, there is a g in $U(2)$ such that $|\psi'\rangle = g^{\otimes n} |\psi\rangle$. We can interpret this g as a rotation of the Bloch sphere, and it is clear that we have $\mathcal{C}_{\psi'} = g\mathcal{C}_\psi$. \square

Theorem 3. *Let ρ be an n -qubit symmetric pure state whose local unitary stabilizer Stab_ρ is infinite. Then one of the following holds.*

- (i) *The state ρ is LU equivalent to the product state $\tau = |\psi\rangle \langle \psi|$, where $|\psi\rangle = |0 \cdots 0\rangle$ and Stab_ρ is isomorphic to $U(1)^n$, where $(e^{it_1}, \dots, e^{it_n})$ in $U(1)^n$ corresponds to*

$$(\exp(-it_1 Z/2), \dots, \exp(-it_n Z/2))$$

in Stab_τ . There is one LU equivalence class of this type.

- (iia) *The state ρ is LU equivalent to the GHZ state $\tau = |\psi\rangle \langle \psi|$, where $|\psi\rangle = (1/\sqrt{2})(|0 \cdots 0\rangle + |1 \cdots 1\rangle)$ for some $n \geq 3$ and Stab_ρ is isomorphic to $U(1)^{n-1} \rtimes \mathbb{Z}_2$, where $(e^{it_1}, \dots, e^{it_{n-1}}, b)$ in $U(1)^{n-1} \rtimes \mathbb{Z}_2$ corresponds to*

$$\left(\exp(-it_1 Z/2), \dots, \exp(-it_{n-1} Z/2), \exp\left(i \left(\sum_k t_k \right) Z/2 \right) \right) \cdot (X, \dots, X)^b$$

in Stab_τ . There is one LU equivalence class of this type.

- (iib) *The state ρ is LU equivalent to the generalized GHZ state $\tau = |\psi\rangle \langle \psi|$, where $|\psi\rangle = a|0 \cdots 0\rangle + b|1 \cdots 1\rangle$ for some $n \geq 3$ with $|a| \neq |b|$, and Stab_ρ is isomorphic to $U(1)^{n-1}$, where $(e^{it_1}, \dots, e^{it_{n-1}})$ in $U(1)^{n-1}$ corresponds to*

$$\left(\exp(-it_1 Z/2), \dots, \exp(-it_{n-1} Z/2), \exp\left(-i \left(\sum_k t_k \right) Z/2 \right) \right)$$

in Stab_τ . We may take a and b to both be positive and real with $a > b$. The LU equivalence classes of this type are parameterized by the interval $0 < t < 1$ by $a = \cos \frac{\pi}{4}t$, $b = \sin \frac{\pi}{4}t$.

(iii) The state ψ is LU equivalent to the singlet state $\tau = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |01\rangle - |10\rangle$ and Stab_ρ is isomorphic to $PU(2)$, where g in $PU(2)$ corresponds to

$$(g, g)$$

in Stab_τ . There is one LU equivalence class of this type.

(iva) The state ψ is LU equivalent to the Dicke state $\tau = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |D_n^{n/2}\rangle$ for some even $n \geq 4$, and Stab_ρ is isomorphic to $U(1) \rtimes \mathbb{Z}_2$, where (e^{it}, b) in $U(1) \rtimes \mathbb{Z}_2$ corresponds to

$$(\exp(-itZ/2), \dots, \exp(-itZ/2)) \cdot (X, \dots, X)^b$$

in Stab_τ . There is one LU equivalent class of this type.

(ivb) The state ψ is LU equivalent to the Dicke state $\tau = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |D_n^k\rangle$ for some $n \geq 3$ and some k in the range $0 < k < n$ and $k \neq n/2$, and Stab_ρ is isomorphic to $U(1)$, where (e^{it}) in $U(1)$ corresponds to

$$(\exp(-itZ/2), \dots, \exp(-itZ/2))$$

in Stab_τ . There are $\lfloor n/2 \rfloor$ LU equivalence classes of this type, with representatives

$$|D_n^{(1)}\rangle, |D_n^{(2)}\rangle, \dots, |D_n^{(\lfloor n/2 \rfloor - 1)}\rangle.$$

Proof of Theorem 3. We show in [8] that an arbitrary pure symmetric state ρ is LU equivalent to one of the states τ listed in (i)–(ivb). Theorem 1 of that paper identifies 4 families of nonzero stabilizer Lie subalgebras, which exponentiate to stabilizer subgroup elements of the forms given in (i)–(ivb). In each case, it is easy to see that the given correspondences are one-to-one. To establish the claimed isomorphisms, it remains to be shown that the groups

- (i) $U(1)^n$
- (iia) $U(1)^{n-1} \rtimes \mathbb{Z}_2$
- (iib) $U(1)^{n-1}$
- (iii) $PU(2)$
- (iva) $U(1) \rtimes \mathbb{Z}_2$
- (ivb) $U(1)$

given in (i)–(ivb) above map surjectively onto the full stabilizer subgroups of the corresponding states given in (i)–(ivb).

Below we give the proof for (iia) and (iva). The other proofs are both similar and easier. The proofs that the homomorphisms in (iia) and (iva) are onto share the following outline. We consider an arbitrary element $U = (g_1, \dots, g_n)$ in Stab_τ , and we wish to show that U is in the image of the given homomorphism. First, we show that it suffices to show that either all g_k are diagonal, or all

g_k are antidiagonal. Then we consider two cases. The first case is where $g_k \equiv g_\ell$ for all k, ℓ , so that U has the form $U \equiv (g_1, \dots, g_1)$ for some g_1 in $U(2)$. The second case with where there exists a pair of qubits k, ℓ such that $g_k \not\equiv g_\ell$. We show that both cases lead to the conclusion that either all the g_k are diagonal, or all the g_k are antidiagonal. By the earlier reduction, this completes the proof.

Proof of surjectivity in Theorem 3 (iia). Let $\rho = |\psi\rangle\langle\psi|$ be the n -qubit GHZ state, where $|\psi\rangle = |0 \dots 0\rangle + |1 \dots 1\rangle$ for some $n \geq 3$, and let $U = (g_1, \dots, g_n)$ be an element of Stab_ρ . We aim to prove that U can be written in the form

$$\left(\exp(-it_1 Z/2), \dots, \exp(-it_{n-1} Z/2), \exp(i \left(\sum_k t_k \right) Z/2) \right) \cdot (X, \dots, X)^b$$

for some real t_1, \dots, t_{n-1} and some $b = 0, 1$.

We begin with the claim that it suffices to show that either g_k is diagonal for all k , or g_k is antidiagonal for all k . Indeed, if every g_k is diagonal, say $g_k \equiv e^{it_k Z}$, then from

$$U |0 \dots 0\rangle \langle 1 \dots 1| U^\dagger = \exp(2i(\sum t_k)) |0 \dots 0\rangle \langle 1 \dots 1|$$

we conclude that $\sum t_k$ is an integer multiple of π , and so $\sum t_k$ may be taken to be zero (because we are working projectively, we have $e^{i\pi Z} = -\text{Id} \equiv \text{Id}$). Hence U is the image of the element $(e^{-it_1/2}, \dots, e^{-it_{n-1}/2})$ in $U(1)^{n-1}$. If every g_k is antidiagonal, then we can write

$$g_k \equiv \begin{bmatrix} 0 & e^{it_k} \\ e^{-it_k} & 0 \end{bmatrix} = \begin{bmatrix} e^{it_k} & 0 \\ 0 & e^{-it_k} \end{bmatrix} X. \tag{2}$$

Then from

$$U |0 \dots 0\rangle \langle 1 \dots 1| U^\dagger = \exp(-2i \sum t_k) |1 \dots 1\rangle \langle 0 \dots 0|$$

we have $\sum t_k$ is π times and integer, U is projectively equivalent to the image of $(e^{-it_1/2}, \dots, e^{-it_{n-1}/2}, 1)$ in $U(1)^{n-1} \rtimes \mathbb{Z}_2$. This establishes the claim.

Next we show that either all g_k are diagonal, or all g_k are antidiagonal.

Case a. Suppose that $g_k \equiv g_\ell$ for all k, ℓ . Then U has the form $U \equiv (h, \dots, h)$ for some h in $U(2)$. As in the proof of Theorem 2, we can read h , and therefore U , as a rigid motion of the Bloch sphere, and conclude that U takes the Majorana configuration for the GHZ state into itself. Thus U is a symmetry of the regular n -gon in the equatorial plane, and is therefore either a rotation about the Z -axis, or a 180-degree-rotation about the X -axis followed by a rotation about the Z -axis. Thus h is either diagonal or antidiagonal.

Case b. Suppose there exist qubits k, ℓ such that $g_k \not\equiv g_\ell$. As in the proof of Theorem 1, let $V = g_\ell^{(k)} g_k^{(\ell)} \prod_{j \neq k, \ell} g_j^{(j)}$, let $h = g_\ell^\dagger g_k$, so that

$$V^\dagger U = h^{(k)} (h^\dagger)^{(\ell)}$$

is in Stab_ρ . Choose u in $U(2)$ to diagonalize h , and let $\tau = u^{\otimes n} \rho (u^{\otimes n})^\dagger$, so that we have $d^{(k)}(d^\dagger)^{(\ell)}$ in Stab_τ , where $d = e^{itZ} \equiv uhu^\dagger$, for some real t . Continuing to follow the proof of Theorem 1, considering the action of $d^{(k)}(d^\dagger)^{(\ell)}$ on qubits k, ℓ , the presence of a standard nonzero coefficient c_{IJ} in the expansion of τ in the computational basis with $J \neq I$ and $J \neq I^c$ in qubits k, ℓ leads to the contradiction that $g_k \equiv g_\ell$, so we conclude that $\tau = |\psi'\rangle \langle \psi'|$ where $|\psi'\rangle = a|0 \cdots 0\rangle + b|1 \cdots 1\rangle$ is an LU-equivalent GHZ state with $|a| = |b|$. The Majorana configuration for τ is a regular n -gon in the equatorial plane, so we may conclude that u is a rigid motion of the Bloch sphere that must be of the form $e^{i\phi Z}$ or $e^{i\phi Z} X$, so u is diagonal or antidiagonal. From this we have that h is diagonal, so $g_k = g_\ell d_{\ell k}$ for some diagonal matrix $d_{\ell k}$. It follows that U is of the form

$$U \equiv (g_1, g_1 d_{12}, \dots, g_1 d_{1n}) = (g_1, \dots, g_1)(1, \text{Id}, d_{12}, \dots, d_{1n}).$$

Since the action of $(\text{Id}, d_{12}, \dots, d_{1n})$ is a rotation about the Z -axis, and U takes the Majorana configuration of τ to itself, it must be that g_1 is a rigid motion of the Bloch sphere coming from either a diagonal or antidiagonal matrix as in case a, so we conclude that all g_k are diagonal or all g_k are antidiagonal, as desired.

Proof of surjectivity in Theorem 3 (iva). Let ρ be the Dicke state $\rho = |\psi\rangle \langle \psi|$, where $|\psi\rangle = \left| D_n^{(n/2)} \right\rangle$ for some even $n \geq 4$, and let $U = (e^{it}, g_1, \dots, g_n)$ be an element of Stab_ρ . We aim to prove that U can be written in the form

$$(\exp(-itZ/2), \dots, \exp(-itZ/2)) \cdot (X, \dots, X)^b$$

for real t and some $b = 0, 1$.

We begin with the claim that it suffices to show that either g_k is diagonal for all k , or g_k is antidiagonal for all k . Suppose that all g_k are diagonal, say $g_k \equiv e^{it_k Z}$. Choose two qubit labels k, ℓ , choose a weight $n/2$ multiindex $I = i_1 i_2 \dots i_n$ such that $i_k = 0, i_\ell = 1$, and let $J = j_1 j_2 \dots j_n$ denote the multiindex that is formed by complementing the k -th and ℓ -th bits of I . Then from

$$U |I\rangle \langle J| U^\dagger = \exp(2i(t_k - t_\ell)) |I\rangle \langle J|$$

we conclude that $t_k - t_\ell$ is an integer multiple of π . This holds for all k, ℓ , so we have $g_k \equiv g_1$ for all k , so that $U \equiv (g_1, \dots, g_1)$. Thus U is the image of $(e^{-t_1/2}, 0)$ in $U(1) \rtimes \mathbb{Z}_2$. If every g_k is antidiagonal, then again we may write g_k in the form of Eq. (2). Considering the action of U on $|I\rangle \langle J|$ above, the same argument goes through with minor changes, and we have that U is the image of $(e^{-t_1/2}, 1)$ in $U(1) \rtimes \mathbb{Z}_2$. This establishes the claim.

Next we show that either all g_k are diagonal, or all g_k are antidiagonal.

Case a. Suppose that $g_k \equiv g_\ell$ for all k, ℓ . Then U has the form $U = (h, \dots, h)$ for some h in $SU(2)$. We can read h as a rotation of the Bloch sphere that must take the Majorana configuration for $|\psi\rangle$ into itself. Thus h is a rotation about the Z -axis, or h is a 180-degree-rotation about the X -axis followed by a Z -axis rotation. In the first case, h is diagonal. In the second case, h is antidiagonal.

Case b. Suppose there exist qubits k, ℓ such that $g_k \not\equiv g_\ell$. By the same argument as for case b in the previous proof of surjectivity for (iia), we conclude that $|\psi\rangle$ is LU equivalent to a state of the form $a|0\cdots 0\rangle + b|1\cdots 1\rangle$, which is either a product state or a generalized GHZ state. But this violates the known LU classification (Theorem 1 of [8]) for symmetric states. We conclude that case b cannot hold, and this ends the proof. \square

4 Conclusion

We have completely classified LU equivalence classes of LU stabilizer subgroups for pure symmetric states. For infinite stabilizer subgroups, we have given a complete classification of LU equivalence classes of symmetric states. For each finite stabilizer subgroup, there are an infinite number of LU equivalence classes of symmetric states. Each family is characterized by a Majorana configuration, and the LU equivalent states are precisely those whose Majorana configurations are obtained by rotating the Bloch sphere.

In future work we hope to extend these results to mixed symmetric states. We are encouraged by the success of recent work [7] by Bastin et al., in which they extend to mixed symmetric states their own SLOCC classification [6] for pure symmetric states.

References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
2. Aulbach, M., Markham, D., Murao, M.: New J. Phys. **12**, 073025 (2010). ArXiv:1003.5643v2 [quant-ph]
3. Aulbach, M., Markham, D., Murao, M.: Geometric entanglement of symmetric states and the majorana representation. In: van Dam, W., Kendon, V.M., Severini, S. (eds) TQC 2010. LNCS, vol. 6519, pp. 141–158. Springer, Heidelberg (2011). <http://arxiv.org/abs/1010.4777>. ArXiv:1010.4777v1 [quant-ph]
4. Markham, D.J.H.: Phys. Rev. A **83**, 042332 (2011). ArXiv:1001.0343v1 [quant-ph]
5. Toth, G., Wieczorek, W., Gross, D., Krischek, R., Schwemmer, C., Weinfurter, H. (2010). ArXiv:1005.3313v3 [quant-ph]
6. Bastin, T., Krins, S., Mathonet, P., Godefroid, M., Lamata, L., Solano, E.: Phys. Rev. Lett. **103**, 070503 (2009). ArXiv:0902.3230v3 [quant-ph]
7. Bastin, T., Mathonet, P., Solano, E. (2010). ArXiv:1011.1243v1 [quant-ph]
8. Cenci, C.D., Lyons, D.W., Snyder, L.M., Walck, S.N.: Quantum Inf. Comput. **10**, 1029. <http://arxiv.org/abs/1007.3920> (2010). ArXiv:1007.3920v1 [quant-ph]
9. Lyons, D.W., Walck, S.N.: J. Math. Phys. **46**, 102106 (2005). ArXiv:quant-ph/0503052
10. Lyons, D.W., Walck, S.N.: J. Phys. A: Math. Gen. **39**, 2443 (2006). ArXiv:quant-ph/0506241
11. Walck, S.N., Lyons, D.W.: Phys. Rev. A **76**, 022303 (2007). ArXiv:0706.1785 [quant-ph]
12. Lyons, D.W., Walck, S.N., Blanda, S.A.: Phys. Rev. A **77**, 022309 (2008). ArXiv:0709.1105 [quant-ph]

13. Lyons, D.W., Walck, S.N.: Phys. Rev. A **78**, 042314 (2008). [10.1103/PhysRevA.78.042314](https://doi.org/10.1103/PhysRevA.78.042314). <http://arxiv.org/abs/0808.2989>. ArXiv:0808.2989v2 [quant-ph]
14. Mathonet, P., Krins, S., Godefroid, M., Lamata, L., Solano, E., Bastin, T.: Phys. Rev. A **81**, 052315 (2010). ArXiv:0908.0886v2 [quant-ph]

Author Index

- Acín, Antonio 13
Aharon, Nati 1
Alagic, Gorjan 53
Audenaert, Koenraad M.R. 39
Cenci, Curt D. 198
Chailloux, André 1
Datta, Animesh 188
Dhara, Chirag 13
Dupuis, Frédéric 23
Florjanczyk, Jan 23
Grangier, Philippe 143
Hayden, Patrick 23
Ioannou, Lawrence M. 121
Jordan, Stephen P. 53
Kerenidis, Iordanis 1
Leung, Debbie 23
Leverrier, Anthony 143
Lyons, David W. 198
Madhok, Vaibhav 188
Masanes, Lluis 13
Massar, Serge 1
McKague, Matthew 104
Meyer, David A. 153
Mhalla, Mehdi 174
Mosca, Michele 121
Murao, Mio 174
Perdrix, Simon 174
Pironio, Stefano 1, 13
Pommersheim, James 153
Reichardt, Ben W. 73
Silman, Jonathan 1
Someya, Masato 174
Turner, Peter S. 174
Walck, Scott N. 198
Wullschleger, Jürg 164