

Andrew Childs
Michele Mosca (Eds.)

LNCS 5906

Theory of Quantum Computation, Communication, and Cryptography

4th Workshop, TQC 2009
Waterloo, Canada, May 2009
Revised Selected Papers

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, 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, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Andrew Childs Michele Mosca (Eds.)

Theory of Quantum Computation, Communication, and Cryptography

4th Workshop, TQC 2009
Waterloo, Canada, May 11-13, 2009
Revised Selected Papers

Volume Editors

Andrew Childs
Institute for Quantum Computing
and Department of Combinatorics and Optimization
University of Waterloo
Waterloo, ON, N2L 3G1 Canada
E-mail: amchilds@uwaterloo.ca

Michele Mosca
Institute for Quantum Computing
and Department of Combinatorics and Optimization
University of Waterloo
Waterloo, ON, N2L 3G1 Canada
E-mail: mmosca@uwaterloo.ca
and
Perimeter Institute for Theoretical Physics
31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada

Library of Congress Control Number: 2009940405

CR Subject Classification (1998): F, D, C.2, G.1-2, E.3, J.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-642-10697-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-10697-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12810949 06/3180 5 4 3 2 1 0

Preface

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

The fourth iteration of TQC was held during May 11–13, 2009, at the Institute for Quantum Computing at the University of Waterloo in Waterloo, Ontario, Canada. The workshop included invited talks, contributed talks, and a poster session, as well as a rump session consisting of short talks on recent developments. Authors of selected contributed talks were invited to submit a paper to these proceedings.

TQC 2009 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: Roger Colbeck, Markus Grassl, Stefan Hengl, Tohya Hiroshima, Min-Hsiu Hsieh, Akinori Kawachi, Harumichi Nishimura, Rudy Raymond, Douglas Stebila, and Tzu-Chieh Wei.

The logistics of the workshop were expertly managed by the Local Organizing Committee, also listed herein, and we thank them for their efforts to make the workshop a success. We are also thankful for the assistance of Kim Kuntz, Wendy Reibel, Alison Conway and Sharon McCalla, who provided administrative support, and Colin Bell, who helped with computing and audiovisual resources.

We would like to thank the invited speakers, Masato Koashi, John Preskill, Miklos Santha, Graeme Smith, and Stephanie Wehner, for their contributions to the program.

TQC 2009 was made possible by financial support from the Institute for Quantum Computing, the Perimeter Institute for Theoretical Physics, the Fields Institute for Research in Mathematical Sciences, MITACS, and QuantumWorks; 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.

September 2009

Andrew Childs
Michele Mosca

Organization

Program Committee

Panos Aliferis	IBM T.J. Watson Research Center, USA
Dave Bacon	University of Washington, USA
Andrew Childs	IQC, University of Waterloo, Canada (Chair)
Masahito Hayashi	Tohoku University, Japan
Patrick Hayden	McGill University, Canada
Hiroshi Imai	University of Tokyo/ERATO-SORST, Japan
Kazuo Iwama	Kyoto University, Japan
Yasuhito Kawano	NTT, Japan
Norbert Lütkenhaus	IQC, University of Waterloo, Canada
Chiara Macchiavello	INFM, University of Pavia, Italy
Michele Mosca	IQC, University of Waterloo/Perimeter Institute, Canada
Maarten van den Nest	MPQ, Germany
Masanao Ozawa	Nagoya University, Japan
Robert Raussendorf	University of British Columbia, Canada
Ben Reichardt	IQC, University of Waterloo, Canada
Renato Renner	ETH Zurich, Switzerland
Alain Tapp	Université de Montréal, Canada
Barbara Terhal	IBM T.J.Watson Research Center, USA
John Watrous	IQC, University of Waterloo, Canada
Andreas Winter	University of Bristol, UK/CQT, National University of Singapore
Shigeru Yamashita	Nara Institute of Science and Technology, Japan

Organizing Committee

Anne Broadbent	IQC, University of Waterloo, Canada
Sarah Croke	Perimeter Institute, Canada
Dmitri Maslov	IQC, University of Waterloo, Canada
Michele Mosca	IQC, University of Waterloo/Perimeter Institute, Canada (Chair)
Simone Severini	IQC, University of Waterloo, Canada
Tzu-Chieh Wei	IQC, University of Waterloo, Canada

Table of Contents

Solutions to the Hidden Subgroup Problem on Some Metacyclic Groups	1
<i>Demerson N. Gonçalves, Renato Portugal, and Carlos M.M. Cosme</i>	
Quantum Online Memory Checking	10
<i>Wim van Dam and Qingqing Yuan</i>	
On the Structure of Protocols for Magic State Distillation	20
<i>Earl T. Campbell and Dan E. Browne</i>	
Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function	33
<i>Takeshi Koshihara and Takanori Odaira</i>	
On the Security and Degradability of Gaussian Channels	47
<i>Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd</i>	
Universal Quantum Computation with a Non-Abelian Topological Memory	56
<i>James R. Wootton, Ville Lahtinen, and Jiannis K. Pachos</i>	
Conditions for the Approximate Correction of Algebras	66
<i>Cédric Bény</i>	
Optimal State Merging without Decoupling	76
<i>Jean-Christian Boileau and Joseph M. Renes</i>	
Optimal Trading of Classical Communication, Quantum Communication, and Entanglement	85
<i>Min-Hsiu Hsieh and Mark M. Wilde</i>	
On the Power of the PPT Constraint in the Symmetric Extensions Test for Separability	94
<i>Miguel Navascués, Masaki Owari, and Martin B. Plenio</i>	
Author Index	107

Solutions to the Hidden Subgroup Problem on Some Metacyclic Groups

D.N. Gonçalves¹, R. Portugal¹, and C.M.M. Cosme²

¹ National Laboratory for Scientific Computation, Petrópolis, RJ, 25651-070, Brazil

² Universidade Federal dos Vales do Jequitinhonha e Mucuri, Department of Mathematics, Teófilo Otoni, MG, 39801-000, Brazil

Abstract. We describe a new polynomial-time quantum algorithm that solves the hidden subgroup problem (HSP) for a special class of metacyclic groups, namely $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, with $q \mid (p-1)$ and $p/q = \text{poly}(\log p)$, where p, q are any odd prime numbers and s is any positive integer. This solution generalizes previous algorithms presented in the literature. In a more general setting, without imposing a relation between p and q , we obtain a quantum algorithm with time and query complexity $2^{O(\sqrt{\log p})}$. In any case, those results improve the classical algorithm, which needs $\Omega(\sqrt{p})$ queries.

1 Introduction

The Hidden Subgroup Problem (HSP) consists in finding a subgroup H in a finite group G hidden by a function which is constant on each coset of H and distinct in different cosets. To be efficient, an algorithm for the HSP has to be polylogarithmic in the order of G . It is well known that if the group G is abelian then the HSP on G can be efficiently solved by a quantum algorithm [1,2], while no general solution is known for the case of nonabelian groups [2]. Two important groups are the *symmetric* and the *dihedral* groups, because efficient algorithms for them imply an efficient solution to the graph isomorphism problem [3], and to a certain lattice-related problem whose hardness is assumed in cryptography [4].

One of the methods used to develop new quantum algorithms for the HSP on a nonabelian group G requires both the use of the abelian Fourier transform and the characterization all the subgroups of G . That method was employed by several authors. Inui and Le Gall [5] have presented an efficient quantum algorithm for the HSP on the group $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$, where p is an odd prime and r is any positive integer. Bacon *et al.* [6] have simplified the hidden subgroup problem over semidirect product groups $\mathbb{Z}_N \rtimes \mathbb{Z}_q$, where N is any positive integer, q is a prime number and $\frac{N}{q} = \text{poly}(\log N)$ by reducing the problem to that of finding the trivial hidden subgroup or a hidden cyclic subgroup of order q . That result has generalized Ettinger and Høyer's paper [7], which reduced the dihedral HSP to the problem of finding a trivial hidden subgroup or a subgroup of order 2.

In this paper, we present an efficient quantum algorithm for solving the HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, where p, q are any odd prime numbers and s is any

positive integer, by fixing an particular homomorphism with $p/q = \text{poly}(\log p)$. This generalizes a result of Ref. [8] for p -hedral groups, which requires $s = 1$. In some aspects, it also generalizes the algorithm presented in Ref. [6], which also requires $s = 1$.

In a more general setting, without imposing a relation between p and q , we present a subexponential-time quantum algorithm for the HSP on $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ by using both the classification of its subgroups and by reducing the problem to that of finding some cyclic subgroups. Our approach employs the ideas behind Kuperberg's sieve for the HSP over dihedral groups [12] and the Ettinger-Høyer's reduction criterion [7]. Our algorithm is subexponential in contrast with the best classical algorithm, that requires $\Omega(\sqrt{p})$ queries.

The paper is organized as follows. In Sec. 2, we define the semidirect product of cyclic groups $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ and characterize the subgroups. In Sec. 3, we show how the HSP on $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ can be reduced to that of finding cyclic subgroups with prime power order. Then, in Sec. 3.1 we present a subexponential-time quantum algorithm for the HSP over $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, for a general homomorphism. In Sec. 3.2 we improve our results and provide a polynomial-time quantum algorithm for a particular class of the semidirect product of cyclic groups $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. Finally, in Sec. 4 we draw our conclusions.

2 The Structure of $\mathbb{Z}_p \rtimes_{\phi} \mathbb{Z}_{q^s}$

The group $\mathbb{Z}_p \rtimes_{\phi} \mathbb{Z}_{q^s}$ is the set $\{(a, b), a \in \mathbb{Z}_p, b \in \mathbb{Z}_{q^s}\}$ with the group operation $(a_1, b_1)(a_2, b_2) = (a_1 + \phi(b_1)(a_2), b_1 + b_2)$, where ϕ is any homomorphism from $\mathbb{Z}_{q^s}$ into $\text{Aut}(\mathbb{Z}_p)$, which is the group of automorphisms of $\mathbb{Z}_p$. The group $\mathbb{Z}_p \rtimes_{\phi} \mathbb{Z}_{q^s}$ is generated by $x = (1, 0)$ and $y = (0, 1)$. Since $\text{Aut}(\mathbb{Z}_p)$ is isomorphic with $\mathbb{Z}_p^*$, the homomorphism ϕ is completely determined by $\alpha = \phi(1)(1) \in \mathbb{Z}_p^*$. The notation (a, b) is equivalent to $x^a y^b$ and the commutation relation is given by $y^b x^a = x^{a\alpha^b} y^b$.

Notice that if an element $\alpha \in \mathbb{Z}_p^*$ defines a semidirect product $\mathbb{Z}_p \rtimes_{\alpha} \mathbb{Z}_{q^s}$ then $\text{ord}(\alpha) = q^t$ for some $t = 0, \dots, s$. The case $t = 0$ reduces to the abelian group $\mathbb{Z}_p \times \mathbb{Z}_{q^s}$. The HSP can be solved efficiently in this case.

Notice that the group $\mathbb{Z}_p^*$ is a cyclic group and let u be an arbitrary generator. We can write $\alpha = u^k$ for some $1 \leq k < p - 1$, and then $\alpha^{q^t} = u^{kq^t} \equiv 1 \pmod{p}$. It follows that $p - 1 \mid kq^t$. Since p and q are prime numbers, we must impose that $q^t \mid p - 1$. Then

$$k = \frac{l(p-1)}{q^t}.$$

For each $0 \leq t \leq s$ and $l \in \mathbb{Z}_{q^t}^*$, the number

$$\alpha := u^{\frac{l(p-1)}{q^t}} \quad (1)$$

defines a semidirect product of cyclic groups, which will be denoted by $G_{t,l} = \mathbb{Z}_p \rtimes_{\alpha} \mathbb{Z}_{q^s}$.

We can eliminate the parameter l because $G_{t,l}$ is isomorphic with $G_{t,1}$ for all values of l . In fact, by defining the application $\Phi_{t,l} : G_{t,1} \rightarrow G_{t,l}$ such that $\Phi_{t,l}(x^a y^b) = x^a y^{l^{-1}b}$, one easily sees that the groups $G_{t,l}$ and $G_{t,1}$ are isomorphic. From now on, let us consider the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ with the homomorphism α given by Eq. (1) with $l = 1$.

By using the relation $y^b x^a = x^{a\alpha^b} y^b$, it can be easily checked that

$$(x^a y^b)^k = \begin{cases} x^{\frac{a(\alpha^{bk}-1)}{\alpha^b-1}} y^{bk} & \text{if } q^t \nmid b, \\ x^{ak} y^{bk} & \text{otherwise} \end{cases} \quad (2)$$

where $q^t = \text{ord}(\alpha)$.

Now we are able to describe the subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$.

Theorem 1. *The subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ are*

Class 1. $\langle x^a y^{q^j} \rangle$ for all $a \in \mathbb{Z}_p$, $0 \leq j < t$;

Class 2. $\langle x^{p^i} y^{q^j} \rangle$ with $0 \leq i \leq 1$ and $t \leq j \leq s$;

Class 3. $\langle x^{p^i}, y^{q^j} \rangle$ with $0 \leq i \leq 1$ and $0 \leq j < t$.

Proof. See Appendix. ■

3 Quantum Algorithms for the HSP over $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$

In this section, we present two quantum algorithms that solves the HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, where p, q are any odd prime numbers and s is any positive integer. In Sec. 3.1, we describe a subexponential-time quantum algorithm for $1 \leq t \leq s$. In Sec. 3.2, we describe a polynomial-time quantum algorithm for $t = 1$.

Let f be the oracle function that hides the subgroup H in $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. It follows from Theorem 1 that there are three possibilities for H : 1) It belongs to Class 1 and we have to find parameters a and j . 2) It belongs to Class 2 and we have to find parameters i and j . 3) It belongs to Class 3 and we have to find parameters i and j . The parameter a is the most difficult one. We describe the algorithm that determines a in the next section.

The outline of the main algorithm is as follows. Let $H_x = H \cap \langle x \rangle$ and $H_y = H \cap \langle y \rangle$. Let function f_x be defined by $f_x(a) = f(a, 0)$, which hides H_x in $\mathbb{Z}_p$. Let function f_y be defined by $f_y(b) = f(0, b)$, which hides H_y in $\mathbb{Z}_{q^s}$. The solution of the abelian HSP on $\mathbb{Z}_p$ and $\mathbb{Z}_{q^s}$ with oracles f_x and f_y respectively determine generators for H_x and H_y . These groups are $H_x = \langle x^{p^i} \rangle$ and $H_y = \langle y^{q^j} \rangle$, for some $0 \leq i \leq 1$ and $0 \leq j \leq s$. From now on the values of i and j are known by us. If $j \geq t$ we learn that $H = \langle x^{p^i} y^{q^j} \rangle$, otherwise, we run the algorithm described in Sec. 3.1 (Sec. 3.2 for $t = 1$). If the number a that the algorithm outputs satisfies $f(x^a y^{q^j}) = f(e)$ then we learn that $H = \langle x^a y^{q^j} \rangle$. If the algorithm of

Sec. 3.1 (Sec. 3.2 for $t = 1$) returns a value a such that $f(x^a y^{q^j}) \neq f(e)$, we learn that $H = \langle x^{p^i}, y^{q^j} \rangle$.

Let us close this section by discussing the complexity of the *classical* algorithm. It follows from Theorem 1 that $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ has $\Omega(p)$ subgroups. Hence, the HSP on that group cannot be solved efficiently in a classical computer by an exhaustive search. Other methods such as the ones presented in Refs. [9,10] for groups with commutator subgroups of polynomial size and for nilpotent groups of constant nilpotency class cannot be applied here. In order to solve the problem classically one needs to find two different inputs g_1 and g_2 for which $f(g_1) = f(g_2)$, that is, find a collision. For each $0 \leq j \leq s$, we have the promise that the function f is q^{s-j} -to-one. One needs to guess $\Theta(\sqrt{pq^j})$ different inputs before being likely to find a pair on which f takes the same output [11]. Therefore the lower bound for the classical algorithm is $\Omega(\sqrt{p})$.

3.1 The Sieve Algorithm

Given a function f that hides the subgroup $H = \langle x^a y^{q^j} \rangle$ in $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, our goal is to find a . We show how one can determine a in subexponential time with high probability. The key points are described the Algorithm 1.

Algorithm 1.

Input: Integers p, q, s, j and a function $f : \mathbb{Z}_p \rtimes \mathbb{Z}_{q^s} \rightarrow X$, where X is some finite set.

Output: A one-qubit state.

1. Prepare the state

$$\frac{1}{\sqrt{2p}} \sum_{m=0}^{p-1} \sum_{n=0}^1 |m\rangle |n\rangle \left| f(x^m y^{nq^j}) \right\rangle.$$

2. Measure the third register.
3. Apply the Fourier transform F_p to the first register

$$F_p |j\rangle = \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \omega_p^{jk} |k\rangle, \text{ where } \omega_p = e^{\frac{2\pi i}{p}}.$$

4. Measure the first register.
-

The output of Algorithm 1 (up to a global phase) is the state

$$|\psi_k^{a,p}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \omega_p^{ak} |1\rangle \right), \quad (3)$$

for some $0 \leq k < p$ randomly distributed.

Notice that, when the state $|\psi_k^{a,p}\rangle$ is obtained, we learn the values of p and k , but we have no information about the parameter a , which determines the hidden

subgroup $\langle x^a y^{q^j} \rangle$. For $0 \leq \gamma \leq \lceil \log p \rceil$, define the function $f^{(\gamma)} : \mathbb{Z}_p \rtimes \mathbb{Z}_{q^s} \rightarrow X$ as

$$f^{(\gamma)}(x^a y^b) = f(x^{2^{-\gamma}a} y^b). \quad (4)$$

Observe that $f^{(\gamma)}$ hides the subgroup

$$H_\gamma = \left\{ x^{a2^\gamma S(k)} y^{kq^j} : k = 0, \dots, q^{s-j} - 1 \right\}. \quad (5)$$

where

$$S(k) = \frac{\alpha^{kq^j} - 1}{\alpha^{q^j} - 1}. \quad (6)$$

Then, for each $0 \leq \gamma \leq \lceil \log p \rceil$ we use the function $f^{(\gamma)}$ as input for the Algorithm 1. This time the output of the Algorithm 1 is a state of the form $|\psi_k^{2^\gamma a, p}\rangle$, where k is uniformly distributed over $\mathbb{Z}_p$. Our goal is to obtain the state $|\psi_1^{2^\gamma a, p}\rangle$. By applying the Fourier transform on the set

$$\left\{ |\psi_1^{2^\gamma a, p}\rangle, \gamma = 0, \dots, \lceil \log p \rceil \right\}, \quad (7)$$

one gets the value of a with high probability. However, the probability of obtain the state $|\psi_1^{2^\gamma a, p}\rangle$ from the Algorithm 1 is $1/p$, which is exponentially small. Thus, we will show how to obtain the state $|\psi_1^{2^\gamma a, p}\rangle$ in subexponential time by using a quantum computer.

First, for two samples $|\psi_{k_1}^{2^\gamma a, p}\rangle$ and $|\psi_{k_2}^{2^\gamma a, p}\rangle$ from the Algorithm 1, we apply the CNOT operator in the tensor product $|\psi_{k_1}^{2^\gamma a, p}\rangle \otimes |\psi_{k_2}^{2^\gamma a, p}\rangle$ using the first qubit as the control qubit. The result is the following state

$$\frac{1}{2} (|00\rangle + \omega_p^{k_2 2^\gamma a} |01\rangle + \omega_p^{k_1 2^\gamma a} |11\rangle + \omega_p^{(k_1+k_2) 2^\gamma a} |10\rangle). \quad (8)$$

Now, measuring the second qubit in the computational basis, up to a global phase, we obtain the state $|\psi_{k_1-k_2}^{2^\gamma a, p}\rangle$ with probability $1/2$. We call this procedures combine-and-measure.

We call Algorithm 1 $2^{O(\sqrt{\log p})}$ times taking function $f^{(\gamma)}$ as input, each time producing a one-qubit quantum state $|\psi_k^{2^\gamma a, p}\rangle$. Let us call L_0 the set formed by those states. The sieve algorithm finds the pairs $|\psi_{k_1}^{2^\gamma a, p}\rangle$ and $|\psi_{k_2}^{2^\gamma a, p}\rangle$ in the set L_0 , such that the first $m = \lceil \sqrt{\log p - 1} \rceil$ bits of k_1 and k_2 are identical. Then, for each pair, we apply the combine-and-measure procedure described in the previous paragraph to produce, with probability $1/2$, the state $|\psi_{k_1-k_2}^{2^\gamma a, p}\rangle$. Denote the set of all these states by L_1 . The set L_1 consists of states of the form $|\psi_k^{2^\gamma a, p}\rangle$ such that the m most significant bits of k are all zeros. By repeating this procedure m times, we obtain with high probability, a set L_m that has at

least one state of the form $|\psi_1^{2^\gamma a, p}\rangle$. The complexity analysis of the algorithm is the same to the one presented in [12] and we will not discuss it here. Thus, we have the

Theorem 2. *The HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, where p, q are odd prime numbers and s is any positive integer has an algorithm with time and query complexity $2^{O(\sqrt{\log p})}$.*

3.2 The Case $H = \langle x^a y \rangle$

In this section, we present an efficient quantum algorithm that solves the HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, when $q \mid p-1$ and $p/q = \text{poly}(\log p)$. This class of group is obtained by choosing $t = 1$ in Eq. (1).

According to Sec. 3, the HSP on $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ can be reduced to the problem of finding a hidden cyclic subgroup of prime power order, such as, $H = \langle x^a y \rangle$. Thus, given a function f that hides the subgroup $H = \langle x^a y \rangle$ in $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, the following procedure efficiently determines the value of a , with high probability, when $q \mid p-1$ and $p/q = \text{poly}(\log p)$. Notice that the order of H is q^s .

First, let us prepare the quantum computer in the initial state

$$|\Psi_1\rangle = \frac{1}{\sqrt{qp}} \sum_{m=0}^{p-1} \sum_{n=0}^{q-1} |m\rangle |n\rangle |f(x^m y^n)\rangle. \quad (9)$$

The arithmetical operations in the first(second) ket are performed modulo $p(q^s)$. Now we measure the third register in the computational basis. The left cosets of H are of the form

$$x^{m_0} H = \{(m_0 + aS(n), n), n = 0, \dots, q^s - 1\}, \quad (10)$$

where $m_0 \in \mathbb{Z}_p$ and

$$S(n) = \frac{\alpha^n - 1}{\alpha - 1} \mod p. \quad (11)$$

Then, the result of the measurement is

$$|\Psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} |m_0 + aS(n)\rangle |n\rangle, \quad (12)$$

for some $0 \leq m_0 < p$ randomly distributed. We have discarded the third register since it will be irrelevant from now on. Now, we apply the Fourier transform operator $F_p \otimes I$ on the state $|\Psi_2\rangle$. The result is

$$|\Psi_3\rangle = \frac{1}{\sqrt{qp}} \sum_{k=0}^{p-1} \sum_{n=0}^{q-1} \omega_p^{k(m_0 + aS(n))} |k\rangle |n\rangle, \quad (13)$$

where ω_p is the primitive p -root of the unity. The next step is to measure the first register in the computational basis. We assume that the result is some $k_0 \in \mathbb{Z}_p^*$.

Then, we have the state

$$|\Psi_4\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{k_0(m_0+aS(n))} |k_0\rangle |n\rangle. \quad (14)$$

The probability to obtain the state $|\Psi_4\rangle$ is $1 - \frac{1}{p}$.

Now, let us consider the operator

$$U |m\rangle |n\rangle = |mS(n)\rangle \left| n - S^{-1} \left(\frac{mS(n)}{k_0} \right) \right\rangle.$$

To show that U is unitary, one has to use the fact that $S(n)$ is injective when $0 \leq n < q$. $S^{-1}(n)$ can be calculated efficiently by employing Shor's discrete logarithm algorithm. Integer powers of α can be calculated efficiently by the repeated squaring method.

The next step is to apply the unitary operator U on $|\Psi_4\rangle$, which yields

$$|\Psi_5\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{k_0(m_0+aS(n))} |k_0S(n)\rangle |0\rangle. \quad (15)$$

To obtain the parameter a from the state $|\Psi_5\rangle$ we use the following argument [6]. The state

$$|\tilde{a}\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \omega_p^{ja} |j\rangle \quad (16)$$

has a high overlap with $|\Psi_5\rangle$ (disregarding the ket $|0\rangle$ of $|\Psi_5\rangle$). In fact, the fidelity between the state $|\tilde{a}\rangle$ and the state $|\Psi_5\rangle$ is $\sqrt{\frac{q}{p}}$. We apply the inverse Fourier transform $F_p^\dagger$ on the state $|\Psi_5\rangle$ and perform a measurement in the computational basis to obtain the value of a with probability q/p . The total success probability of obtain a is $(1 - \frac{1}{p})\frac{q}{p}$.

We run the above procedure l times, where $l = \frac{p}{2(p-1)}\frac{p}{q} = O(\text{poly}(\log p))$ to get the value of a with probability $1/2$.

Theorem 3. *There is a quantum algorithm solving, in polynomial time, the HSP over the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, with $q \mid (p-1)$ and $p/q = \text{poly}(\log p)$, where p, q are odd prime numbers and s is any positive integer.*

4 Conclusion

We have presented quantum algorithms for the HSP on the group $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, where p, q are any odd prime numbers and s is any positive integer. By using the classification of subgroups of $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$, we have simplified the HSP to that of finding cyclic subgroups with prime power order. The first one is a subexponential-time quantum algorithm with complexity $2^{O(\sqrt{\log p})}$. This algorithm works for any homomorphism which defines the semidirect product. The second one is a

polynomial-time quantum algorithm for a special class of metacyclic groups with $q \mid (p-1)$ and $p/q = \text{poly}(\log p)$. Both algorithms are probabilistic with a success probability greater than $1/2$.

The results of this work generalize the results obtained in Ref. [6] and Ref. [8]. The latter authors use the non-abelian Fourier transform to solve the HSP in $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ ($s = 1$). It is interesting to analyze the possibility of obtaining equivalent results for $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$ using the non-abelian Fourier transform.

Acknowledgments

We would like to thank G. Leal and F.L. Marquezino for useful discussions. We acknowledge support from CAPES.

References

1. Kitaev, A.Y.: Quantum measurements and the abelian stabilizer problem. ArXiv preprint quant-ph/9511026 (1995)
2. Lomont, C.: Hidden Subgroup Problem - Review and Open Problems. ArXiv preprint quant-ph/0411037 (2004)
3. Hallgren, S., Moore, C., Rötteler, M., Russell, A., Sen, P.: Limitations of quantum coset states for graph isomorphism. In: Proceedings 38th ACM Symposium on Theory of Computing (STOC 2006), pp. 604–617 (2006)
4. Regev, O.: Quantum Computation and Lattice Problems. SIAM J. Comp. 33(3), 738–760 (2004)
5. Inui, Y., Le Gall, F.: Efficient Quantum Algorithms For The Hidden Subgroup Problem Over Semi-Direct Product Groups. Quantum Information & Computation 7(5), 559–570 (2007)
6. Bacon, D., Childs, A.M., van Dam, W.: From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups. In: Proc. of 46th Ann. IEEE Symp. on Foundations of Computer Science - FOCS 2005, pp. 469–478 (2005)
7. Ettinger, M., Høyer, P.: On Quantum Algorithms for Noncommutative Hidden Subgroups. Adv. Appl. Math. 25(3), 239–251 (2000)
8. Moore, C., Rockmore, D., Russell, A., Schulman, L.J.: The power of basis selection in fourier sampling: hidden subgroup problems in affine groups. In: SODA 2004: Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, pp. 1113–1122 (2004)
9. Ivanyos, G., Magniez, F., Santha, M.: Efficient Quantum Algorithms for some Instances of the Non-Abelian Hidden Subgroup Problem. International Journal of Foundations of Computer Science 14(5), 723–740 (2003)
10. Ivanyos, G., Sanselme, L., Santha, M.: An Efficient Quantum Algorithm for the Hidden Subgroup Problem in Nil-2 Groups. In: Lader, E.S., Bornstein, C., Nogueira, L.T., Faria, L. (eds.) LATIN 2008. LNCS, vol. 4957, pp. 759–771. Springer, Heidelberg (2008)
11. Kutin, S.: Quantum Lower Bound for the Collision Problem with Small Range. Theory of Computing 1(1), 29–36 (2005)
12. Kuperberg, G.: A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. SIAM J. Comput. 35(1), 170–188 (2005)

Appendix

In this appendix, we prove Theorem 1.

Proof. Let H be a subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_{q^s}$. If H is cyclic then it follows from Eq. (2) that either H belongs to Class 1 or to Class 2. Now suppose that the subgroup H is given by a set of n generators where n is any positive integer, i.e. $H = \langle x^{a_1}y^{b_1}, \dots, x^{a_n}y^{b_n} \rangle$. If $q^t \mid b_1, \dots, q^t \mid b_n$, define $q^{\lambda_i} = \gcd(b_i, q^s)$. Thus, we can write $H = \langle x^{a_1}y^{v_1q^{\lambda_1}}, \dots, x^{a_n}y^{v_nq^{\lambda_n}} \rangle$ where $v_k \in \mathbb{Z}_{q^s}^* \cup \{0\}$ for all $k = 1, \dots, n$. Consider $\lambda = \min \{\lambda_1, \dots, \lambda_n\}$. If $a_i = 0$ for all $i = 1, \dots, n$ then $H = \langle y^{q^\lambda} \rangle$ and we learn that H is in the Class 2. On the other hand, if there exists at least one index i such that $a_i \neq 0$ then, it is straightforward to show that $H = \langle xy^{q^\lambda} \rangle$ and therefore H belongs to Class 2.

Now, let us deal with the case $q^t \nmid b_1, \dots, q^t \nmid b_n$. Define $q^{j_1} = \gcd(b_1, q^s)$, $\dots$, $q^{j_n} = \gcd(b_n, q^s)$ and $j = \min \{j_1, \dots, j_n\}$, where $0 \leq j < t$. Suppose that there are generators $x^{a_i}y^{b_i}$ and $x^{a_j}y^{b_j}$ in H that do not commute. In this case, it is not difficult to see that $H = \langle x, y^{q^j} \rangle$, which implies that H belongs to Class 3. Now, suppose that all the generators of the subgroup H commute. Let $b_j = \min \{b_1, \dots, b_n\}$, then we can write $b_k = b_j + v_k$, $v_k \in \mathbb{Z}_{q^s}$ for all $k = 1, \dots, n$. Thus, the subgroup H can be written in the form

$$H = \langle x^{a_1}y^{b_j+v_1}, \dots, x^{a_j}y^{b_j}, \dots, x^{a_n}y^{b_j+v_n} \rangle. \quad (17)$$

Using the identity

$$x^{a_j+a_k} \alpha^{b_j-a_j} \alpha^{b_j+v_k} y^{b_j+v_k} = x^{a_k} y^{b_j+v_k}$$

for all $k = 1, \dots, n$, one can check that $H = \langle x^{a_i}y^{b_j} \rangle = \langle x^{a_i}y^{q^j} \rangle$, for some $a_i \in \mathbb{Z}_p$ and $0 \leq j < t$. Hence, H belongs to Class 1.

Finally, let $H = \langle x^{a_1}y^{b_1}, \dots, x^{a_n}y^{b_n} \rangle$ for some $n \in \mathbb{N}$ such that there exists indices $1 \leq j_1 < j_2 < \dots < j_k \leq n$ such that $q^t \nmid b_{j_1}, \dots, q^t \nmid b_{j_k}$. For simplicity, let us suppose that $j_1 = 1, \dots, j_k = k$. Thus, we can write the subgroup H in the following form

$$H = \langle x^{a_1}y^{b_1}, \dots, x^{a_k}y^{b_k}, x^{p^\kappa}y^{q^\gamma} \rangle, \quad (18)$$

for some $0 \leq \kappa \leq 1$ and $t \leq \gamma < t$. As we have discussed in the second paragraph, the subgroup $\langle x^{a_1}y^{b_1}, \dots, x^{a_k}y^{b_k} \rangle$ can be written either as $\langle x^{p^i}, y^{q^j} \rangle$, for some $0 \leq i \leq 1$ and $0 \leq j < t$ or in the form $\langle x^a y^{q^j} \rangle$, for some $a \in \mathbb{Z}_p$ and $0 \leq j < t$. Thus, we can write $H = \langle x^{p^i}, y^{q^j}, x^{p^\kappa}y^{q^\gamma} \rangle = \langle x^{p^m}, y^{q^j} \rangle$, where $m = \min \{i, \kappa\}$, or $H = \langle x^a y^{q^j}, x^{p^\kappa}y^{q^\gamma} \rangle$. In the latter case, it is not hard to check that $H = \langle x, y^{q^j} \rangle$ if $\kappa = 0$ or $H = \langle x^a y^{q^j} \rangle$ if $\kappa = 1$. ■

Quantum Online Memory Checking

Wim van Dam^{1,2} and Qingqing Yuan^{1,3}

¹ Department of Computer Science, University of California, Santa Barbara

² Department of Physics, University of California, Santa Barbara

³ Microsoft Corporation, Redmond, WA

Abstract. The problem of memory checking considers storing files on an unreliable public server whose memory can be modified by a malicious party. The main task is to design an online memory checker with the capability to verify that the information on the server has not been corrupted. To store n bits of public information, the memory checker has s private reliable bits for verification purpose; while to retrieve each bit of public information the checker communicates t bits with the public memory. Earlier work showed that, for classical memory checkers, the lower bound $s \times t \in \Omega(n)$ holds. In this article we study *quantum* memory checkers that have s private qubits and that are allowed to quantum query the public memory using t qubits. We prove an exponential improvement over the classical setting by showing the existence of a quantum checker that, using quantum fingerprints, requires only $s \in O(\log n)$ qubits of local memory and $t \in O(\text{polylog } n)$ qubits of communication with the public memory.

1 Introduction

The problem of memory checking was first introduced by Blum et al. [2] as an extension of program checking. In this problem, a memory checker receives a sequence of “store” and “retrieve” operations from a user, and the checker has to relay these commands to an unreliable server. By making additional requests to the unreliable memory and using a small private and reliable memory for storing additional information, the checker is required to give correct answers (with high probability) to the user’s retrieve operations that are in accordance the previous store instructions, or report error when the information has been corrupted. Blum et al. [2] made a distinction between “online” and “offline” memory checkers: an *online memory checker* must detect the error immediately after receiving an errant response from the memory, while an *offline checker* is allowed to output whether they are all handled correctly until the end of the operation sequence.

There are two main complexity measures regarding memory checkers: the *space complexity*, which is the size of its private reliable memory, and the *query complexity*, which is the size of the messages between the memory checker and the public memory per user request. The goal is to have a reliable checker with low space complexity and low query complexity against any (probabilistic, polynomial time) adversary corrupting the public memory.

With s be the space complexity and t the query complexity of an online memory checker, both Blum et al. [2] and Naor and Rothblum [6] proved that for classical online memory checking one has the lower bound $s \times t \in \Omega(n)$.

Our Result. We looked at the efficiency of online memory checkers that are allowed to operate in a quantum mechanical way. After defining the proper model, we present an online memory checker using quantum fingerprints that requires only $s \in O(\log n)$ bits of private memory and $t \in O(\text{polylog } n)$ queries to the public memory. We also prove its correctness and security. Specifically we show that for an error rate $\epsilon > 0$ it is sufficient for the memory checker to privately keep $O(\log(1/\epsilon))$ copies of the quantum fingerprints of the public memory (each requiring $O(\log n)$ qubits). The parameters of the specific error correcting code that we use for the quantum fingerprints introduces a constant multiplicative term in this quantity $O(\log(1/\epsilon))$.

2 Preliminaries

In this section, we present the model of memory checker in the quantum settings. We also briefly review some of the techniques used in our quantum algorithms for online memory checking.

2.1 Memory Checker

We first introduce the classical definition of memory checker, and then extend it to quantum settings.

Definition 1. Classical Memory Checkers (see [2,6]). A memory checker is a probabilistic Turing machine $\mathcal{C}$ with five tapes: a read-only input tape for $\mathcal{C}$ to read the requests from user $\mathcal{U}$, a write-only output tape for $\mathcal{C}$ to write its response to the user's requests or that the memory $\mathcal{M}$ is “buggy”, a write-only tape for $\mathcal{C}$ to write requests to $\mathcal{M}$, a read-only tape for $\mathcal{C}$ reading response from $\mathcal{M}$, and a read-write work tape as a secret, reliable memory.

Quantum Memory checker: In our quantum mechanical extension of this definition, the input and output tape between $\mathcal{C}$ and $\mathcal{U}$ both remain classical, as well as the memory $\mathcal{M}$. The checker $\mathcal{C}$, however, is now allowed to make quantum queries to the memory $\mathcal{M}$ and the secret work-tape of $\mathcal{C}$ and the two read and write-only tapes between $\mathcal{C}$ and $\mathcal{M}$ now support quantum bits. This model is illustrated in Fig. 1.

The user $\mathcal{U}$ presents the “store” and “retrieve” requests to $\mathcal{C}$ and after each “retrieve” request, $\mathcal{C}$ must write an answer to the output tape or output that $\mathcal{M}$ is “buggy” if the public memory $\mathcal{M}$ has been corrupted. We say a memory *acts correctly* if the returns of a “retrieve” operation are consistent with the contents written by the previous adjacent “store” operation. For any operation sequence of polynomial length in the total size n of the data stored by $\mathcal{U}$ on $\mathcal{M}$ and error rate $0 < \epsilon < \frac{1}{2}$, it is required that:

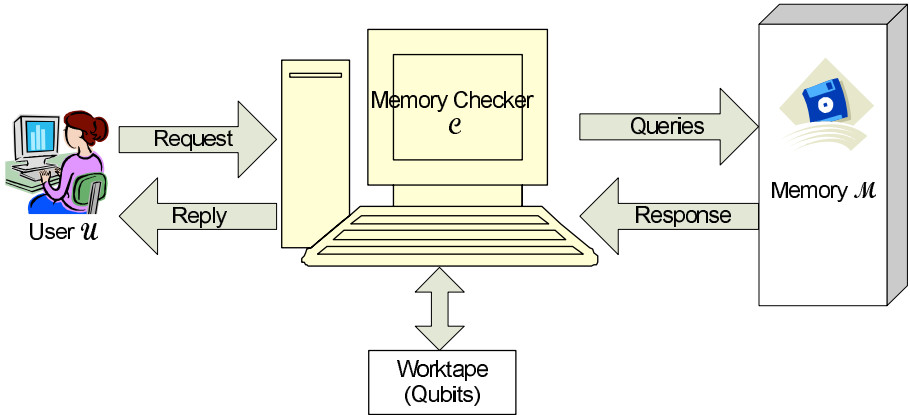


Fig. 1. A quantum mechanical memory checker: The user presents classical “store” or “retrieve” request to the checker, which, with high probability, returns the correct answer or reports “buggy” when the memory has been corrupted. The checker can make quantum queries to the memory, such that it acquires a superposition of values. In addition, the checker is also allowed to have a private, secure work tape that consists of qubits and that is much smaller than the public memory.

- If $\mathcal{M}$ ’s output to the “retrieve” operation is correct, $\mathcal{C}$ also answers $\mathcal{U}$ ’s request with correctness probability at least $1 - \epsilon$.
- If $\mathcal{M}$ ’s output is incorrect for some operation, $\mathcal{C}$ outputs “buggy” with probability at least $1 - \epsilon$.

There are two important measures of the complexity of a memory checker: the size s of its secret memory (the *space complexity*) and the number t of bits exchanged between $\mathcal{C}$ and $\mathcal{M}$ per request from the user (the *query complexity*). We follow the convention that we only consider the *query complexity* for *retrieve requests* such that the query complexity for *store requests* may be unbounded. Obviously, if the secret memory is sufficiently large, the solution to this problem is trivial as $\mathcal{C}$ can simply store the n bits on its work-tape. More interesting is the case where the space complexity t is sublinear (typically logarithmic) in n .

As noted in [2] and [6], memory checkers can be categorized into “online” and “offline” versions. In the offline model, the checker $\mathcal{C}$ is allowed to output “buggy” at any point before the last “retrieve” request in the sequence if $\mathcal{M}$ ’s answers to some request is incorrect. The online model is more restricted as $\mathcal{C}$ is required to detect the error immediately once $\mathcal{M}$ gives an incorrect answer to the request.

In this paper, we focus on online memory checkers. As noted in the Introduction, it is known that for classical online memory checkers, we have the lower bound $s \times t \in \Omega(n)$ [6]. Below it will be shown that with quantum memory checkers one can get an exponential reduction on this lower bound.

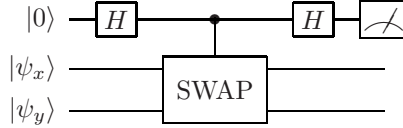
2.2 Quantum Simultaneous Message Protocol

Buhrman et al. [3] extended the classical simultaneous message (SM) model [9,7] to the quantum setting. In this model there are three players: Alice has a bit-string x , Bob has another bit-string y , and they do not share entanglement or randomness, but they each send one quantum message to a referee, Carol, who tries to compute the function value $f(x, y)$. The complexity measure of this protocol is the number of qubits used in the messages. Classically, for the EQUALITY function (Carol's output has to be $f = 1$ if $x = y$, and $f = 0$ otherwise), Newman and Szegedy [7] showed that the randomized SM complexity of the EQUALITY function on $\{0, 1\}^n$ has the lower bound $\Omega(\sqrt{n})$. Buhrman et al. presented a quantum protocol for the EQUALITY function that enabled the referee to compute $f(x, y)$ by comparing the two “quantum fingerprints” $|\psi_x\rangle$ and $|\psi_y\rangle$ of x and y sent by Alice and Bob, respectively. The communication complexity of this protocol is $O(\text{polylog } n)$ qubits.

The protocol works as following: for $x, y \in \{0, 1\}^n$ we use an error correcting code $E : \{0, 1\}^n \rightarrow \{0, 1\}^m$ with $m = cn$. The Hamming distance between two distinct codewords $E(x)$ and $E(y)$ (with $x \neq y$) is at least δm , with $\delta > 0$ a constant. Let $E_i(x)$ denote the i^{th} bit of $E(x)$. Alice constructs the superposition

$$|\psi_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^m (-1)^{E_i(x)} |i\rangle$$

as the fingerprint of her input x . Similarly Bob construct $|\psi_y\rangle$ for his input y and both of them send the fingerprints (of size $\log m = O(\log n)$ qubits) to Carol. Carol performs the “Controlled-SWAP test” shown in the following circuit:



If the measurement of the first register is 0, Carol decides that $x = y$; otherwise she concludes $x \neq y$. It is easy to show that the probability of Carol measuring “0” equals $\frac{1}{2} + \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2$ and the probability of measuring “1” is $\frac{1}{2} - \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2$. Therefore, when $x = y$ the probability of Carol measuring “0” is 1, while when $x \neq y$ the probability of measuring “0” is at most $\frac{1}{2} + \frac{1}{2}|\langle\psi_x|\psi_y\rangle|^2$. If we perform this test repeatedly for k copies of $|\psi_x\rangle$ and $|\psi_y\rangle$ with $x \neq y$, the probability of measuring all zeros is $(\frac{1+|\langle\psi_x|\psi_y\rangle|^2}{2})^k$, which decays exponentially in k .

2.3 Locally Decodable Codes

To construct the quantum fingerprints, we first encode the string using error correcting codes. In this paper, we use a locally decodable codes (see for example Katz and Trevisan [5]) such that a single bit x_j of the original data can be probabilistically reconstructed by reading only a small number of locations in

the encoding $E(x)$. Formally speaking [5], for fixed $\delta, \epsilon > 0$ and integer q we say that $E : \{0, 1\}^n \rightarrow \{0, 1\}^m$ is a (q, δ, ϵ) -*locally decodable code* (LDC) if there exists a probabilistic algorithm that reads at most q bits of $E(x)$ to determine one of the bits of x_j and if that same algorithm returns the correct value with probability at least $1/2 + \epsilon$ on all strings $y \in \{0, 1\}^m$ with Hamming distance $d(y, E(x)) \leq \delta m$.

It is not important for us to choose a perfect LDC in our memory checker. In our algorithm, considering the fact that it takes too much time if it starts from the original string to construct the quantum fingerprints, we encode the string and store its codeword on the public memory to speed up the processing. On the other hand, if we use any other error correcting code where decoding requires to query the whole codeword, it takes too much time for the user to retrieve a bit. This leads us to use LDCs. For our purposes it will be sufficient to use the construction of Babai et al. [1], who constructed an LDC with $q \in \text{polylog}(n)$ queries and $m \in O(n^2)$ for fixed δ and ϵ .

3 Quantum Algorithm for Online Memory Checking

In this section, we state the main theorem of this paper.

Theorem 1. *For any error rate $\epsilon > 0$, there exists a quantum online memory checker with space complexity $s \in O(\log(1/\epsilon) \log n)$ and query complexity $t \in O(\log(1/\epsilon) \log n + \text{polylog } n)$, where n is the size of the public bitstring. This checker answers the user correctly with constant probability at least $1 - \epsilon$ when the memory $\mathcal{M}$ acts correctly, and it replies “buggy” with probability at least $1 - \epsilon$ when $\mathcal{M}$ has been corrupted.*

We prove Theorem 1 by presenting a quantum online memory checker with the claimed upper bounds on the space complexity s and query complexity t of the checker.

3.1 Online Memory Checking Using Quantum Fingerprints

The proposed quantum memory checker $\mathcal{C}$ uses the following ingredients. Let $x = x_1 \dots x_n$ be the string that the user $\mathcal{U}$ wants to write to the public memory $\mathcal{M}$.

Public: The memory checker $\mathcal{C}$ uses a q -query locally decodable code $E : \{0, 1\}^n \rightarrow \{0, 1\}^m$ and writes the codeword $E(x) \in \{0, 1\}^m$ to the public memory $\mathcal{M}$.

Private: The memory checker maintains k copies of the quantum fingerprint

$$|\psi_x\rangle := \frac{1}{\sqrt{m}} \sum_{j=1}^m (-1)^{E(x)_j} |j\rangle$$

of x in its private memory (the value of k will be determined later).

Every time a “retrieve” instruction is executed, the memory checker obtains k summary states $|y\rangle$ of the current state of the public memory $\mathcal{M}$. By comparing these new quantum fingerprints with those in the checker’s private memory, the checker can detect any malicious changes that would corrupt the decoding of $E(x)$ to the public memory with high probability. Specifically, the checker uses the following two protocols.

Retrieve (x_i) protocol:

- When a “retrieve” request is issued by the user the memory checker queries the public memory to obtain k “summary states”

$$|y\rangle = \frac{1}{\sqrt{m}} \sum_j (-1)^{y_j} |j\rangle.$$

- The checker performs the Controlled-SWAP test on the k copies of $|y\rangle$ and $|\psi_x\rangle$ as defined in Section 2.2.
- If any of the k measurement outputs 1, the checker replies “buggy”.
- Otherwise, the checker runs the decoding algorithm of the locally decodable code E to reconstruct the bit x_j the user requests (which requires q queries to the public memory) and returns this bit to the user.
- The checker then replaces the $|\psi_x\rangle$ fingerprints in its local memory with k new summaries $|y\rangle$ of the public memory.

Store (x) Protocol:

- When a “store” request is issued, the checker first queries the public memory as in the first 3 steps of the previous protocol to verify that the public memory and private fingerprints coincide with each other.
- The checker computes the codeword $E(x)$ for the new input and writes it to the memory.
- It also computes new fingerprint $|\psi_x\rangle$ and stores k copies into its private memory.

The complexity measure of this protocol is as follows. For simplicity, we assume here the sub-optimal parameters of the LDC of Babai et al. [1] with $q \in \text{polylog } n$ and $m \in O(n^2)$. The space complexity is the private memory holding the fingerprints of x , which is $O(k \log n)$ qubits; the query complexity is the number of qubits answered by $\mathcal{M}$ per request, which includes the k copies of the fingerprints and the queries of LDC; this amounts to $O(k \log n + \text{polylog } n)$ qubits.

3.2 Correctness of the Quantum Online Memory Checker

Based on the definition of online memory checker in Section 2, a correct checker should answer the user correctly when the public memory $\mathcal{M}$ is correct with probability at least $1 - \epsilon$; and the checker should detect the error when $\mathcal{M}$ ’s

output is incorrect with probability also at least $1 - \epsilon$, such that $0 < \epsilon < \frac{1}{2}$ is the error rate of the protocol. Let us examine the behavior of our quantum online memory checker.

- When $\mathcal{M}$ is uncorrupted, i.e. when $y = E(x)$, we have $|\langle \psi_x | y \rangle| = 1$ and the probability of measuring 0 after the Controlled-SWAP test is 1. Hence the checker will output the correct answer in this case.
- When $\mathcal{M}$ has been changed by the adversary, i.e. when $y \neq E(x)$, Lemma 1 and Lemma 2 applies.

Lemma 1. *Assume a memory checker uses error correcting codes of length m with Hamming distance between two distinct codeword being at least δm (where $\delta > 0$ is a constant). With $k = \lceil \frac{\log \epsilon}{\log(1-2\delta+2\delta^2)} \rceil$ copies of the fingerprint $|\psi_x\rangle$, the checker will detect the difference between the two fingerprints $|\psi_{\tilde{x}}\rangle$ and $|\psi_x\rangle$ with probability at least $1 - \epsilon$.*

Proof. Since we are using error correcting code where two distinct codewords have Hamming distance at least δm , at least δm bits of the public memory have been changed. Hence for two distinct codeword $E(x)$ and $E(\tilde{x})$, $|\langle \psi_x | \psi_{\tilde{x}} \rangle| \leq 1 - 2\delta$. Therefore, for k copies, we measure all zeros with probability at most

$$\left(\frac{1 + |\langle \psi_x | \psi_{\tilde{x}} \rangle|^2}{2} \right)^k \leq (1 - 2\delta + 2\delta^2)^k.$$

In order for the checker to detect the error of the memory with probability at least $1 - \epsilon$, the above equation should have a value less than ϵ . Therefore, if we pick $k \geq \lceil \frac{\log \epsilon}{\log(1-2\delta+2\delta^2)} \rceil$, the checker will output “buggy” with probability at least $(1 - \epsilon)$ when $\mathcal{M}$ is corrupted.

Lemma 1 only deals with the situation where the codeword is changed to another codeword. There remains one problem though. The adversary can change a few bits of $\mathcal{M}$ in small steps such that at no point there will be big difference between the summary of the public memory and the private fingerprints of the checker. But after a sequence of such changes, the codeword can eventually be changed into another $E(\tilde{x})$ with $\tilde{x} \neq x$. In this situation, we have to determine if it possible for the checker to detect the attack with high probability. Let us formalize this situation.

Problem of incremental changes of public memory: The adversary changes a codeword $E(x)$ into another legal codeword $E(\tilde{x})$ with $x \neq \tilde{x}$ in T steps: in each step, the adversary flips d_i bits of the public memory ($1 \leq i \leq T$), so that at step T , it will be changed into another codeword, i.e. $\sum_{i=1}^T d_i \geq \delta m$. Without loss of generality, we assume that in each step the adversary changes different bits, so that once a bit is flipped in one step, it will not be flipped back in the following steps. The problem we are interested in is what the probability is for the checker to detect such an attack.

In each step, the probability for the checker to accept the response from $\mathcal{M}$ is at most $\frac{1}{2} + \frac{1}{2}(|\langle \psi_x | \psi_y \rangle|^2) = \frac{1}{2} + \frac{1}{2}(1 - \frac{2d_i}{m})^2$. Define $\Delta_i := \frac{d_i}{m}$ such that

$\Delta = \sum_{i=1}^T \Delta_i \geq \delta$. Therefore, the probability P_T for the checker to measure all “0” (accept) for all T steps is

$$P_T(\Delta_1, \dots, \Delta_T) = \prod_{i=1}^T (1 - 2\Delta_i + 2\Delta_i^2).$$

Lemma 2. *If the adversary changes Δm bits of the codeword in T steps, then the highest possible probability of the checker not detecting the corruption is achieved if all bits get flipped in one step. That is, for all $\Delta_i \geq 0$ with $\Delta_1 + \dots + \Delta_T = \Delta$ we have $P_T(\Delta_1, \dots, \Delta_T) \leq P_1(\Delta)$.*

Proof. We prove this lemma by induction on T .

First, we prove that $P_2(\Delta_1, \Delta_2) \leq P_1(\Delta_1 + \Delta_2)$. We have

$$P_1(\Delta_1 + \Delta_2) = P_1(\Delta) = 1 - 2\Delta + 2\Delta^2$$

and

$$\begin{aligned} P_2(\Delta_1, \Delta_2) &= P_2(\Delta_1, \Delta - \Delta_1) \\ &= (1 - 2\Delta_1 + 2\Delta_1^2)(1 - 2(\Delta - \Delta_1) + 2(\Delta - \Delta_1)^2) \end{aligned}$$

Therefore,

$$P_1(\Delta_1 + \Delta_2) - P_2(\Delta_1, \Delta_2) = 4\Delta_1(\Delta - \Delta_1)(\Delta + \Delta_1(\Delta - \Delta_1)) \geq 0$$

The last inequality holds because $0 \leq \Delta_1 \leq \Delta$.

Assuming the lemma holds for all $T = k - 1$, let us examine $T = k$.

$$P_k(\Delta_1, \dots, \Delta_k) = \prod_{i=1}^k (1 - 2\Delta_i + 2\Delta_i^2)$$

By definition and the induction hypothesis for $T = 2$ and $T = k - 2$,

$$\begin{aligned} P_k(\Delta_1, \dots, \Delta_k) &= P_{k-2}(\Delta_1, \dots, \Delta_{k-2}) \cdot P_2(\Delta_{k-1}, \Delta_k) \\ &\leq P_1(\Delta_1 + \dots + \Delta_{k-2}) \cdot P_1(\Delta_{k-1} + \Delta_k) \\ &\leq P_1(\Delta_1 + \dots + \Delta_k) = P_1(\Delta) \end{aligned}$$

Therefore, Lemma 2 holds for all $T \geq 1$.

From this lemma it follows that the probability that the adversary remains undetected is bounded by $P_T(\Delta_1, \dots, \Delta_T) \leq P_1(\delta) = 1 - 2\delta + 2\delta^2$, with $\Delta_1 + \dots + \Delta_T \geq \delta$.

The just derived probabilities are based on one copy of $|\psi_x\rangle$ and $|y\rangle$. When we have k copies, the probability of measuring all zeros is not greater than $(1 - 2\delta + 2\delta^2)^k$. Therefore, if we pick $k \geq \lceil \frac{\log \epsilon}{\log(1 - 2\delta + 2\delta^2)} \rceil$, the checker will output “buggy” with probability at least $(1 - \epsilon)$ if $\mathcal{M}$ is being corrupted.

Therefore, we can conclude that when we pick $k \geq \lceil \frac{\log \epsilon}{\log(1-2\delta+2\delta^2)} \rceil$, our quantum online memory checker works correctly. Since δ and ϵ are predetermined constants, k is a constant as well. Therefore, the total complexity of this checker is: space complexity $O(\log(1/\epsilon) \log n)$ and query complexity $O(\log(1/\epsilon) \log n + \text{poly}(\log n))$. This finishes the proof of Theorem 1.

Applying the same techniques as in [6], we have the conclusion that our algorithm reaches the lower bound for quantum online memory checking.

4 Open Question

The online memory checker in this article uses quantum mechanics both in its local memory and the communications with the public memory. A variation of this model is a checker that stores quantum information in its local memory, but communicates in classical bits to the public memory.

In a simultaneous message protocol, if one message is quantum, while the other is restricted to be classical, Regev and De Wolf have shown that it requires a total of $\Omega(\sqrt{n/\log n})$ bits/qubits to compute the EQUALITY function [4], and hence such a hybrid setting is not significantly more efficient than classical-classical protocols. This result however does not directly translate into a lower bound on the $s \times t$ complexity for quantum memory checking with classical communication.

Using the same techniques as in [6], a quantum online memory checker with classical queries can be reduced to a modified consecutive messages (CM) protocol. In this CM protocol, Alice is allowed to send quantum messages to Carol and publish a quantum public message, while Bob is restricted to classical messages. For this CM protocol, there is an efficient solution as following: Receiving an input x , Alice computes its quantum fingerprints $|\psi_x\rangle$ and publish it as a public message; Bob, receiving y , computes a quantum fingerprints $|\psi_y\rangle$ and compares it with $|\psi_x\rangle$; Bob then sends Carol the result of the Controlled-SWAP testing, who outputs the final result. The communication complexity for this protocol is $O(\log n)$.

Due to the difference between the quantum-classical CM model and SM protocol for EQUALITY testing, it is not easy to draw a conclusion for the lower bound of quantum online memory checking with classical communications. Nevertheless we conjecture that there is no efficient quantum online memory checker for this setting.

5 Conclusion

In this paper, we consider the problem of constructing an online memory checker. By using the quantum fingerprints, we reduce the space complexity s and query complexity t from $s \times t \in \Omega(n)$ to $s \in O(\log n)$ and $t \in O(\log n)$.

Acknowledgment. This material is based upon work supported by the National Science Foundation under Grant No. 0729172 (“Quantum Algorithms for Data Streams”).

References

1. Babai, L., Fortnow, L., Levin, L.A., Szegedy, M.: Checking computations in polylogarithmic time. In: STOC 1991: Proceedings of the twenty-third annual ACM symposium on Theory of computing, pp. 21–32. ACM, New York (1991)
2. Blum, M., Evans, W.S., Gemmell, P., Kannan, S., Naor, M.: Checking the correctness of memories. *Algorithmica* 12(2/3), 225–244 (1994)
3. Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum fingerprinting. *Physical Review Letters* 87, 167902 (2001)
4. Gavinsky, D., Regev, O., de Wolf, R.: Simultaneous communication protocols with quantum and classical messages. *Chicago Journal of Theoretical Computer Science* 2008(7) (December 2008), <http://arxiv.org/abs/0807.2758>
5. Katz, J., Trevisan, L.: On the efficiency of local decoding procedures for error-correcting codes. In: STOC 2000: Proceedings of the thirty-second annual ACM symposium on Theory of computing, pp. 80–86. ACM, New York (2000)
6. Naor, M., Rothblum, G.N.: The complexity of online memory checking. *Journal of the ACM* 56(1), 1–46 (2009)
7. Newman, I., Szegedy, M.: Public vs. private coin flips in one round communication games (extended abstract). In: STOC 1996: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 561–570. ACM, New York (1996)
8. Trevisan, L.: Some applications of coding theory in computational complexity. *Quaderni di Matematica* 13, 347–424 (2004)
9. Yao, A.C.-C.: Some complexity questions related to distributive computing. In: STOC 1979: Proceedings of the eleventh annual ACM symposium on Theory of computing, pp. 209–213. ACM, New York (1979)

On the Structure of Protocols for Magic State Distillation

Earl T. Campbell and Dan E. Browne

Department of Physics and Astronomy, University College London, Gower Street,
London, WC1E 6BT, UK
`e.campbell@ucl.ac.uk`,
`d.browne@ucl.ac.uk`

Abstract. We present a theorem that shows that all useful protocols for magic state distillation output states with a fidelity that is upper-bounded by those generated by a much smaller class of protocols. This reduced class consists of the protocols where multiple copies of a state are projected onto a stabilizer codespace and the logical qubit is then decoded.

1 Introduction

To prevent noise and decoherence from destroying quantum information, the information can be stored in delocalised degrees of freedom of a larger system. This may be an encoding in a stabilizer code, where information is stored in a subspace of states that are eigenstates of particular tensor products of Pauli operators, known as the stabilizer of the code [1,2]. More exotic physical systems, composed of particles obeying anyonic statistics, can store quantum information in topological degrees of freedom [3,4]. However, to perform computational tasks it is necessary to manipulate the quantum information without producing correlated and uncorrectable errors, which is a more difficult task once the information is delocalized.

A logical operation that is performed *transversally* does not couple subsystems within the same encoding block [5]. It cannot produce correlated errors, and hence is well suited for a fault tolerant computation scheme. For example, an encoded Hadamard applied to the 7-qubit Steane code [1] is simply 7 single qubit Hadamards, $H_L = H^{\otimes 7}$, and so is transversal.

It has, however, been recently shown that no stabilizer code can protect against a generic noise model and provide a universal set of transversal gates [6]. Furthermore, the only experimentally observed anyons also fall short of providing a universal set of topologically protected gates [7,8,9]. In stabilizer codes the most common group of transversal gates is the Clifford group, the group of unitaries that map the set of tensor products of Pauli operators to itself. The Clifford group is also inherently protected in some topological schemes for quantum computation. Above fault tolerance error thresholds, high fidelity Clifford group unitaries can be achieved. It is therefore well motivated to abstract away

from fault tolerant operations on encoded qubits, and consider ideal Clifford group operations acting on unencoded qubits.

Quantum devices which only prepare stabilizer states and perform unitaries in the Clifford group can be efficiently simulated by a classical computer, and so cannot offer any computational advantage [10,11]. Despite this, such devices can be promoted to a fully universal quantum computer by using a resource of pure single-qubit non-stabilizer states, such as the so-called magic states [12]. Since preparation of these resource states is not typically fault tolerant, Bravyi and Kitaev introduced “magic state distillation”, a class of protocols which, given perfect Clifford operations, allow one to distill from many copies of certain mixed states, a state which is closer in fidelity to a pure non-stabilizer state. Repeated iteration of the protocol generates, in the limit of many iterations, one of a number of pure non-stabilizer states, known as the “magic states”. Given a supply of such states, Clifford group unitaries are sufficient for universal quantum computation [12].

A number of protocols for magic state distillation have been proposed [12,13,14,15], but all follow the same format. They prescribe projecting several copies of the initial state onto a stabilizer codespace and then decoding from the codespace to a single qubit state. The prominence of stabilizer codes in magic state distillation, and a dearth of other species of protocol, is rather surprising, since the protocols have several key differences from quantum error correction schemes. For example, the initial state is an uncorrelated tensor product, not a code-state subject to local noise, and unlike in quantum error correction, error syndromes detected via the stabilizer measurements cannot be corrected. Here we resolve this puzzle by proving that for every effective magic state protocol there exists a stabilizer code protocol that achieves the same or better fidelity.

In the following sections we first define some key concepts and present examples. In section 5 we present the main theorem of this paper, and in the following sections and appendix we present a proof.

2 Clifford Reductions

We pose the problem of magic state distillation within the framework of what we call n -to-1 Clifford reductions:

Definition 1. *An n -to-1 qubit Clifford reduction takes an n -qubit resource state ρ_{nR} and outputs a single qubit ρ' using ideal Clifford unitaries, preparation of stabilizer states, classical feedforward, classical randomness, Pauli measurements and postselection.*

Most current protocols for magic state distillation take a resource state composed of n copies of a non-stabilizer state, so $\rho_{\text{nR}} = \rho_{\text{IR}}^{\otimes n}$. However, our definition encompasses any n -qubit mixed state. This definition covers all possible protocols that can be executed by a device capable of performing Clifford group operations to a quantum system whilst being controlled by a classical computer. We call a Clifford reduction a successful round of magic state distillation when the output

qubit has an improved fidelity w.r.t some pure non-stabilizer state. Here we are only really concerned with distillation on the level of an individual round. However, it is worth noting that generally distillation protocols require many rounds of concatenation, with many copies of the output qubit forming the resource for distillation in the next Clifford reduction.

Formally, n -to-1 qubit Clifford reductions are described by quantum operations of the following form:

$$\rho' = \frac{\text{tr}_{\text{nR}-1, \text{A}} \left(\sum_i K_i (\rho_{\text{nR}} \otimes |0\rangle\langle 0|^{\otimes m}) K_i^\dagger \right)}{\text{tr} \left(\sum_i K_i (\rho_{\text{nR}} \otimes |0\rangle\langle 0|^{\otimes m}) K_i^\dagger \right)}, \quad (1)$$

where the first n qubits are a resource in a non-stabilizer state ρ_{nR} and the next m qubits are ancilla in the stabilizer state $|0\rangle\langle 0|$. The partial trace is subscripted by $\text{nR} - 1, \text{A}$, to indicate that we trace over the ancillary Hilbert space, collectively labeled A, and every qubit in the resource Hilbert space, labeled nR, except for a single qubit labeled qubit 1. Each of the K_i are Clifford group Kraus operators and have the form:

$$K_i = k_i P_{i,N} C_{i,N} \dots P_{i,x} C_{i,x} \dots P_{i,1} C_{i,1}, \quad (2)$$

where $C_{i,x}$ are Clifford group unitaries and $P_{i,x}$ are Pauli projectors. In terms of the protocol, Pauli projectors occur when we measure a Pauli operator $s_{i,x}$ and postselect on outcome “+1”, or equivalently measure $-s_{i,x}$ and postselect on outcome “-1”, such that $P_{i,x} = (\mathbb{1} + s_{i,x})/2$. Finally, k_i is a real number smaller than or equal to unity. As with all quantum operations, we require $\sum_i K_i^\dagger K_i \leq \mathbb{1}$. The Kraus operator index i labels each *branch* of the protocol, with proliferation of branches occurring whenever a protocol specifies: (i) that we apply a different operation depending on the value of a random classical variable; (ii) we make a Pauli measurement but postselect on more than one outcome, possibly feeding forwarding that outcome to determine later operations, or (iii) we introduce an ancillary stabilizer state that is mixed. We can assume the ancilla are in the state $|0\rangle\langle 0|^{\otimes m}$ without loss of generality, as a Kraus operator can always rotate this state into a different pure stabilizer state.

3 The Steane Code Protocol

Before continuing with our general examination of protocols for magic state distillation, we will give a concrete example. The single-qubit pure stabilizer states are eigenstates of X , Y or Z and mixed stabilizer states are any probabilistic ensembles of these pure states. In the Bloch sphere, this convex set with 6 vertices forms the *stabilizer octahedron* shown in figure 1. The only non-stabilizer states known to be distillable from mixed states are eigenstates of Clifford group unitaries, such as the Hadamard H and the T operation¹. The corresponding

¹ The T rotation performs, $TXT^\dagger = Y$, $TYT^\dagger = Z$.

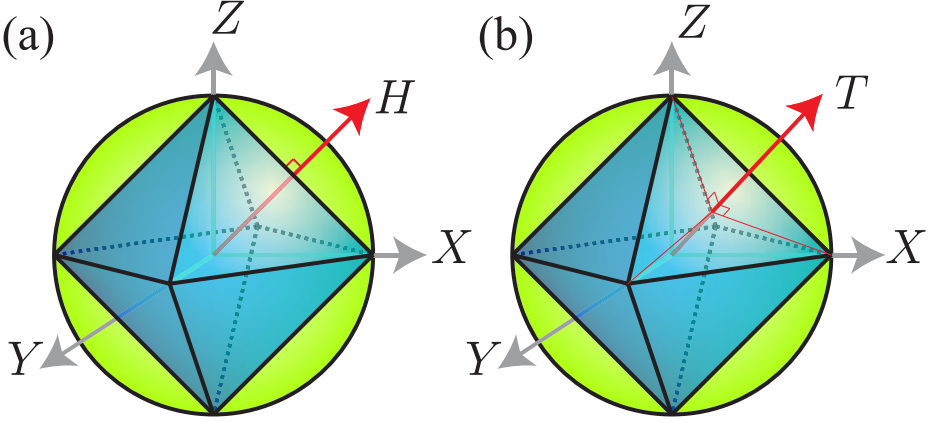


Fig. 1. The octahedron of mixed stabilizer states within the Bloch sphere with (a) the axis of the Hadamard rotation shown (b) the axis of the T rotation shown. The Hadamard axis bisects an edge of the stabilizer octahedron, and the T axis bisects the center of a face of the stabilizer octahedron. About their axes the Hadamard rotation is a 180 degree rotation, and the T rotation is a 120 degree rotation. Notice that the stabilizer octahedron has six vertices corresponding to the six pure stabilizer states.

eigenstates are denoted $|H\rangle = H|H\rangle$ and $|T\rangle = T|T\rangle$, and depolarized mixtures for these eigenstates are:

$$\begin{aligned}\rho(f, \sigma_H) &= (\mathbb{1} + (2f - 1)(X + Z)/\sqrt{2})/2, \\ \rho(f, \sigma_T) &= (\mathbb{1} + (2f - 1)(X + Y + Z)/\sqrt{3})/2,\end{aligned}\tag{3}$$

with fidelity $f = 1, 0$ for ideal magic states and $0 < f < 1$ when noisy. Other distillable magic states emerge from symmetries the stabilizer octahedron. Given the ability to prepare noisy copies of $\rho(f, \sigma_H)$, we can attempt a protocol proposed by Reichardt [13]:

1. Prepare a resource state $\rho_{\text{nR}} = \rho(f, \sigma_T)^{\otimes 7}$;
2. Measure the 6 stabilizer generators of the Steane code;
3. If any of the measurements give -1 then restart;
4. Otherwise, the protocol has succeeded. Decode the encoded state from the Steane codespace to a single qubit state.

Provided the fidelity, with respect to $|T\rangle$, of the initial noisy copies exceeds some threshold, the output qubit has an improved fidelity. Concatenation allows improvement towards fidelities arbitrarily close to unity. For completeness, we list the stabilizer generators of the Steane code:

$$\begin{aligned}X_1 X_2 X_3 X_4 \mathbb{1}_5 \mathbb{1}_6 \mathbb{1}_7, & X_1 X_2 \mathbb{1}_3 \mathbb{1}_4 X_5 X_6 \mathbb{1}_7, X_1 \mathbb{1}_2 X_3 \mathbb{1}_4 X_5 \mathbb{1}_6 X_7, \\ Z_1 Z_2 Z_3 Z_4 \mathbb{1}_5 \mathbb{1}_6 \mathbb{1}_7, & Z_1 Z_2 \mathbb{1}_3 \mathbb{1}_4 Z_5 Z_6 \mathbb{1}_7, Z_1 \mathbb{1}_2 Z_3 \mathbb{1}_4 Z_5 \mathbb{1}_6 Z_7.\end{aligned}\tag{4}$$

Note that the sign of all these operators is positive. Also note that the protocol post-selects only states resulting from positive measurement outcomes, and that states from other outcomes are discarded. As we will see later, in magic state distillation protocols there is always one choice of measurement outcome that leads to a fidelity unsurpassed by any other outcome.

4 Stabilizer Reductions

In addition to Reichardt's protocol there are numerous other protocols for magic state distillation, but they follow the same pattern of projecting onto the codespace of a stabilizer code, and decoding the logical qubit onto a single qubit. Codes that have been used in this context include the Steane code [13], the 5-qubit code [12], the 23 qubit Golay code [13], a 15-qubit quantum Reed-Muller code [12], and the simple 2 qubit parity checking code [15]. Furthermore, numerous other protocols derived from stabilizer codes have been numerically tested [12,15]. Note that, Knill's scheme for postselected quantum computing [16] contains a protocol reminiscent of magic state distillation, but which at first appears to be unrelated to any stabilizer code. However, Reichardt [13] has shown that Knill's proposal is actually closely related to the aforementioned quantum Reed-Muller code [12]. All of these protocols are what we call n -to-1 qubit stabilizer reductions:

Definition 2. *An n -to-1 qubit stabilizer reduction performs the following: (i) take an n -qubit resource ρ_{nR} ; (ii) measure the $(n-1)$ generating operators of an n -qubit stabilizer code $\mathcal{S}_{n-1}$ with one logical qubit; (iii) postselect on the all “+1” measurement syndrome; (iv) decode the logical qubit of the stabilizer code onto a single output qubit, ρ' .*

When we obtain the desired measurement outcome, the resource state is projected into the codespace of the stabilizer code supporting one logical qubit. All states inside the codespace are stabilized, $s|\psi\rangle = |\psi\rangle$, by all operators s that are elements to the stabilizer of the code $\mathcal{S}_{n-1}$. An encoded basis within this codespace is defined by a logical Pauli operator X_L that is not an element of the stabilizer code but does commute with all elements of the stabilizer. The encoded basis states are then $|+_L\rangle$ and $|-_L\rangle$, where $X_L|\pm_L\rangle = \pm|\pm_L\rangle$ and $s|\pm_L\rangle = |\pm_L\rangle$. The projection operator onto the codespace can be expressed in terms of the encoded basis states:

$$P_{\mathcal{S}_{n-1}} = |+_L\rangle\langle+_L| + |-_L\rangle\langle-_L| . \quad (5)$$

Another integral component of our definition of stabilizer reductions is *decoding*. We consider a decoding to be any Clifford unitary that maps $|+_L\rangle \rightarrow |+\rangle|\phi\rangle$ and $|-_L\rangle \rightarrow |-\rangle|\phi\rangle$, where $|\phi\rangle$ is a stabilizer state for all qubits except qubit 1. Note that there are many suitable decoding Clifford unitaries, partly because there are many suitable $|\phi\rangle$, but also because we are not interested in how the unitary maps states other than the encoded states $|\pm_L\rangle$.

Having defined the building blocks of a stabilizer reduction, it follows that after a successful stabilizer reduction the output qubit will be:

$$\rho' = \frac{\text{tr}_{\text{nR}-1} \left(C_{\text{decode}} P_{\mathcal{S}_{n-1}} \rho_{\text{nR}} P_{\mathcal{S}_{n-1}} C_{\text{decode}}^\dagger \right)}{\text{tr} \left(C_{\text{decode}} P_{\mathcal{S}_{n-1}} \rho_{\text{nR}} P_{\mathcal{S}_{n-1}} C_{\text{decode}}^\dagger \right)}, \quad (6)$$

This is also a Clifford reduction with a single Kraus operator:

$$\begin{aligned} K &= C_{\text{decode}} P_{\mathcal{S}_{n-1}}, \\ &= |+, \phi\rangle\langle +_L| + |-, \phi\rangle\langle -_L|, \end{aligned} \quad (7)$$

Whilst all stabilizer reductions are Clifford reductions, the converse is not true.

5 Theorem Outline

Since the class of Clifford reductions encompasses the class of stabilizer reductions, one might be tempted to hypothesize that in some scenarios it is desirable to employ a Clifford reduction not based on stabilizer codes. However, there is no existing evidence for this, as all existing protocols are essentially stabilizer reductions. We say “essentially” because a word of caution is necessary. Many existing proposals make use of the idea of twirling [12], a randomizing process, which thus requires more than one Kraus operator for its description. However, while twirling is useful as an analytic tool for simplifying proofs, it is not necessary in a physical implementation. For every stabilizer reduction that is preceded by twirling, there exists a derandomized stabilizer reduction where one applies the optimal choice of Clifford unitaries. This will be amongst the results we prove in deriving our main theorem, which we now state:

Theorem 1. *For all n -to-1 qubit Clifford reductions, all n -qubit resources ρ_{nR} and all single qubit pure states $|\Psi\rangle$, with an output qubit ρ' of fidelity $\langle\Psi|\rho'|\Psi\rangle$, at least one of the following is true:*

- (i) *there exists a stabilizer state with an equal, or greater, fidelity, so $\langle\Psi|\rho'|\Psi\rangle \leq |\langle\Psi|\phi\rangle|^2$, where $|\phi\rangle$ is any single qubit pure stabilizer state; or*
- (ii) *there exists an n -to-1 stabilizer code reduction that also consumes ρ_{nR} and outputs a qubit ρ'' with equal, or greater, fidelity, such that $\langle\Psi|\rho'|\Psi\rangle \leq \langle\Psi|\rho''|\Psi\rangle$.*

Our theorem contains two clauses, later to be referred to as clause (i) and (ii), and either one or both clauses may hold true in any individual case. However, only clause (ii) is interesting in the context of magic state distillation, as when clause (i) holds we could have achieved the same functionality without consuming the resource state ρ_{nR} at all.

6 Clifford Kraus Operators

Before proceeding, we derive a canonical form for Clifford group Kraus operators that we will employ throughout this paper. By definition, Clifford group operators conjugate Pauli operators to Pauli operators, such that $C\sigma'C^\dagger = \sigma$ and hence $\sigma C = C\sigma'$. Since Pauli projectors are composed of a Pauli operator and the identity — recall $P = (\mathbb{1} + \sigma)/2$ — then we also find that $PC = CP'$. All Clifford Kraus operators are composed of some sequence of Clifford unitaries and Pauli projectors, but by repeated conjugation all Clifford unitaries can be brought to the end of the operator, such that:

$$K = kC_N \dots C_2 C_1 P'_N \dots P'_2 P'_1 , \quad (8)$$

where we drop the subscript of K_i for brevity. Next, we prove that sequential non-commuting Pauli projectors, $P'_i P'_{i+1}$, can be simplified to a single Pauli projector. Each of these Pauli projectors has an associated stabilizer s'_i and s'_{i+1} , which must anticommute when the projectors do not commute. Therefore:

$$\begin{aligned} P'_i P'_{i+1} &= (\mathbb{1} + s'_i)(\mathbb{1} + s'_{i+1})/4 , \\ &= (\mathbb{1} + s'_i + s'_{i+1} + s'_i s'_{i+1})/4 , \\ &= (s'_i + s'_{i+1})(\mathbb{1} + s'_{i+1})/4 , \\ &= C' P'_{i+1} / \sqrt{2} , \end{aligned} \quad (9)$$

where $C' = (s'_i + s'_{i+1})/\sqrt{2}$ is a Clifford unitary that maps the projected subspace of P'_{i+1} to that of P'_i . This shows that sequential anti-commuting projectors can always be replaced by a single projector followed by a Clifford unitary. Continuing the process of conjugating through Clifford unitaries and removing non-commuting projectors, all K can be reordered to begin with commuting stabilizer projections followed by Clifford unitaries:

$$K = k' C P , \quad (10)$$

with P being:

$$P = P''_l \dots P''_2 P''_1 ; P''_a P''_b - P''_b P''_a = 0 ; \quad (11)$$

a collection of stabilizer projectors associated with a codespace of some stabilizer code, $\mathcal{S}_l$, with l generators $(s_1, s_2, \dots, s_l)$ where $s_j = 2P_j - \mathbb{1}$.

7 Branch Expansion/Reduction

Here we eliminate the need for considering many branches, and hence many K_i , by showing how one branch always provides an upperbound on the output fidelity. However, before eliminating excess branches, we must unpack some hidden branches from (1). This unpacking uses the property that a joint Hilbert space $\mathcal{H} \otimes \mathcal{H}'$, partially traced over Hilbert space $\mathcal{H}'$ satisfies:

$$\text{tr}_{\mathcal{H}'}[\rho] = \sum_j \text{tr}_{\mathcal{H}'}[(\mathbb{1}_{\mathcal{H}} \otimes |\phi_j\rangle\langle\phi_j|)\rho(\mathbb{1}_{\mathcal{H}} \otimes |\phi_j\rangle\langle\phi_j|)] , \quad (12)$$

where the set $\{|\phi_j\rangle\}$ form any orthonormal basis over Hilbert space $\mathcal{H}'$. This equation expresses the property that if one depolarises the state of an ancillary sub-system before tracing it out, it does not change the reduced state of the remaining sub-system. Applying this formula to (1) gives:

$$\rho' \propto \text{tr}_{\text{nR}-1, \text{A}} \left[\sum_{i, \mathbf{j}} (\mathbb{1}_1 \otimes |\mathbf{j}\rangle\langle\mathbf{j}|) K_i (\rho_{\text{nR}} \otimes |0\rangle\langle 0|^{\otimes m}) K_i^\dagger (\mathbb{1}_1 \otimes |\mathbf{j}\rangle\langle\mathbf{j}|) \right] , \quad (13)$$

where the bit-string $\mathbf{j} = (j_2, j_3, \dots, j_{n+m})$ has $n + m - 1$ elements and specifies a computational basis state $|\mathbf{j}\rangle = |j_2, j_3, \dots, j_{n+m}\rangle$, and since the partial trace excludes only the first qubit, this is the only qubit not included in $|\mathbf{j}\rangle$. The summation is performed over all i and all bit-strings $\mathbf{j}$. Note that, for brevity we drop the denominator and hence use a proportionality sign. We can now simplify the expression:

$$\rho' \propto \text{tr}_{\text{nR}-1, \text{A}} \left[\sum_{i, \mathbf{j}} K_{i, \mathbf{j}} (\rho_{\text{nR}} \otimes \mathbb{1}_\text{A}) K_{i, \mathbf{j}}^\dagger \right] , \quad (14)$$

where the new Kraus operators have incorporated the projectors:

$$K_{i, \mathbf{j}} = (\mathbb{1}_1 \otimes |\mathbf{j}\rangle\langle\mathbf{j}|_{\text{nR}-1, \text{A}}) K_i (\mathbb{1}_{\text{nR}} \otimes |0\rangle\langle 0|_\text{A}^{\otimes m}) . \quad (15)$$

We say this unpacks hidden branches because we are now summing over two indices $i, \mathbf{j}$. On first inspection, our introduction of these extra branches might seem mysterious, so we need some intuition to ground our mathematics. We observe that the new Kraus operator $K_{i, \mathbf{j}}$ always outputs a separable state, as qubits 2 through to $n + m$ are all projected into a computational basis state, and so are disentangled from the output qubit, labeled 1. In contrast, the original Kraus operator K_i allowed for qubit one to be entangled with the other qubits, and so after applying the partial trace we may incur further mixing of the output qubit. In exposing these hidden branches, what we have gained is certainly of the state of all qubits except the output qubit.

Having laid bare all branches, we now perform branch reduction, which relies on the convexity of fidelity measures. In general, for any mixture $\rho' = \sum_i p_i \rho'_i$, the fidelity w.r.t $|\Psi\rangle$ is convex, and so:

$$\langle \Psi | \rho' | \Psi \rangle \leq \langle \Psi | \rho'_{\text{Max}} | \Psi \rangle = \text{Max}_{\rho'_i} \langle \Psi | \rho'_i | \Psi \rangle . \quad (16)$$

Hence, for any Clifford reduction and any $|\Psi\rangle$, the fidelity is upper-bounded by the fidelity produced by one of the branches, so that

$$\langle \Psi | \rho' | \Psi \rangle \leq \langle \Psi | \frac{\text{tr}_{\text{nR}-1, \text{A}} \left[K_{\text{Max}} (\rho_{\text{nR}} \otimes \mathbb{1}_\text{A}) K_{\text{Max}}^\dagger \right]}{\text{tr} \left[K_{\text{Max}} (\rho_{\text{nR}} \otimes \mathbb{1}_\text{A}) K_{\text{Max}}^\dagger \right]} | \Psi \rangle , \quad (17)$$

where $K_{\text{Max}} = K_{i, \mathbf{j}}$ is the Kraus operator with i and $\mathbf{j}$ that maximize fidelity. The validity of this expression can be conveyed by a simple metaphor about a

foolish handyman and a smart handyman. The foolish handyman has a toolbox containing a number of screwdrivers of varying quality, and whenever he wishes to use a screwdriver he reaches in and selects one at random, hoping it is the best. The smart handyman has the same selection of screwdrivers, and also selects from his toolbox at random, however he only keeps his best screwdriver in his toolbox and leaves the rest at home. Here we do the same with our best Kraus operator.

8 Exposing the Decoding

Here we rearrange the optimal Kraus operator into a more intuitive form, which shows when the operator is either a trivial projection onto a stabilizer state or a more useful stabilizer reduction. From (15), we have:

$$K_{\text{Max}} = (\mathbb{1}_1 \otimes |\tilde{\mathbf{j}}\rangle\langle\tilde{\mathbf{j}}|_{\text{nR}-1,\text{A}}) K_i (\mathbb{1}_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m}) . \quad (18)$$

Examining the last projector applied, $(\mathbb{1}_1 \otimes |\tilde{\mathbf{j}}\rangle\langle\tilde{\mathbf{j}}|_{\text{nR}-1,\text{A}})$, this projects all but one qubit into a computational basis state. Consequentially, the whole operator must project onto either a two-dimensional, logical, subspace or a definite stabilizer state. In the former case, since all qubits but qubit 1 are left in a computational basis state, any logical qubit must have been decoded onto qubit 1. This is the rough intuition for what we shall now show formally. We first expand out K_i in the decomposition of (10):

$$K_{\text{Max}} = (\mathbb{1}_1 \otimes |\tilde{\mathbf{j}}\rangle\langle\tilde{\mathbf{j}}|_{\text{nR}-1,\text{A}}) k_i C_i P_i (\mathbb{1}_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m}) . \quad (19)$$

This operator begins with two consecutive projections, first $(\mathbb{1}_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m})$ then P_i . These projectors always reduce to a single projector (see Sect. 6), possibly followed by some Clifford unitary:

$$K_{\text{Max}} \propto (\mathbb{1}_1 \otimes |\tilde{\mathbf{j}}\rangle\langle\tilde{\mathbf{j}}|_{\text{nR}-1,\text{A}}) C'_i (P_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m}) . \quad (20)$$

where the first projector applied, $|0\rangle\langle 0|_{\text{A}}^{\otimes m}$, must always remain the first applied, though it is supplemented by a possible extra projector, P_{nR} , acting on the resource Hilbert space. Next, we expand out the identity operation, such that:

$$\mathbb{1}_1 = |+\rangle\langle +|_1 + |-\rangle\langle -|_1 , \quad (21)$$

We make this substitution to track how our potential logical qubit is influenced by the rest of the operator. It follows that:

$$K_{\text{Max}} \propto (|+\rangle\langle +|, \tilde{\mathbf{j}}) \langle +, \tilde{\mathbf{j}}| + |-\rangle\langle -, \tilde{\mathbf{j}}| C'_i (P_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m}) . \quad (22)$$

Next, we absorb the Clifford unitary into these stabilizer states, so that:

$$K_{\text{Max}} \propto (|+\rangle\langle +|, \tilde{\mathbf{j}}) \langle +_L| + |-\rangle\langle -, \tilde{\mathbf{j}}| \rangle P_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m} , \quad (23)$$

where $|\pm_L\rangle = (C'_i)^\dagger |\pm, \tilde{\mathbf{j}}\rangle$ are orthogonal stabilizer states. All that remains is to determine the effect of the projector $P_{\text{nR}} \otimes |0\rangle\langle 0|_{\text{A}}^{\otimes m}$ on these stabilizer states, and one can verify (details in App. A) that this projection gives either:

- (a) $K_{\text{Max}} \propto |\phi_1, \tilde{\mathbf{j}}\rangle\langle\pm'_L|$ where $|\phi_1\rangle$ is a single qubit stabilizer state on qubit 1; or
- (b) $K_{\text{Max}} \propto |+, \tilde{\mathbf{j}}\rangle\langle+_L| + |-, \tilde{\mathbf{j}}\rangle\langle-_L|$ where $|\pm'_L\rangle$ are orthogonal stabilizer states.

These different forms correspond to clause (i) and (ii) of our theorem. For form (a), the maximized Kraus operator K_{Max} projects qubit one onto a stabilizer state $|\phi_1\rangle$, and this state gives an upper bound on the fidelity of the Clifford reduction. Hence clause (i) of the theorem is always true when K_{Max} has form (a). Although form (b) is a stabilizer reduction, it still acts on the ancillary Hilbert space. In the next section, we show that the ancillary component can be eliminated, and so form (b) will entail the truth of clause (ii) of our theorem.

9 Ancillae Add Nothing

Here we show that when K_{Max} has form (b), we can find an equivalent Kraus operator that acts on only the resource qubits but outputs the same mixture. To see this, we first note that because $(P_{\text{nR}} \otimes |0\rangle\langle 0|_A^{\otimes m})|\pm'_L\rangle = |\pm'_L\rangle$, we can conclude that $|\pm'_L\rangle = |\pm''_L\rangle_{\text{nR}}|0\rangle_A^{\otimes m}$. Furthermore, we also know that $|\pm, \tilde{\mathbf{j}}\rangle$ is a separable state such that $|\pm, \tilde{\mathbf{j}}\rangle = |\pm, \tilde{\mathbf{j}}_{\text{nR}}\rangle_{\text{nR}}|\tilde{\mathbf{j}}_A\rangle_A$. Therefore, the Kraus operator has a simple tensor product structure w.r.t the ancillary/resource partitioning:

$$K_{\text{Max}} \propto \mathcal{K} \otimes |\tilde{\mathbf{j}}_A\rangle\langle 0|^{\otimes m}; \quad (24)$$

where we introduce the calligraphic $\mathcal{K}$ to describe the Kraus operator that only acts on the resource Hilbert space:

$$\mathcal{K} = |+, \tilde{\mathbf{j}}_{\text{nR}}\rangle\langle+_L| + |-, \tilde{\mathbf{j}}_{\text{nR}}\rangle\langle-_L|. \quad (25)$$

Substituting (24) into (17), we see that the ancillary terms can be traced out:

$$\begin{aligned} \langle\Psi|\rho'|\Psi\rangle &\leq \langle\Psi|\frac{\text{tr}_{\text{nR}-1,A}[(\mathcal{K} \otimes |\mathbf{j}_A\rangle\langle 0|^{\otimes m})(\rho_{\text{nR}} \otimes \mathbb{1}_A)(\mathcal{K} \otimes |\mathbf{j}_A\rangle\langle 0|^{\otimes m})^\dagger]}{\text{tr}[(\mathcal{K} \otimes |\mathbf{j}_A\rangle\langle 0|^{\otimes m})(\rho_{\text{nR}} \otimes \mathbb{1}_A)(\mathcal{K} \otimes |\mathbf{j}_A\rangle\langle 0|^{\otimes m})^\dagger]}|\Psi\rangle \quad (26) \\ \langle\Psi|\rho'|\Psi\rangle &\leq \langle\Psi|\frac{\text{tr}_{\text{nR}-1}[\mathcal{K}\rho_{\text{nR}}\mathcal{K}^\dagger]}{\text{tr}[\mathcal{K}\rho_{\text{nR}}\mathcal{K}^\dagger]}|\Psi\rangle. \end{aligned}$$

This expressions proves clause (ii) of our theorem, as $\mathcal{K}$ can always be accomplished by an n -to-1 qubit stabilizer reduction.

10 Conclusions and Acknowledgments

We have proven a theorem that shows that any protocol that uses Clifford group operations to reduce a non-stabilizer resource to a single qubit has a fidelity upperbounded by the fidelity of either a trivial protocol or a protocol derived from a stabilizer code, which we call a stabilizer reduction. Our theorem reveals why all known protocols for magic state distillation can be described by stabilizer reductions. Furthermore, this theorem will form an essential component in a

following paper [17] where the authors prove that for a particular family of resource states, all possible stabilizer reductions, and hence all possible Clifford reductions, do not have distillation thresholds that are tight against the set of stabilizer states.

The proof presented here has been cast in a general framework that compares two different classes of protocols, but it seems likely that there are numerous possible extensions. It should be fairly easy to extend the proof to cover qudit generalizations of the Clifford group and stabilizer states. More speculative is the question of whether a similar theorem holds for continuous variable quantum devices, where gaussian states and gaussian operations are frequently analogous [18] to stabilizer states and Clifford group operations. Finally, it might also be worthwhile exploring whether entanglement distillation obeys a similar theorem when the ideal Clifford group operations are also restricted to be local with respect to some partitioning.

The authors would like to thank Shashank Virmani, Matthew Hoban, Tobias Osborne, Ben Reichardt and Steve Flammia for interesting discussions. We acknowledge support from the Royal Commission for the Exhibition of 1851, the QIP IRC, QNET and the National Research Foundation and Ministry of Education, Singapore.

References

1. Steane, A.: Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A* 452, 2551 (1996)
2. Gottesman, D.: Theory of fault tolerant quantum computing. *Phys. Rev. A* 57, 127–137 (1998)
3. Kitaev, A.: Fault-tolerant quantum computation by anyons. *Ann. Phys.* 303, 2 (2003)
4. Raussendorf, R., Harrington, J., Goyal, K.: Topological fault-tolerance in cluster state quantum computation. *New J. Phys.* 9, 199 (2007)
5. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge (2000)
6. Eastin, B., Knill, E.: Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.* 102, 110502 (2009)
7. Moore, G., Read, N.: Nonabelions in the fractional quantum Hall effect. *Nuclear Physics B* 360, 362 (1991)
8. Lloyd, S.: Quantum computation with abelian anyons. *Quantum Information Processing* 1, 13 (2002)
9. Douçot, B., Vidal, J.: Pairing of Cooper pairs in a fully frustrated Josephson-junction chain. *Phys. Rev. Lett.* 88, 227005 (2002)
10. Gottesman, D.: *Stabilizer Codes and Quantum Error Correction*. PhD thesis, Caltech Ph.D. Thesis (1997)
11. Anders, S., Briegel, H.J.: Fast simulation of stabilizer circuits using a graph-state representation. *Phys. Rev. A* 73, 022334 (2006)
12. Bravyi, S., Kitaev, A.: Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* 71, 022316 (2005)
13. Reichardt, B.W.: Quantum universality from magic states distillation applied to CSS codes. *Quantum Information Processing* 4, 251 (2005)

14. Reichardt, B.W.: Error-detection-based quantum fault-tolerance threshold. *Algorithmica* 55, 517 (2009)
15. Reichardt, B.W.: Quantum universality by distilling certain one- and two-qubit states with stabilizer operations. arXiv:quant-ph/0608085v1 (2006)
16. Knill, E.: Quantum computing with realistically noisy devices. *Nature* 434, 39 (2005)
17. Campbell, E.T., Browne, D.E.: Bound States for Magic State Distillation. arXiv:0908.0836 (2009)
18. Bartlett, S.D., Sanders, B.C., Braunstein, S.L., Nemoto, K.: Efficient classical simulation of continuous variable quantum information processes. *Phys. Rev. Lett.* 88(9), 097904 (2002)

A Appendix: Deriving the Two Forms (a) and (b)

Here we show that the Kraus operator of (23) must be of either form (a) or (b). By definition Pauli projectors take stabilizer state to stabilizer states with the addition of some constant, so:

$$K_{\text{Max}} \propto c_+ |+, \tilde{\mathbf{j}}\rangle \langle +'_L| + c_- |-, \tilde{\mathbf{j}}\rangle \langle -'_L|, \quad (27)$$

where $|\pm'_L\rangle = (P_{\text{nR}} \otimes |0\rangle \langle 0|_{\text{A}}^{\otimes m}) |\pm_L\rangle / \sqrt{c_{\pm}}$ are stabilizer states but are not necessarily orthogonal. The variables $c_{\pm}$ can be assumed to be real by absorbing any phase into the definitions of $|\pm'_L\rangle$. Since relative phase may prove important, we remark that the phase absorbed will always be a multiple of i , and we will account for its effect later. If one term vanishes, either because $c_+ = 0$ or $c_- = 0$, then:

$$(a1) : K_{\text{Max}} \propto |\pm, \tilde{\mathbf{j}}\rangle \langle \pm'_L|; \quad (28)$$

which we refer to as form (a1) as this Kraus operator projects onto a stabilizer state, but in general projections onto a stabilizer state may occur in a different basis. When neither term vanishes, the coefficients must be equal, so $c_+ = c_-$. To deduce this equality, we first consider the first Pauli measurement, $P_i = (\mathbb{1} + s_i)/2$, on the stabilizer states $|\pm'_L\rangle$. Because the stabilizing operators of $|+_L'\rangle$ and $|-_L'\rangle$ differ only in phase, either both states are eigenstates of s_i or neither state is an eigenstate of s_i . For eigenstates of a projector, the projector either has no effect, or maps the state to zero. Hence, when $c_+ \neq 0$ or $c_- \neq 0$, the projectors acting on eigenstates must have no effect. As for projectors where $|+_L'\rangle$ and $|-_L'\rangle$ are not eigenstates of s_i , the measurement outcomes are equally random, so $\text{tr}[P_i |\pm_L\rangle \langle \pm_L|] = 1/2$. The same argument holds for subsequent Pauli measurements, and so we have that $c_+ = c_- = (1/2)^m$ where m is the number of component Pauli projections with a non-trivial effect. Now, if $|+_L'\rangle$ and $|-_L'\rangle$ retain their orthogonality, then form (b) follows immediately:

$$(b) : K_{\text{Max}} \propto |+, \tilde{\mathbf{j}}\rangle \langle +'_L| + |-, \tilde{\mathbf{j}}\rangle \langle -'_L|. \quad (29)$$

If we wish to remove any phase absorbed into the definition of $|\pm'_L\rangle$, this is simple as the phase is always a factor of i , and this can be removed by adding a subsequent Clifford unitary $\mathbb{1} \otimes (|+\rangle \langle +| + i^N |-\rangle \langle -|)_1$.

The last remaining possibility is when neither term vanishes but $|+_L'\rangle$ and $|-_L'\rangle$ lose their orthogonality. Since the initial states had commuting stabilizing operators, and the projection can not change this, if the vectors $|\pm_L'\rangle$ are not orthogonal they must correspond to the same state up to a relative phase i^N , and so $|-_L'\rangle = i^N|+_L'\rangle$. Hence, in this case

$$(a2) : K_{\text{Max}} \propto |+, \tilde{\mathbf{j}}\rangle\langle+_L'| + i^N|-, \tilde{\mathbf{j}}\rangle\langle+_L'| , \quad (30)$$

$$\propto |\phi_1, \tilde{\mathbf{j}}\rangle\langle+_L'| .$$

where $|\phi_1\rangle = (|+\rangle + i^N|-\rangle)/\sqrt{2}$ is a stabilizer state on the equator of the Bloch sphere. Hence, form (a1) and form (a2) account for all possible single qubit projections, and hence jointly comprise form (a). This completes our proof that we always have either form (a) or (b).

Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function

Takeshi Koshihara and Takanori Odaira

Area of Informatics, Graduate School of Science and Engineering,
Saitama University, Japan
koshihara@mail.saitama-u.ac.jp

Abstract. We provide a quantum bit commitment scheme which has statistically-hiding and computationally-binding properties from any approximable-preimage-size quantum one-way function, which is a generalization of perfectly-hiding quantum bit commitment scheme based on quantum one-way permutation due to Dumais, Mayers and Salvail. In the classical case, statistically-hiding bit commitment scheme is constructible from any one-way function. However, it is known that the round complexity of the classical statistically-hiding bit commitment scheme is $\Omega(n/\log n)$ for the security parameter n . Our quantum scheme as well as the Dumais-Mayers-Salvail scheme is non-interactive, which is advantageous over the classical schemes.

Keywords: Quantum bit commitment, one-way function, non-interactive.

1 Introduction

A bit commitment is a fundamental cryptographic protocol between two parties. The protocol consists of two phases: commit phase and reveal phase. In the commit phase, the sender, say Alice, has a bit b in her private space and she wants to commit b to the receiver, say Bob. They exchange messages and at the end of the commit phase Bob gets some information that represents b . In the reveal phase, Alice confides b to Bob by exchanging messages. At the end of the reveal phase, Bob judges whether the information gotten in the reveal phase really represents b or not. Basically, there are three requirements for secure bit commitment: the correctness, the hiding property and the binding property. The correctness guarantees that if both parties are honest then, for any bit $b \in \{0, 1\}$ Alice has, Bob accepts with certainty. The hiding property guarantees that (cheating) Bob cannot reveal the committed bit during the commit phase. The binding property guarantees that (cheating) Alice cannot commit her bit b such that Alice maliciously reveals $b \oplus 1$ as her committed bit but Bob accepts.

In the classical case, a simple argument shows the impossibility of bit commitment with the hiding and the binding properties both statistical. Thus, either hiding or binding must be computational. A construction of statistically-binding

scheme (Naor scheme) from any pseudorandom generator was given by Naor [19]. Since the existence of one-way functions is equivalent to that of pseudorandom generators [13], a statistically-binding scheme can be based on any one-way function. A construction of statistically-hiding scheme (NOVY scheme) from one-way permutation was given by Naor, Ostrovsky, Venkatesan and Yung [20]. After that, the assumption of the existence of one-way permutation was relaxed to that of approximable-preimage-size one-way function [8]. Finally, Haitner and Reingold [10] showed that a statistically-hiding scheme can be based on any one-way function by using excellent techniques in [21].

Since a statistically-binding (resp., statistically-hiding) bit commitment scheme is a building block for zero-knowledge proof (resp., zero-knowledge argument) systems [7,2], it is desirable to be efficient from several viewpoints (e.g., the total size of messages exchanged during the protocol, or the round number of communications in the protocol). While the round complexity of Naor's statistically-binding scheme is $O(1)$, the matching lower bound of the round complexity of statistically-hiding scheme is $\Theta(n/\log n)$ [15,9,11] for the security parameter n .

Let us move on the quantum case. After the unconditionally security of the BB84 quantum key distribution protocol was shown, the possibility of unconditionally secure quantum bit commitments had been investigated. Unfortunately, the impossibility of unconditionally secure quantum bit commitment was shown [16,17]. Thus, alternative approaches such as quantum string commitment [14] or cheat-sensitive quantum bit commitment [1,12,3] have been studied.

In this paper, we take the computational approach as in the classical case. Along this line, Dumais, Mayers and Salvail [6] showed a construction of perfectly-hiding quantum bit commitment scheme (DMS scheme) based on quantum one-way permutation. The non-interactivity in the DMS scheme is advantageous over the classical statistically-hiding bit commitments. Unfortunately, we have not find any candidate for quantum one-way permutation, because known candidates for classical one-way permutation are no longer one-way in the quantum setting due to Shor's algorithm [24]. Thus, reducing complexity assumption has been required. We observe that the DMS scheme is a kind of quantum counterpart of the NOVY scheme. Another important observation is that the "onto" property of quantum one-way permutation and the one-wayness can be respectively discussed. This observation enables us to replace one-way permutations in the DMS scheme with more general ones. By using the universal hashing technique for generalization over the NOVY scheme in [8] (originally appeared in [13]), we generalize the DMS scheme and show that a statistically-hiding quantum bit commitment scheme is constructible from any approximable-preimage-size quantum one-way function without losing the non-interactivity. (Note that approximable-preimage-size quantum one-way functions includes one-to-one quantum one-way functions as a special case and one-to-one quantum-one-way functions are more likely to exist. Also note that we do not need the quantum privacy amplification [22] due to the construction though we use the universal hashing technique.)

Actually, we show that if the underlying function is general quantum one-way then the computationally-binding property for quantum bit commitment is guaranteed, and if the underlying function has “almost-onto” property then the statistically-hiding property is guaranteed. This separable discussion enables us to realize what properties of quantum one-way functions are necessary in order to construct statistically-hiding and computationally-binding non-interactive quantum bit commitment schemes. Moreover, this opens the possibility of non-interactive quantum bit commitment schemes with both computationally-binding and hiding properties. If they exist, this is advantageous over the Naor scheme which is of the round complexity $O(1)$ but interactive. Finally note that if we allow interaction then Crépeau, L  gar   and Salvail [5] shows the existence of statistically-hiding and computationally-binding quantum bit commitment schemes of the round complexity $O(n^2)$ based on any quantum one-way function.

2 Preliminaries

2.1 Notations and Conventions

We denote the m -dimensional Hilbert space by H_m . Let $\{|0\rangle, |1\rangle\}$ denote the computational basis for H_2 . When the context requires, we write $|b\rangle_+$ to denote $|b\rangle$ in the computational basis. Let $\{|0\rangle_\times, |1\rangle_\times\}$ denote the diagonal basis, where $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. For any $x = x_1x_2 \cdots x_n \in \{0, 1\}^n$ and $\theta \in \{+, \times\}$, $|x\rangle_\theta$ denotes the state $\otimes_{i=1}^n |x_i\rangle_\theta$. We denote $|0\rangle \otimes \cdots \otimes |0\rangle$ by $|0\rangle$. For projections, we denote $\mathcal{P}_+^0 = |0\rangle\langle 0|$, $\mathcal{P}_+^1 = |1\rangle\langle 1|$, $\mathcal{P}_\times^0 = |0\rangle_\times\langle 0|_\times$, and $\mathcal{P}_\times^1 = |1\rangle_\times\langle 1|_\times$. For any $x \in \{0, 1\}^n$, we denote $\mathcal{P}_+^x = \otimes_{i=1}^n \mathcal{P}_+^{x_i}$ and $\mathcal{P}_\times^x = \otimes_{i=1}^n \mathcal{P}_\times^{x_i}$. For the sake of simplicity, we also write $\mathcal{P}^x$ instead of $\mathcal{P}_+^x$. We define $\theta(0) = +$ and $\theta(1) = \times$. Thus, for any $w \in \{0, 1\}$, $\{\mathcal{P}_{\theta(w)}^x\}_{x \in \{0, 1\}^n}$ is the von Neumann measurement.

For density matrices σ and ρ , we define $\delta(\sigma, \rho) \stackrel{\text{def}}{=} \|\sigma - \rho\|_1$, where $\|A\|_1 = \text{tr}\sqrt{A^\dagger A}$. For two classical random variables X and Y , there exists the corresponding density matrices ρ_X and ρ_Y . We sometimes write $\delta(X, Y)$ instead of $\delta(\rho_X, \rho_Y)$. We denote the min-entropy of a random variable X by $\mathbf{H}_\infty(X)$ and the Renyi entropy (of order 2) by $\mathbf{H}_2(X)$.

We denote the uniform distribution over $\{0, 1\}^n$ by U_n . For a set A , we sometimes use the same symbol to denote the uniform distribution over the set A . A function $\nu : \mathbb{N} \rightarrow \mathbb{R}$ is *negligible* if for every polynomial p there exists $n_0 \in \mathbb{N}$ such for all $n \geq n_0$, $\nu(n) < 1/p(n)$.

2.2 Quantum One-Way Functions

In order to give definitions of quantum one-way functions, we have to decide a model of quantum computation. In this paper, we consider (uniform or non-uniform) quantum circuit family. As a universal quantum gate set, we take the controlled-NOT, the one-qubit Hadamard gate, and arbitrary one-qubit non-trivial rotation gate. The computational complexity of a circuit $\mathcal{C}$ is measured

by the number of elementary gates (in the universal gate set) contained in $\mathcal{C}$ and denoted by $\text{size}(\mathcal{C})$. For any circuit family $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$, if $\text{size}(\mathcal{C}_n)$ is bounded by $p(n)$ for some polynomial p , $\mathcal{C}$ is called p -size circuit family.

Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a function family. To compute f , we need a circuit family $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ where $\mathcal{C}_n$ is a circuit on $m(n) \geq \ell(n)$ qubits. To compute $f_n(x)$ for $x \in \{0, 1\}^n$, we apply $\mathcal{C}_n$ to $|x\rangle \otimes |0\rangle^{\otimes m(n)-n}$. The output of $\mathcal{C}_n$ is obtained by the von Neumann measurement in the computational basis on $\ell(n)$ qubits.

Definition 1. A function family $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ is *quantum one-way* if

- there exists a p -size circuit family $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$ such that, for all $n \geq 1$ and all $x \in \{0, 1\}^n$, $\mathcal{C}_n(|x\rangle \otimes |\mathbf{0}\rangle) = f_n(x)$ with certainty;
- for every p -size circuit family $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}$, $\Pr[f_n(\mathcal{D}_n(f_n(U_n))) = f_n(U_n)]$ is negligible.

Definition 2. A function family $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ is $r(n)$ -*regular quantum one-way* if

- f is quantum one-way;
- for every n and every $x \in \{0, 1\}^n$, we have $|\{x' \in \{0, 1\}^n : f_n(x') = f_n(x)\}| = 2^{r(n)}$.

Definition 3. A function family $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ is *approximable-preimage-size (APS, for short) quantum one-way* if

- f is quantum one-way;
- the function $d_n(y) \stackrel{\text{def}}{=} \lceil \log(|f_n^{-1}(y)|) \rceil$ is computable with certainty by a p -size circuit family.

2.3 Quantum Bit Commitment

In a non-interactive quantum bit commitment scheme, honest Alice with her bit w starts with a system $\mathbf{H}_{\text{all}} = \mathbf{H}_{\text{keep}} \otimes \mathbf{H}_{\text{open}} \otimes \mathbf{H}_{\text{commit}}$ in the initial state $|\mathbf{0}\rangle$, executes a quantum circuit $\mathcal{C}_{n,w}$ on $|\mathbf{0}\rangle$ returning the final state $|\psi_w\rangle \in \mathbf{H}_{\text{all}}$ and finally sends the subsystem $\mathbf{H}_{\text{commit}}$ to Bob in the reduced state $\rho_B(w) = \text{tr}_A(|\psi_w\rangle\langle\psi_w|)$, where Alice's Hilbert space is $\mathbf{H}_A = \mathbf{H}_{\text{keep}} \otimes \mathbf{H}_{\text{open}}$. Once the system $\mathbf{H}_{\text{commit}}$ is sent to Bob, Alice has only access to $\rho_A(w) = \text{tr}_B(|\psi_w\rangle\langle\psi_w|)$, where Bob's Hilbert space is $\mathbf{H}_B = \mathbf{H}_{\text{commit}}$. To reveal the commitment, Alice needs only to send the system $\mathbf{H}_{\text{open}}$ together with w . Bob then checks the value of w by measuring the system $\mathbf{H}_{\text{open}} \otimes \mathbf{H}_{\text{commit}}$ with some measurement that is fixed by the protocol in view of w . Bob obtains w_0 , $w = 1$, or $w = \perp$ when the value of w is rejected.

Cheating Alice must start with the state $|\mathbf{0}\rangle$ of some system $\mathbf{H}_{\text{all}} = \mathbf{H}_{\text{extra}} \otimes \mathbf{H}_A \otimes \mathbf{H}_{\text{commit}}$. A quantum circuit $\mathcal{D}_n$ that acts on $\mathbf{H}_{\text{all}}$ is executed to obtain a state $|\psi\rangle$ and the subsystem $\mathbf{H}_{\text{commit}}$ is sent to Bob. Later, any quantum circuit $\mathcal{O}_n$

which acts on $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$ can be executed before sending the subsystem H_{open} to Bob. The important quantum circuits which act on $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$ are the quantum circuits $\mathcal{O}_{n,0}$ (resp., $\mathcal{O}_{n,1}$) which maximizes the probability that bit $w = 0$ (resp., $w = 1$) is revealed with success. Therefore, any attack can be modeled by triplets of quantum circuits $\{(\mathcal{D}_n, \mathcal{O}_{n,0}, \mathcal{O}_{n,1})\}_{n \in \mathbb{N}}$.

Let $s_0(n)$ (resp., $s_1(n)$) be the probability that she succeeds to reveal 0 (resp., 1) using the corresponding optimal circuit $\mathcal{O}_{n,0}$ (resp., $\mathcal{O}_{n,1}$). The definition of $s_w(n)$ explicitly requires that the value of w , which cheating Alice tries to open, is chosen not only before the execution of the measurement on $H_{\text{open}} \otimes H_{\text{commit}}$ by Bob but also before the execution of the circuit $\mathcal{O}_{n,w}$ by cheating Alice.

In the quantum setting, it is pointed out in [17] that the requirement “ $s_0(n) = 0 \vee s_1(n) = 0$ ” for the binding condition is too strong. Thus, we adopt a weaker condition $s(n) \stackrel{\text{def}}{=} s_0(n) + s_1(n) - 1 \leq \varepsilon$ where $\varepsilon(n)$ is negligible, which is the same condition as in [6].

Since we consider the computational binding, we modify the above discussion so as to fit the computational setting. Instead of the triplet $(\mathcal{D}_n, \mathcal{O}_{n,0}, \mathcal{O}_{n,1})$, we consider a pair $(\mathcal{D}_{n,0}, \mathcal{U}_n)$. If we set $\mathcal{D}_{n,0} = (\mathcal{O}_{n,0} \otimes \mathcal{I}_{\text{commit}}) \cdot \mathcal{D}_n$, and $\mathcal{U}_n = \mathcal{O}_{n,1} \cdot \mathcal{O}_{n,0}^\dagger$, we can easily see that the adversary’s strategy does not change. Note that $\mathcal{D}_{n,0}$ acts in H_{all} and $\mathcal{U}_n$ is restricted to act only in $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$.

Definition 4. A non-interactive quantum bit commitment is *computationally-binding* if, for every a family $\{(\mathcal{D}_{n,0}, \mathcal{U}_n)\}_{n \in \mathbb{N}}$ of p-size circuit pairs, $s(n)$ is negligible.

Definition 5. A non-interactive quantum bit commitment is *statistically-hiding* if $\delta(\rho_B(0), \rho_B(1))$ is negligible.

2.4 Universal Hashing

Let $H = \{H_n\}_{n \in \mathbb{N}}$ be a sequence of function families, where each H_n is a family of functions mapping binary strings of length $\ell(n)$ to strings of length $v(n)$. We say that H_n is *2-universal hash family* if for any distinct $x, x' \in \{0, 1\}^{\ell(n)}$ and $y, y' \in \{0, 1\}^{v(n)}$,

$$\Pr_{h \leftarrow H_n} [h(x) = y \wedge h(x') = y'] = 2^{-2v(n)}.$$

(See, e.g., [4] for an implementation of 2-universal hash family. For example, there exists a 2-universal hash family H_n such that $|H_n| = 2^{2n}$.)

One of the useful applications of universal hash family is smoothing the min-entropy of given distribution. The following is also known as privacy amplification.

Lemma 1. (*Leftover Hash Lemma*) Let V_n be a random variable over $\{0, 1\}^{\ell(n)}$ such that $H_\infty(V_n) = \lambda_n$ and H_n be a 2-universal hash family where each $h \in H_n$ maps strings of length $\ell(n)$ to strings of length $v(n) = \lambda_n - 2 \log(\varepsilon^{-1})$. Then $\delta((H_n, H_n(V_n)), (H_n, U_{v(n)})) \leq \varepsilon/2$.

3 Our Scheme

Our scheme is almost similar to the DMS scheme. Instead of a family of one-way permutations, we use just a function family. Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a function family. The quantum bit commitment scheme takes the security parameter n and the description of function family f as common inputs. For given f and the security parameter n , Alice and Bob determines f_n . In the commit phase, Alice with her bit w first chooses $x \in \{0, 1\}^n$ uniformly and computes $y = f_n(x)$. Next, Alice sends the quantum state $|f_n(x)\rangle_{\theta(w)} \in \mathbf{H}_{\text{commit}}$ to Bob. Bob then stores the received quantum state until the reveal phase. In the reveal phase, Alice first announces w and x to Bob. Next, Bob measures ρ_B with measurement $\{P_{\theta(w)}^y\}_{y \in \text{range}(f_n)}$ and obtains the classical output $y' \in \text{range}(f_n)$. Lastly, Bob accepts if and only if $y' = f_n(x)$.

Before we mention the security of our scheme, we introduce another property for (not necessarily quantum one-way) functions.

Definition 6. A function family $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ is *almost-onto* if $\delta(f_n(U_n), U_{\ell(n)})$ is negligible.

Theorem 1. Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a quantum one-way function family. Then our scheme is computationally binding.

Theorem 2. Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a family of almost-onto functions. Then our scheme is statistically hiding.

We will show the proofs in the next section. Note that the “almost-onto” property is not necessary to show the computationally-binding and the one-wayness is not necessary to show the statistically-hiding. Thus, above two theorems can be regarded as a refinement of the security proof for the DMS scheme.

Lemma 2. Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a family of $r(n)$ -regular quantum one-way functions and $\{H_n\}_{n \in \mathbb{N}}$ be a sequence of a 2-universal hash family H_n , where each function h in H_n maps strings of length $\ell(n)$ to strings of length $(1 - 2c)n - r(n)$ for some constant $c < 1/2$. Then

$$f' = \{f'_n(h, x) \stackrel{\text{def}}{=} (h, h(f_n(x))) : H_n \times \{0, 1\}^n \rightarrow H_n \times \{0, 1\}^{(1-2c)n-r(n)}\}_{n \in \mathbb{N}}$$

is a family of almost-onto quantum one-way functions.

Proof. We consider the construction $f'_n(h, x) = (h, h(f_n(x)))$. From Lemma 1, we have

$$\delta((H_n, H_n(f_n(U_n))), (H_n, U_{(1-2c)n-r(n)})) < 2^{-cn-1}.$$

If there exists an inverter for f' we can construct an inverter for f by a simple reduction argument. $\square$

Corollary 1. A statistically-hiding and computationally-binding quantum bit commitment scheme is constructible from a regular quantum one-way function family.

Lemma 3. Let $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$ be a family of APS quantum one-way functions, $\mathcal{H} = \{H_n\}_{n \in \mathbb{N}}$ a sequence of 2-universal hash family H_n where each $h \in H_n$ maps strings of length n to strings of length n , and $\mathcal{H}' = \{H'_n\}_{n \in \mathbb{N}}$ a sequence of 2-universal hash family H'_n where each $h' \in H'_n$ maps strings of length $n + \ell(n) + \log |H_n|$ to strings of length $n(1 - 3c) - l + \log |H_n|$ for some constant $c < 1/3$. Then,

$$f'' = \{f''_n(h', h, x) \stackrel{\text{def}}{=} (h', h'(h, h(x)_{1 \dots (d_n(f_n(x))+2)}, 0^{n-(d_n(f_n(x))+2)}, f_n(x))) : \mathcal{H}' \times \mathcal{H} \times \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}\}_{n \in \mathbb{N}}$$

is a family of almost-onto quantum one-way functions, where $h(x)_{1 \dots (d_n(f_n(x))+2)}$ denotes the most significant bits of $h(x)$.

Proof. First, we consider the following construction:

$$f'_n(h, x) = (h, h(x)_{1 \dots (d_n(f_n(x))+2)}, 0^{n-(d_n(f_n(x))+2)}, f_n(x)).$$

From Lemma 5.2 in [13], we have

$$\mathbf{H}_2(f'_n(H_n, U_n)) \geq n - 1 + \log |H_n|.$$

Next, we consider

$$f''_n(h', h, x) = (h', h'(f'_n(h, x)))$$

and let $x' = (h, x)$. Then we can write $f''_n(h', x') = (h', h'(f'_n(x')))$. Here, we use the following standard fact.

Fact. Let D be a distribution over some finite domain such that $\mathbf{H}_2(D) \geq k$. Then every $\varepsilon > 0$ there exists a distribution D' over the same domain such that $\mathbf{H}_\infty(D') \geq k - \log(\varepsilon^{-1})$ and $\delta(D, D') \leq \varepsilon$.

In order to apply the above fact, we set $\varepsilon = 2^{-cn}$. Then, there exists a distribution Y_n over $\{0, 1\}^{n+\ell(n)+\log |H_n|}$ such that $\mathbf{H}_\infty(Y_n) \geq n(1 - c) - 1 + \log |H_n|$ and $\delta(Y_n, f'_n(H_n, U_n)) \leq 2^{-cn}$. By Lemma 1, we have

$$\delta((H'_n, H'_n(Y_n)), (H'_n, U_{n(1-c-2c)-1+\log |H_n|})) < 2^{-cn}.$$

By the triangle inequality, we have

$$\delta((H'_n, H'_n(f'_n(H_n, U_n))), (H'_n, U_{n(1-3c)-1+\log |H_n|})) < 2^{-cn} + 2^{-cn} = 2^{1-cn}.$$

If there exists an inverter for f'' we can construct an inverter for f by a simple reduction argument. $\square$

Corollary 2. A statistically-hiding and computationally-binding quantum bit commitment scheme is constructible from an APS quantum one-way function family.

4 Security Analysis

4.1 Computational Binding

First, we consider the most general adversary $\{\mathcal{D}_{n,0}, \mathcal{U}_n\}_{n \in \mathbb{N}}$ against the binding property of our scheme. Through this subsection, we show Theorem 1, namely, that any such adversary can be used to invert the underlying one-way function. Actually, the proof is almost similar to the proof in [6] except some modification. For the readability, we show the whole proof.

We separate the whole system into three parts: the system H_{commit} that encodes the functional value, the system H_{open} that encodes inputs to the function, and the system H_{keep} is the reminder of the system (thus including H_{keep} for simplicity). Then the states $|\tilde{\psi}_{n,0}\rangle = \mathcal{D}_{n,0}|\mathbf{0}\rangle$ and $|\tilde{\psi}_{n,1}\rangle = \mathcal{U}_n|\tilde{\psi}_{n,0}\rangle$ can be generally written as

$$\begin{aligned} |\tilde{\psi}_{n,0}\rangle &= \sum_{x,y \in \{0,1\}^n} |\alpha_{0,x,y}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |y\rangle_+^{\text{commit}}, \quad \text{and} \\ |\tilde{\psi}_{n,1}\rangle &= \sum_{x,y \in \{0,1\}^n} |\alpha_{1,x,y}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |y\rangle_{\times}^{\text{commit}}, \end{aligned}$$

where $\sum_{x,y} \|\alpha_{0,x,y}\|^2 = \sum_{x,y} \|\alpha_{1,x,y}\|^2 = 1$.

First, we consider the perfect case as a simple case.

Perfect Case. Here, we assume that an adversary $\{\mathcal{D}_{n,0}, \mathcal{U}_n\}_{n \in \mathbb{N}}$ reveals the committed bit in both ways perfectly. This means that $s_0(n) = s_1(n) = 1$. Then we have $\|\alpha_{w,x,y}\|^2 = 0$ if $f_n(x) \neq y$. That is, the states $|\psi_{n,0}\rangle$ and $|\psi_{n,1}\rangle$ can be written as follows.

$$\begin{aligned} |\psi_{n,0}\rangle &= \sum_{x \in \{0,1\}^n} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_+^{\text{commit}} = \mathcal{D}_{n,0}|\mathbf{0}\rangle \quad \text{and} \\ |\psi_{n,1}\rangle &= \sum_{y \in \{0,1\}^n} |\alpha_{1,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_{\times}^{\text{commit}} = \mathcal{U}_n|\psi_{n,0}\rangle, \end{aligned}$$

where $\sum_x \|\alpha_{0,x}\|^2 = \sum_x \|\alpha_{1,x}\|^2 = 1$.

Let $\mathcal{P}_+^{u,\text{commit}}$ and $\mathcal{P}_{\times}^{u,\text{commit}}$ be the projection operators $\mathcal{P}_+^u$ and $\mathcal{P}_{\times}^u$ respectively, acting in H_{commit} . We are interested in properties on the state $|\varphi_{n,0}^u\rangle = \mathcal{P}_{\times}^{u,\text{commit}}|\psi_{n,0}\rangle$ which plays an important role for the inverter.

Now we consider an algorithm to invert y . Thus, we assume that y is encoded as input to the inverter in H_{inv} . Before considering the inverter, we consider properties on the states $|\varphi_{n,0}^u\rangle$ for every $u \in \{0,1\}^{\ell(n)}$:

1. $\|\varphi_{n,0}^u\|^2 = 2^{-\ell(n)/2}$;
2. there exists an efficient circuit $\mathcal{W}_n$ on $H_{\text{inv}} \otimes H_{\text{open}} \otimes H_{\text{commit}}$ which if u is in H_{inv} , unitarily maps $|\psi_{n,0}\rangle$ to $2^{\ell(n)/2}|\varphi_{n,0}^u\rangle$;
3. $\mathcal{U}_n|\varphi_{n,0}^u\rangle = \sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}$.

If the above properties are true, we can consider an inverter as follows. On input y , the inverter generates the state $|\psi_{n,0}\rangle$ by applying $\mathcal{D}_{n,0}$ to $|0\rangle$, then applies $\mathcal{W}_n$ and $\mathcal{U}_n$ in order, and finally measures $\mathbf{H}_{\text{open}}$ to obtain $z \in f_n^{-1}(y)$.

In what follows, we show each property is true. First, we show Property 1. We write $|\psi_{n,0}\rangle$ using the diagonal basis for $\mathbf{H}_{\text{commit}}$, and then we have

$$\begin{aligned} |\psi_{n,0}\rangle &= 2^{-\ell(n)/2} \sum_{u,v \in \{0,1\}^{\ell(n)}} (-1)^{u \odot v} \left(\sum_{z \in f_n^{-1}(v)} |\alpha_{0,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \right) \otimes |u\rangle_{\times}^{\text{commit}} \\ &= 2^{-\ell(n)/2} \sum_{\substack{u \in \{0,1\}^{\ell(n)} \\ v \in \text{range}(f_n)}} (-1)^{u \odot v} \left(\sum_{z \in f_n^{-1}(v)} |\alpha_{0,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \right) \otimes |u\rangle_{\times}^{\text{commit}} \\ &= 2^{-\ell(n)/2} \sum_{\substack{u \in \{0,1\}^{\ell(n)} \\ x \in \{0,1\}^n}} (-1)^{u \odot f_n(x)} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}. \end{aligned}$$

Since

$$|\varphi_{n,0}^u\rangle = 2^{-\ell(n)/2} \sum_{x \in \{0,1\}^n} (-1)^{u \odot f_n(x)} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}},$$

Property 1 holds. Next, we consider Property 3. Since the state $|\psi_{n,1}\rangle$ can be written as

$$|\psi_{n,1}\rangle = \sum_{u \in \text{range}(f_n)} \left(\sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \right) \otimes |u\rangle_{\times}^{\text{commit}},$$

it implies that for every $u \in \text{range}(f_n)$

$$\begin{aligned} \mathcal{U}_n |\varphi_{n,0}^u\rangle &= \mathcal{U}_n \mathcal{P}_{\times}^{u, \text{commit}} |\psi_{n,0}\rangle = \mathcal{P}_{\times}^{u, \text{commit}} \mathcal{U}_n |\psi_{n,0}\rangle \\ &= \mathcal{P}_{\times}^{u, \text{commit}} |\psi_{n,1}\rangle = \sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}. \end{aligned}$$

(Note that $\mathcal{U}_n$ is restricted to act in $\mathbf{H}_{\text{keep}} \otimes \mathbf{H}_{\text{open}}$ and thus $\mathcal{U}_n$ and $\mathcal{P}_{\times}^{u, \text{commit}}$ are commutable.) Thus, Property 3 holds. Finally, we consider Property 2. We describe how to implement $\mathcal{W}_n$ mapping from

$$|u\rangle^{\text{inv}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_{+}^{\text{commit}}$$

into

$$(-1)^{u \odot f_n(x)} |u\rangle^{\text{inv}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}$$

for every $u \in \text{range}(f_n)$ and $x \in \{0,1\}^n$, which satisfies the requirement. First we apply the mapping $|u\rangle^{\text{inv}} \otimes |f_n(x)\rangle^{\text{commit}} \mapsto (-1)^{u \odot f_n(x)} |u\rangle^{\text{inv}} \otimes |f_n(x)\rangle^{\text{commit}}$, which can be efficiently implemented by using the Hadamard gate and the

controlled-NOT gate. Secondly, we apply the mapping $|x\rangle^{\text{open}} \otimes |u\rangle^{\text{commit}} \mapsto |x\rangle^{\text{open}} \otimes |u \oplus f_n(x)\rangle^{\text{commit}}$, which can be implemented by the efficient evaluation circuit of f_n . Thirdly, we apply the mapping $|y\rangle^{\text{inv}} \otimes |u\rangle^{\text{commit}} \mapsto |y\rangle^{\text{inv}} \otimes |y \oplus u\rangle^{\text{commit}}$, which can be efficiently implemented by using the controlled-NOT gate. Finally, we apply the Hadamard gate to the all qubits in $\mathbf{H}_{\text{commit}}$. It is easy to verify that the above procedure satisfies the requirement. Thus, Property 2 holds.

General Case. In general case, we assume that $s_0(n) + s_1(n) \geq 1 + 1/p(n)$ for some polynomial p , where

$$s_0(n) = \sum_{v \in \{0,1\}^n} \|\alpha_{0,v,f_n(v)}\|^2 \quad \text{and} \quad s_1(n) = \sum_{v \in \{0,1\}^n} \|\alpha_{1,v,f_n(v)}\|^2. \quad (1)$$

Now, we consider a transformation $\mathcal{T}_n$ acting in $\mathbf{H}_{\text{open}} \otimes \mathbf{H}_{\text{commit}} \otimes \mathbf{H}_{\text{test}}$. We define $\mathcal{T}_n$ as follows:

$$\mathcal{T}_n : |x\rangle^{\text{open}} \otimes |y\rangle^{\text{commit}} \otimes |a\rangle^{\text{test}} \mapsto |x\rangle^{\text{open}} \otimes |y\rangle^{\text{commit}} \otimes |f_n(x) \oplus y \oplus a\rangle^{\text{test}}.$$

Then we have

$$\begin{aligned} \mathcal{T}_n(|\tilde{\psi}_{n,0}\rangle \otimes |\mathbf{0}\rangle) &= \sum_{f_n(x) \neq z} |\alpha_{0,x,z}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |z\rangle^{\text{commit}} \otimes |f_n(x) \oplus z\rangle^{\text{test}} \\ &\quad + \sum_{x \in \{0,1\}^n} |\alpha_{0,x,f_n(x)}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle^{\text{commit}} \otimes |\mathbf{0}\rangle^{\text{test}}. \end{aligned}$$

Here, we consider the case where the measurement on $\mathbf{H}_{\text{test}}$ gives the outcome $|\mathbf{0}\rangle$. Then, the adversary obtains the quantum residue:

$$|\psi_{n,0}\rangle = \sum_{x \in \{0,1\}^n} |\alpha_{x,0}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle^{\text{commit}}$$

where $|\alpha_{0,x}\rangle^{\text{keep}} = (s_0(n))^{-1/2} |\alpha_{0,x,f_n(x)}\rangle^{\text{keep}}$, with probability

$$s_0(n) = \sum_{v \in \{0,1\}^n} \|\alpha_{0,v,f_n(v)}\|^2 = |\langle \psi_{n,0} | \tilde{\psi}_{n,0} \rangle|^2.$$

It is easy to see that $\mathcal{T}_n$ has an efficient implementation. Now, we can consider an inverter as follows. On input y , the inverter generate the state $|\tilde{\psi}_{n,0}\rangle$ by applying $\mathcal{D}_{n,0}$ to $|\mathbf{0}\rangle$, then applies $\mathcal{T}_n$ and measures $\mathbf{H}_{\text{test}}$. We apply in order $\mathcal{W}_n$ and $\mathcal{U}_n$ to the outcome of the measurement and finally measures $\mathbf{H}_{\text{open}}$ to hopefully obtain $z \in f_n^{-1}(y)$.

We have to estimate the success probability of the inverter. To this end, we define two projections:

$$\begin{aligned} \mathcal{P}_0 &\stackrel{\text{def}}{=} \sum_{x \in \{0,1\}^n} \mathcal{P}^{x,\text{open}} \otimes \mathcal{P}_+^{f_n(x),\text{commit}} \quad \text{and} \\ \mathcal{P}_1 &\stackrel{\text{def}}{=} \sum_{x \in \{0,1\}^n} \mathcal{P}^{x,\text{open}} \otimes \mathcal{P}_\times^{f_n(x),\text{commit}}. \end{aligned}$$

From Eq. (1), we have $s_0(n) = \|\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2$ and $s_1(n) = \|\mathcal{P}_1|\tilde{\psi}_{n,1}\rangle\|^2$. Here, we claim that the success probability p_{inv} satisfies

$$p_{\text{inv}} = \|\mathcal{P}_1\mathcal{U}_n\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2.$$

We will see this claim. As mentioned, after the application of $\mathcal{T}_n$, the state is $|y\rangle^{\text{inv}} \otimes |\psi_{n,0}\rangle$ with probability $\|\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2 = s_0(n)$, where y is the input to the inverter. As we see in the perfect case, $\mathcal{W}_n$ maps the state $|\psi_{n,0}\rangle$ into $2^{\ell(n)/2}|\varphi_{n,0}^y\rangle = 2^{\ell(n)/2}\mathcal{P}_\times^{y,\text{commit}}|\psi_{n,0}\rangle$. After that, we apply $\mathcal{U}_n$ and measure $\mathbf{H}_{\text{open}}$. Thus, the success probability $p_{\text{inv}}(y)$ for input y is written as

$$\begin{aligned} p_{\text{inv}}(y) &= s_0(n)2^{\ell(n)} \left\| \left(\sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \mathcal{P}_\times^{y,\text{commit}} \mathcal{U}_n |\psi_{n,0}\rangle \right\|^2 \\ &= 2^{\ell(n)} \left\| \left(\sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \mathcal{P}_\times^{y,\text{commit}} \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2. \end{aligned}$$

Averaging over all value according to the output distribution of f_n , we have

$$\begin{aligned} p_{\text{inv}} &= \sum_{y \in \text{range}(f_n)} \Pr[y = f_n(U_n)] p_{\text{inv}}(y) \\ &= \sum_{y \in \text{range}(f_n)} \left\| \left(\left(\sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \otimes \mathcal{P}_\times^{y,\text{commit}} \right) \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2 \\ &= \left\| \left(\sum_{y \in \text{range}(f_n)} \left(\left(\sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \otimes \mathcal{P}_\times^{y,\text{commit}} \right) \right) \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2 \\ &= \|\mathcal{P}_1\mathcal{U}_n\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2. \end{aligned}$$

Furthermore, we rewrite the above to easily estimate the value of p_{inv} .

$$\begin{aligned} p_{\text{inv}} &= \|\mathcal{P}_1\mathcal{U}_n\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2 = \|\mathcal{P}_1\mathcal{U}_n(\mathcal{I} - \mathcal{P}_0^\perp)|\tilde{\psi}_{n,0}\rangle\|^2 \\ &= \|\mathcal{P}_1\mathcal{U}_n|\tilde{\psi}_{n,0}\rangle - \mathcal{P}_1\mathcal{U}_n\mathcal{P}_0^\perp|\tilde{\psi}_{n,0}\rangle\|^2 \\ &= \|\mathcal{P}_1|\tilde{\psi}_{n,1}\rangle - \mathcal{P}_1\mathcal{U}_n\mathcal{P}_0^\perp|\tilde{\psi}_{n,0}\rangle\|^2. \end{aligned}$$

Using the triangle inequality and $s_1(n) > 1 - s_0(n)$, we have

$$\begin{aligned} p_{\text{inv}} &\geq \left(\|\mathcal{P}_1|\tilde{\psi}_{n,1}\rangle\| - \|\mathcal{P}_1\mathcal{U}_n\mathcal{P}_0^\perp|\tilde{\psi}_{n,0}\rangle\| \right)^2 \\ &\geq \left(\|\mathcal{P}_1|\tilde{\psi}_{n,1}\rangle\| - \|\mathcal{P}_0^\perp|\tilde{\psi}_{n,0}\rangle\| \right)^2 \\ &= \left(\sqrt{s_1(n)} - \sqrt{1 - s_0(n)} \right)^2. \end{aligned}$$

Let us recall that we assume that $s_0(n) + s_1(n) > 1 + 1/p(n)$ for some polynomial p . After some calculation, we have $p_{\text{inv}} > 1/4(p(n))^2$. This violates the assumption that f is one-way, which completes the proof of Theorem 1. $\square$

4.2 Statistical Hiding

Proof. (of Theorem 2) We can write $\rho_B(0)$ and $\rho_B(1)$ as follows:

$$\begin{aligned}\rho_B(0) &= \sum_{x \in \{0,1\}^n} 2^{-n} |f_n(x)\rangle_+ \langle f_n(x)| \quad \text{and} \\ \rho_B(1) &= \sum_{x \in \{0,1\}^n} 2^{-n} |f_n(x)\rangle_{\times} \langle f_n(x)|.\end{aligned}$$

Let

$$\rho_0 = \sum_{y \in \{0,1\}^{\ell(n)}} 2^{-\ell(n)} |y\rangle_+ \langle y| \quad \text{and} \quad \rho_1 = \sum_{y \in \{0,1\}^{\ell(n)}} 2^{-\ell(n)} |y\rangle_{\times} \langle y|.$$

Then $\rho_0 = \rho_1$ since they are both the identity matrices of the same dimension. Since $\delta(\rho_B(0), \rho_0) < \varepsilon$ and $\delta(\rho_B(1), \rho_1) < \varepsilon$ for some negligible function ε , by the triangle inequality we have $\delta(\rho_B(0), \rho_B(1)) < 2\varepsilon$, which is still negligible. $\square$

5 Concluding Remarks

As we have seen, the most important property for statistically-hiding and computationally-binding non-interactive quantum bit commitment is the “almost-onto” property of quantum one-way functions. Generally speaking, the range of the one-way function is sparse. Thus, if we have a general construction of almost-onto quantum one-way function, then statistically-hiding quantum bit commitment scheme is constructible from any quantum one-way function. As long as we know, the best possible way towards such goal is Rompel’s construction [23] of universal one-way hash functions from any one-way function. Unfortunately, the range is still large. On the other hand, we can consider the following construction: $f'(x, r) = E(f(x), r)$ for one-way function f and the randomness extractor E with random input r . From the definition of the randomness extractor, f' is clearly almost-onto. However, f' sometimes loses the one-wayness, or it is difficult to find some reduction from f' to f .

As alternative approach, techniques in [21] might be available. In turn, we might need some interaction, which makes the security analysis difficult.

Acknowledgment

We would like to thank the reviewers for their comments which help us to improve the presentation.

References

1. Aharonov, D., Ta-Shma, A., Vazirani, U.V., Yao, A.C.-C.: Quantum bit escrow. In: Proc. 32nd ACM Symp. Theory of Computing, pp. 705–714 (2000)
2. Brassard, G., Chaum, D., Crépeau, C.: Minimum disclosure proofs of knowledge. J. Comput. Syst. Sci. 37(2), 156–189 (1988)

3. 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(32), 022316 (2008)
4. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. *J. Comp. Syst. Sci.* 18(2), 143–154 (1979)
5. Crépeau, C., Légaré, F., Salvail, L.: How to convert the flavor of a quantum bit commitment. In: Pfitzmann, B. (ed.) *EUROCRYPT 2001*. LNCS, vol. 2045, pp. 60–77. Springer, Heidelberg (2001)
6. Dumais, P., Mayers, D., Salvail, L.: Perfectly concealing quantum bit commitment from any quantum one-way permutation. In: Preneel, B. (ed.) *EUROCRYPT 2000*. LNCS, vol. 1807, pp. 300–315. Springer, Heidelberg (2000)
7. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM* 38(3), 691–729 (1991)
8. Haitner, I., Horvitz, O., Katz, J., Koo, C.-Y., Morselli, R., Shaltiel, R.: Reducing complexity assumptions for statistically-hiding commitment. *J. Cryptol.* 22(3), 283–310 (2009); Cramer, R. (ed.): *EUROCRYPT 2005*. LNCS, vol. 3494, pp. 58–77. Springer, Heidelberg (2005)
9. Haitner, I., Reingold, O.: A new interactive hashing theorem. In: *Proc. 22nd IEEE Conf. Computational Complexity*, pp. 319–332 (2007)
10. Haitner, I., Reingold, O.: Statistically-hiding commitment from any one-way function. In: *Proc. 39th ACM Symp. Theory of Computing*, pp. 1–10 (2007)
11. Haitner, I., Hoch, J.J., Reingold, O., Segev, G.: Finding collisions in interactive protocols — A tight lower bound on the round complexity of statistically-hiding commitments. In: *Proc. 48th IEEE Symp. Foundations of Computer Sciences*, pp. 669–679 (2007)
12. Hardy, L., Kent, A.: Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.* 92(15), 157901 (2004)
13. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *SIAM J. Comput.* 28(4), 1364–1396 (1999)
14. Kent, A.: Quantum bit string commitment. *Phys. Rev. Lett.* 90(23), 237901 (2003)
15. Koshiba, T., Seri, Y.: Round-efficient one-way permutation based perfectly concealing bit commitment scheme, *Electronic Colloquium on Computational Complexity*, TR06-093 (2006)
16. Lo, H.-K., Chau, H.F.: Is quantum bit commitment really possible? *Phys. Rev. Lett.* 78(17), 3410–3413 (1997)
17. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* 78(17), 3414–3417 (1997)
18. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) *Post-Quantum Cryptography*, pp. 147–191. Springer, Heidelberg (2009)
19. Naor, M.: Bit commitment using pseudorandomness. *J. Cryptol.* 4(2), 151–158 (1991)
20. Naor, M., Ostrovsky, R., Venkatesan, R., Yung, M.: Perfect zero-knowledge arguments for NP using any one-way permutation. *J. Cryptol.* 11(2), 87–108 (1998)
21. Nguyen, M.-H., Ong, S.-J., Vadhan, S.P.: Statistical zero-knowledge arguments for NP from any one-way function. In: *Proc. 47th IEEE Symp. Foundations of Computer Science*, pp. 3–14 (2006)

22. Renner, R.: Security of quantum key distribution, Ph.D. Thesis, ETH Zurich (2005), quant-ph/0512258
23. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: Proc. 22nd ACM Symp. Theory of Computing, pp. 387–394 (1990)
24. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)

On the Security and Degradability of Gaussian Channels

Stefano Pirandola^{1,2}, Samuel L. Braunstein², and Seth Lloyd^{1,3}

¹ Research Laboratory of Electronics, MIT, Cambridge MA 02139, USA

² Department of Computer Science, University of York, York YO10 5DD, UK

³ Department of Mechanical Engineering, MIT, Cambridge MA 02139, USA

Abstract. We consider the notion of canonical attacks, which are the cryptographic analog of the canonical forms of a one-mode Gaussian channel. Using this notion, we explore the connections between the degradability properties of the channel and its security for quantum key distribution. Finally, we also show some relations between canonical attacks and optimal Gaussian cloners.

1 Introduction

Today, quantum cryptography is one of the most promising areas in quantum information science. This is particularly true in the framework of continuous variable (CV) systems [1], which are quantum systems characterized by infinite-dimensional Hilbert spaces. The increasing interest in CV quantum cryptography is mainly due to the practical advantages of quantum key distribution (QKD) using Gaussian states [2,3,4,5,6]. Furthermore, this Gaussian QKD has been also extended to multiple quantum communications [7] and the non-trivial possibility of a quantum direct communication has been also explored [8]. Very recently, a new insight in the theory of quantum channels has been provided by the canonical classification of the one-mode Gaussian channels [9] (see also Refs. [10,11] and the *compact version* of this classification in Ref. [5]). These channels have been proven to be unitarily equivalent to canonical forms of six different classes [9], whose degradability properties have been also studied [11]. Here, we exploit these concepts in the scenario of quantum cryptography. In particular, we consider the notion of canonical attacks as the cryptographic analog of the canonical forms. By adopting the individual version of these canonical attacks, we explore the connections between the degradability properties of the channel and its security for QKD. Then, we also show when (and in what sense) these attacks can be considered equivalent to individual attacks using optimal Gaussian cloners.

2 Quantum Communication Scenario

The simplest continuous variable system is a single bosonic mode, i.e., a quantum system described by a pair of quadrature operators $\hat{\mathbf{x}}^T := (\hat{q}, \hat{p})$ with $[\hat{q}, \hat{p}] = 2i$. In particular, a single-mode bosonic state ρ with Gaussian statistics is called

Gaussian state and it is completely characterized by a 2×2 covariance matrix $\mathbf{V}$ plus a displacement vector $\bar{\mathbf{x}} \in \mathbb{R}^2$. Then, a one-mode Gaussian channel is a completely positive trace-preserving (CPT) map $\mathcal{G}(\mathbf{T}, \mathbf{N}, \mathbf{d})$ transforming an input Gaussian state $\rho_a(\mathbf{V}_a, \bar{\mathbf{x}}_a)$ of a sender (Alice) into an output Gaussian state $\rho_b(\mathbf{V}_b, \bar{\mathbf{x}}_b)$ of a receiver (Bob) via the relations $\mathbf{V}_b = \mathbf{T}\mathbf{V}_a\mathbf{T}^T + \mathbf{N}$ and $\bar{\mathbf{x}}_b = \mathbf{T}\bar{\mathbf{x}}_a + \mathbf{d}$. Here, $\mathbf{d} \in \mathbb{R}^2$ and $\mathbf{T}, \mathbf{N}$ are 2×2 real matrices, with $\mathbf{N}^T = \mathbf{N} > 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2$. Up to unitaries on the input and the output, every one-mode Gaussian channel is equivalent to a map $\mathcal{C}$, called the *canonical form*, which is a Gaussian channel with $\mathbf{d} = \mathbf{0}$ and $\mathbf{T}_c, \mathbf{N}_c$ diagonal [9]. According to Ref. [5], the explicit expressions of $\mathbf{T}_c$ and $\mathbf{N}_c$ depend on three symplectic invariants of the channel: the generalized *transmission* $\tau := \det \mathbf{T}$ (ranging from $-\infty$ to $+\infty$), the *rank* $r := [\text{rk}(\mathbf{T})\text{rk}(\mathbf{N})]/2$ (with possible values $r = 0, 1, 2$) and the *temperature* $\bar{n}$ (which is a positive number related to $\det \mathbf{N}$ [5]). These three invariants $\{\tau, r, \bar{n}\}$ completely characterize the two matrices $\mathbf{T}_c, \mathbf{N}_c$ and, therefore, the corresponding canonical form $\mathcal{C} = \mathcal{C}(\tau, r, \bar{n})$. In particular, the first two invariants $\{\tau, r\}$ determine the class of the form [5,9]. The full classification is explicitly shown in the following table

τ	r	Class	Form	$\mathbf{T}_c$	$\mathbf{N}_c$
0	0	A_1	$\mathcal{C}(0, 0, \bar{n})$	$\mathbf{0}$	$(2\bar{n} + 1)\mathbf{I}$
0	1	A_2	$\mathcal{C}(0, 1, \bar{n})$	$\frac{\mathbf{I} + \mathbf{Z}}{2}$	$(2\bar{n} + 1)\mathbf{I}$
1	1	B_1	$\mathcal{C}(1, 1, 0)$	$\mathbf{I}$	$\frac{\mathbf{I} - \mathbf{Z}}{2}$
1	2	B_2	$\mathcal{C}(1, 2, \bar{n})$	$\mathbf{I}$	$\bar{n}\mathbf{I}$
1	0	$B_2(\text{Id})$	$\mathcal{C}(1, 0, 0)$	$\mathbf{I}$	$\mathbf{0}$
(0, 1)	2	$C(\text{Att})$	$\mathcal{C}(\tau, 2, \bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(1 - \tau)(2\bar{n} + 1)\mathbf{I}$
> 1	2	$C(\text{Amp})$	$\mathcal{C}(\tau, 2, \bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(\tau - 1)(2\bar{n} + 1)\mathbf{I}$
< 0	2	D	$\mathcal{C}(\tau, 2, \bar{n})$	$\sqrt{-\tau}\mathbf{Z}$	$(1 - \tau)(2\bar{n} + 1)\mathbf{I}$

In this table, the values of $\{\tau, r\}$ in the first two columns specify a particular class A_1, A_2, B_1, B_2, C and D [12]. Within each class, the possible canonical forms are expressed in the third column, where also the third invariant $\bar{n}$ must be considered. The corresponding expressions of $\mathbf{T}_c, \mathbf{N}_c$ are shown in the last two columns, where $\mathbf{Z} := \text{diag}(1, -1)$, $\mathbf{I} := \text{diag}(1, 1)$ and $\mathbf{0}$ is the zero matrix.

By adopting a Stinespring dilation of the quantum channel, we can describe a canonical form $\mathcal{C}(\tau, r, \bar{n})$ via a symplectic transformation $\mathbf{M}_{ae\tilde{e}}$ mixing the input signal mode $\{a\}$ with two vacuum environmental modes $\{e, \tilde{e}\}$ and yielding the output modes $\{b\}$ for Bob and $\{c, \tilde{c}\}$ for the environment [see Fig. 1(i)]. Such a dilation is known to be unique up to partial isometries. For class B_2 , also known as an *additive-noise channel*, the Stinespring dilation corresponds to an optimal Gaussian cloner (OGC) which clones asymmetrically in the clones but symmetrically in the quadratures [13]. Such a machine transforms the input mode $\{a\}$ and the two vacuum modes $\{e, \tilde{e}\}$ into a pair of clone modes $\{b, c\}$ and an anticlon mode $\{\tilde{c}\}$. In particular the reduced state of the output clone $k = b, c$ is given by the modulated state

$$\rho_k = \int d^2\gamma G_{\chi_k}(\gamma) \hat{D}(\gamma) \rho_a \hat{D}^\dagger(\gamma), \quad G_{\chi_k}(\gamma) := \frac{1}{\pi\chi_k} \exp\left(-\frac{|\gamma|^2}{\chi_k}\right), \quad (1)$$

where $\hat{D}(\gamma)$ is the displacement operator and χ_k is the cloning noise variance satisfying $\chi_b\chi_c = 1$ with $\chi_b = \bar{n}$.

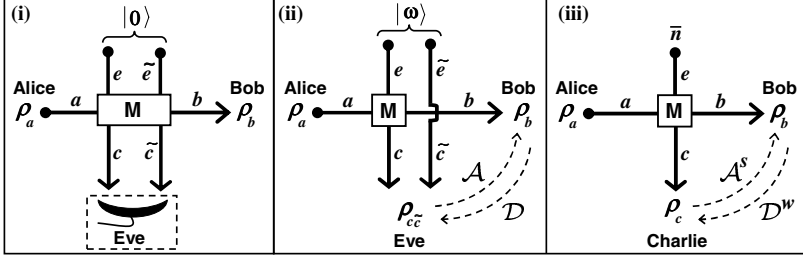


Fig. 1. Inset (i): Stinespring dilation of a canonical form. It describes a canonical attack by including the optimal coherent detection of all the outputs $\{c, \tilde{c}\}$ collected in all the uses of the channel. Both the dilation and the attack are unique up to isometries acting on the environmental modes $\{c, \tilde{c}\}$. Inset (ii): Stinespring dilation of a canonical form of every class but B_2 ; the form is antidegradable (degradable) if there exists a map $\mathcal{A}$ ($\mathcal{D}$) such that $\rho_b = \mathcal{A}(\rho_{c\tilde{c}})$ [$\rho_{c\tilde{c}} = \mathcal{D}(\rho_b)$]. Inset (iii): Physical representation of a canonical form of every class but B_2 ; the form is strongly antidegradable (weakly degradable) if there exists a map $\mathcal{A}^s$ ($\mathcal{D}^w$) such that $\rho_b = \mathcal{A}^s(\rho_c)$ [$\rho_c = \mathcal{D}^w(\rho_b)$].

It is important to notice that class B_2 is the unique class where the Stinespring dilation cannot be simplified to a single-mode description [9]. For all the other classes, in fact, we can consider a dilation where the symplectic transformation $\mathbf{M}_{ae\tilde{e}}$ can be decomposed as $\mathbf{M}_{ae} \oplus \mathbf{I}_{\tilde{e}}$, involving the signal mode $\{a\}$ and *only one* mode $\{e\}$ of the two-mode environment $\{e, \tilde{e}\}$ [see Fig. 1(ii)]. This is possible if the environment is prepared in a two-mode squeezed vacuum (TMSV) state $|\omega\rangle_{e\tilde{e}}$, i.e., in a pure Gaussian state with correlation matrix

$$\mathbf{V}_{e\tilde{e}}(\omega) = \begin{pmatrix} \omega \mathbf{I} & \sqrt{\omega^2 - 1} \mathbf{Z} \\ \sqrt{\omega^2 - 1} \mathbf{Z} & \omega \mathbf{I} \end{pmatrix}, \quad \omega := 2\bar{n} + 1 \geq 1. \quad (2)$$

Such a dilation $\{\mathbf{M}_{ae} \oplus \mathbf{I}_{\tilde{e}}, |\omega\rangle\}$ is the purification of a single-mode *physical representation* [14] $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$, where $\mathbf{M}_{ae}$ mixes the signal mode $\{a\}$ with a single environmental mode $\{e\}$, prepared in a thermal state $\rho_e(\bar{n})$ with $\bar{n}$ average photons [11]. This physical representation can also be seen as a quantum broadcast channel where the symplectic $\mathbf{M}_{ae}$ relates the output quadratures $\hat{\mathbf{x}}_{out}^T = (\hat{q}_b, \hat{p}_b, \hat{q}_c, \hat{p}_c)$ of two receivers (Bob and Charlie) to the input quadratures $\hat{\mathbf{x}}_{in}^T = (\hat{q}_a, \hat{p}_a, \hat{q}_e, \hat{p}_e)$ of a sender (Alice) and a thermal environment [see Fig. 1(iii)].

An important property of all the canonical forms (except B_2 [15]) is their *degradability* or *antidegradability* [11,16]. A canonical form is called *strongly antidegradable* if it has a single-mode physical representation $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$ where Charlie can reconstruct Bob's state ρ_b via some CPT map $\mathcal{A}^s$, i.e., $\rho_b = \mathcal{A}^s(\rho_c)$. Notice that the strong antidegradability $\{a\} \rightarrow \{c\} \rightarrow \{b\}$ is a sufficient but not necessary condition for the (standard) antidegradability $\{a\} \rightarrow \{c, \bar{c}\} \rightarrow \{b\}$, where Bob's state is reconstructed by considering all the degrees of freedom of the environment (Eve). In fact, the form is called *antidegradable* if there exists a CPT map $\mathcal{A}$ such that $\rho_b = \mathcal{A}(\rho_{c\bar{c}})$. In the same way, one can consider the *weak degradability* $\{a\} \rightarrow \{b\} \rightarrow \{c\}$ which is implied by the (standard) degradability $\{a\} \rightarrow \{b\} \rightarrow \{c, \bar{c}\}$. In fact, degradability corresponds to the existence of a map $\mathcal{D}$ such that $\rho_{c\bar{c}} = \mathcal{D}(\rho_b)$, while weak degradability corresponds to the existence of a map $\mathcal{D}^w$ such that $\rho_c = \mathcal{D}^w(\rho_b)$ for some physical representation. Clearly the weak/strong notions coincide with the standard ones when $\bar{n} = 1$.

From the point of view of practical quantum cryptography, classes C and D are the most important ones. These classes are full-rank ($r = 2$) and represent the unique classes where the invariant τ can take a continuum of values, except for the singular points $\tau = 0$ and $\tau = 1$. Because of this continuity, we call the canonical forms $\mathcal{C}(\tau, 2, \bar{n})$ of classes C and D as *regular*. For these forms, one can consider a single-mode physical representation $\{\mathbf{M}_{ae}, \rho(\bar{n})\}$ with symplectic matrix

$$\mathbf{M}_{ae}(\tau) = \begin{pmatrix} \sqrt{|\tau|} & 0 & \sqrt{|1-\tau|} & 0 \\ 0 & s(\tau)\sqrt{|\tau|} & 0 & s(1-\tau)\sqrt{|1-\tau|} \\ s(\tau-1)\sqrt{|1-\tau|} & 0 & s(\tau)\sqrt{|\tau|} & 0 \\ 0 & -\sqrt{|1-\tau|} & 0 & \sqrt{|\tau|} \end{pmatrix}, \quad (3)$$

where $s(\cdots)$ is the sign function. Notice that Eq. (3) corresponds to a beam splitter for $0 < \tau < 1$ and to an amplifier for $\tau > 1$. A regular canonical form $\mathcal{C}(\tau, 2, \bar{n})$ is strongly antidegradable (weakly degradable) if and only if $\tau \leq 1/2$ ($\tau \geq 1/2$) [11].

3 Quantum Cryptography Scenario

In the standard scenario of quantum cryptography, the environment is completely under control of a malicious eavesdropper (Eve). Here, a one-mode channel can be generally seen as the effect of a collective attack, where Eve probes the signals using individual interactions and then performs a coherent detection of all the outputs collected in all the uses of the channel. According to Ref. [5], one can define as a “canonical attack” a collective attack that generates a one-mode Gaussian channel in canonical form. This is actually a particular form of the most general collective Gaussian attack that is completely characterized in Ref. [5]. Up to partial isometries, a canonical attack is described by combining the two-mode Stinespring dilation $\{\mathbf{M}_{ae\bar{e}}, |0\rangle\}$ of the canonical form with the optimal coherent detection of all the environmental outputs, which are collected in all the uses of the channel [see Fig. 1(i) including Eve]. In the special case

of the class B_2 , the corresponding B_2 canonical attacks are OGC attacks where both the clone and anticlone are used in the final coherent measurement. In all the other cases, the canonical attacks can be simplified according to Fig. 1(ii) where Eve uses a single-mode symplectic interaction $\mathbf{M}_{ae}$ and the TMSV state specified by Eq. (2). In particular, the *regular canonical attacks* are the ones with $\mathbf{M}_{ae}(\tau)$ given in Eq. (3). These attacks can be associated to a pair $\{\tau, \omega\}$ with $\tau \neq 0, 1$.

In this paper, we consider the individual version of the regular canonical attacks (denoted by $\{\tau, \omega\}_{ind}$), where Eve is restricted to incoherent detections of her outputs (and no isometry is applied). By adopting this kind of attack, we derive the security thresholds of the coherent state protocol of Ref. [3]. In this protocol, Alice prepares a coherent state $\rho_a := |\alpha\rangle\langle\alpha|$ whose amplitude α is Gaussianly modulated with variance μ . Then, Alice sends the state through the channel, whose output is homodyned by Bob. In particular, Bob randomly switches between the detection of $\hat{q}_b$ and $\hat{p}_b$, the effective sequence being classically communicated at the end of the protocol (basis revelation). Here, the optimal attack $\{\tau, \omega\}_{ind}$ is a direct generalization of the delayed-choice entangling cloner attack of Ref. [3,17] (retrieved in the particular case $0 < \tau < 1$). This means that Eve stores all her outputs in a quantum memory, awaits the basis revelation and, then, performs the correct sequence of $\hat{q}$ and $\hat{p}$ detections on her outputs. This is equivalent to saying that, for each run of the protocol where Bob chooses the $\hat{q}$ quadrature, Eve also detects the $\hat{q}$ quadrature on her modes $\{c, \tilde{c}\}$. In particular, we can assume as first detection one of $\hat{q}_{\tilde{c}}$, which is equivalent to the remote preparation of a $\hat{q}$ -squeezed state on the input mode $\{e\}$ with variance $\langle \hat{q}_e^2 \rangle = \omega^{-1}$ [17]. As a consequence, Eve is always able to control the input environment $\{e\}$ in such a way as to enhance her detection of the output mode $\{c\}$ in the same quadrature which is effectively chosen by Bob.

By adopting this optimal attack, let us explicitly derive the security thresholds of the coherent state protocol in the limit of high modulation $\mu \rightarrow +\infty$. From Eqs. (2) and (3), we derive the following variance and conditional variance for Bob's output

$$V_B(\mu) = \langle \hat{q}_b^2 \rangle = \langle \hat{p}_b^2 \rangle = |\tau|(\mu + 1) + |1 - \tau|\omega, \quad V_{B|A} = V_B(\mu = 0). \quad (4)$$

Then, we have the following signal-to-noise formula for the classical mutual information

$$I_{AB} := \frac{1}{2} \log \frac{V_B}{V_{B|A}} \xrightarrow{\mu \gg 1} \frac{1}{2} \log \frac{\mu}{\eta(\omega, \tau)}, \quad (5)$$

where the total noise $\eta(\omega, \tau) := \Delta + \chi(\omega, \tau)$ is given by the sum of the quantum shot-noise $\Delta = 1$ and the *equivalent noise* of the channel

$$\chi(\omega, \tau) = \left| \frac{1 - \tau}{\tau} \right| \omega. \quad (6)$$

From the point of view of the classical mutual information of Eq. (5), the regular canonical form $\mathcal{C}(\tau, 2, \bar{n})$ is equivalent to a form $\mathcal{C}(1, 2, \bar{n})$ of the class B_2

(additive-noise channel), where the input classical signal α with Gaussian modulation μ is subject to the additive Gaussian noises χ and Δ (coming from the channel and the measurement, respectively). In fact, in such a case, we would have

$$V_B = \mu + \Delta + \chi, \quad V_{B|A} = \Delta + \chi, \quad (7)$$

which leads exactly to Eq. (5) for $\mu \rightarrow +\infty$. In order to analyze the security thresholds, it is useful to introduce the so-called *excess noise*

$$\varepsilon := \eta(\omega, \tau) - \eta(1, \tau) = \left| \frac{1 - \tau}{\tau} \right| (\omega - 1) \quad (8)$$

so that

$$\chi(\varepsilon, \tau) = \left| \frac{1 - \tau}{\tau} \right| + \varepsilon, \quad (9)$$

i.e., the equivalent noise can be decomposed in pure- τ noise and excess noise $\varepsilon \geq 0$. Roughly speaking, ε quantifies the effect of the input thermal noise (ω) in the equivalent additive description of the quantum channel, which is specified by Eq. (7).

In order to derive the security thresholds, let us compute the mutual information I_{AE} (between Alice and Eve) and I_{BE} (between Bob and Eve). It is easy to check that

$$V_E(\mu) = \langle \hat{q}_c^2 \rangle = \langle \hat{p}_c^2 \rangle = |1 - \tau| (\mu + 1) + |\tau| \omega^{-1}, \quad (10)$$

$$V_{E|A} = |1 - \tau| + |\tau| \omega^{-1}, \quad V_{B|E} = [|\tau| (\mu + 1)^{-1} + |1 - \tau| \omega]^{-1}, \quad (11)$$

and, therefore,

$$I_{AE} := \frac{1}{2} \log \frac{V_E}{V_{E|A}} \xrightarrow{\mu \gg 1} \frac{1}{2} \log \frac{\mu}{1 + \chi^{-1}}, \quad I_{BE} := \frac{1}{2} \log \frac{V_B}{V_{B|E}} \xrightarrow{\mu \gg 1} \frac{1}{2} \log \tau^2 \chi \mu. \quad (12)$$

Then, we can compute the secret-key rates in direct reconciliation (DR, $\blacktriangleright$) and reverse reconciliation (RR, $\blacktriangleleft$), i.e.,

$$R^{\blacktriangleright} := I_{AB} - I_{AE} \rightarrow \frac{1}{2} \log \frac{1 + \chi^{-1}}{1 + \chi}, \quad R^{\blacktriangleleft} := I_{AB} - I_{BE} \rightarrow \frac{1}{2} \log \frac{1}{\tau^2 \chi (1 + \chi)}. \quad (13)$$

From $R^{\blacktriangleright} = 0$ we derive the security threshold $\chi(\varepsilon, \tau) = 1$ or, equivalently, the curve $\varepsilon^{\blacktriangleright} = \varepsilon^{\blacktriangleright}(\tau)$ shown in Fig. 2. From such a figure we clearly see how strong antidegradability (holding for $\tau \leq 1/2$) is a sufficient condition for the insecurity of the channel in DR (since $\varepsilon^{\blacktriangleright} = 0$ for every $\tau \leq 1/2$). However, it is not a necessary condition as shown by the existence of the insecure regions for $\tau \geq 1/2$ and $\varepsilon > \varepsilon^{\blacktriangleright}(\tau)$ (where the channel is insecure but weakly degradable). This is a consequence of the fact that Eve is much more powerful than Charlie, thanks to her active control of the input environment. In fact, even if no strong antidegradability can be found in the range $\tau \geq 1/2$, the channel can be still antidegradable, e.g., within the insecure regions for $\tau \geq 1/2$ and $\varepsilon > \varepsilon^{\blacktriangleright}(\tau)$.

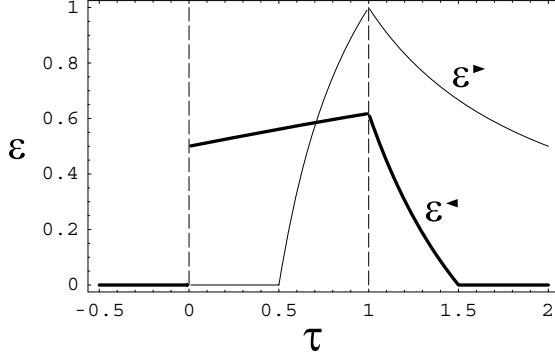


Fig. 2. Security thresholds in DR (thin curve) and RR (thick curve) in the presence of an individual and regular canonical attack $\{\tau, \omega\}_{ind}$ (where $\tau \neq 0, 1$). Such thresholds are expressed in terms of maximum-tolerable excess noise ε versus τ . For a given τ , only the positive ε 's below the curves are secure.

We recover a full equivalence between strong antidegradability and insecurity only in the case $\varepsilon = 0$, where the channel does not introduce thermal noise. In such a case, in fact, the strong antidegradability coincides with the standard antidegradability and the security threshold ($\tau = 1/2$) corresponds exactly to the threshold between antidegradability and degradability.

The fact that the strong antidegradability is a sufficient condition for the insecurity in DR is quite obvious. In fact, it implies the antidegradability, where Eve can reconstruct Bob's state and, therefore, retrieve at least the same information of Bob in decoding Alice's signals (i.e., $\exists \mathcal{A}^s \Rightarrow \exists \mathcal{A} \Rightarrow I_{AE} \geq I_{AB}$). However, the situation is completely different in RR, where Alice and Eve try to guess Bob's outcomes. In such a case, even if the channel is strongly antidegradable, Bob's outcomes can be much more correlated to Alice's variables than Eve's ones. In general, the only way for Eve to beat Alice in RR consists in introducing an environment which is squeezed enough to make her correlations prevail. From $R^\blacktriangleleft = 0$ we derive the discontinuous [18] security threshold

$$\varepsilon^\blacktriangleleft = \varepsilon^\blacktriangleleft(\tau) := \frac{\sqrt{4 + \tau^2} - |\tau| - 2|1 - \tau|}{2|\tau|}, \quad (14)$$

shown in Fig. 2. From Fig. 2 it is clear that, even if the channel is strongly antidegradable, QKD can be secure. This is due to the existence of the secure region for $0 < \tau \leq 1/2$ and $\varepsilon < \varepsilon^\blacktriangleleft(\tau)$. Notice that for $\tau > 1$, i.e., for an amplifying channel, reverse reconciliation is outperformed by direct reconciliation. This is in accordance with the previous results of Ref. [19].

According to the expression of I_{AE} in Eq. (12), the Alice-Eve channel can also be described by an additive-noise channel where the input classical signal α (with variance μ) is modulated by an equivalent channel's noise χ^{-1} and a homodyne

detection noise $\Delta = 1$. In fact, we retrieve the same mutual information I_{AE} of Eq. (12) by considering

$$V_E = \mu + \Delta + \chi^{-1}, \quad V_{E|A} = \Delta + \chi^{-1}, \quad (15)$$

and taking the asymptotic limit for $\mu \rightarrow +\infty$. By considering both the Alice-Bob and Alice-Eve channels, one easily checks that the optimal $\{\tau, \omega\}_{ind}$ has therefore an equivalent additive description when direct reconciliation and high modulation are considered. Such an additive description corresponds to an individual OGC attack where Eve clones the input signals with cloning variances $\chi_b = \chi$ and $\chi_c = \chi^{-1}$, stores her clones in a quantum memory and, then, makes the correct homodyne detections after the basis revelation [20]. Such an individual attack is optimal since the saturation of the uncertainty principle $\chi_b \chi_c = 1$ minimizes the information-disturbance trade-off, which can be expressed by the product of the output conditional variances

$$V_{B|A} V_{E|A} = (\Delta + \chi)(\Delta + \chi^{-1}). \quad (16)$$

In direct reconciliation and high modulation, an individual OGC attack with noise χ represents therefore an equivalent additive description of the optimal attack $\{\tau, \omega\}_{ind}$ via Eq. (6). To be precise, there is a whole class of optimal attacks $\{\tau, \omega\}_{ind}$, with different τ and ω but the same $\chi = \chi(\omega, \tau)$, which are equivalent to an individual OGC attack. Notice that this equivalence is true for the “switching” protocol of Ref. [3], but not for the “non-switching” protocol of Ref. [4].

4 Conclusion

In this paper, we have investigated recent notions and properties of the one-mode Gaussian channels in the scenario of quantum cryptography. In particular, we have considered the canonical attacks, which are the cryptographic analog of the canonical forms. We have adopted the individual version of these attacks in order to study the connections between the degradability properties of a Gaussian channel and its security for QKD. We have also explicitly clarified the connections between the various notions of degradability and antidegradability. Finally, we have shown some connections between individual canonical attacks and optimal Gaussian cloners.

Acknowledgments

S.P. was supported by a Marie Curie Fellowship of the European Community. S.L. was supported by the W.M. Keck foundation center for extreme quantum information theory (xQIT).

References

1. Braunstein, S.L., van Loock, P.: Rev. Mod. Phys. 77, 513 (2005)
2. Hillery, M.: Phys. Rev. A. 61, 022309 (2000); Ralph, T.C.: Phys. Rev. A 61, 010303(R) (2000)
3. Grosshans, F., Grangier, P.: Phys. Rev. Lett. 88, 057902 (2002); Grosshans, F., et al.: Nature 421, 238 (2003)
4. Weedbrook, C., et al.: Phys. Rev. Lett. 93, 170504 (2004); Lance, A.M., et al.: Phys. Rev. Lett. 95, 180503 (2005)
5. Pirandola, S., Braunstein, S.L., Lloyd, S.: Phys. Rev. Lett. 101, 200504 (2008)
6. Pirandola, S., Garcia-Patron, R., Braunstein, S.L., Lloyd, S.: Phys. Rev. Lett. 102, 050503 (2009)
7. Pirandola, S., Mancini, S., Lloyd, S., Braunstein, S.L.: Nature Physics 4, 726 (2008)
8. Pirandola, S., et al.: Europhys. Lett. 84, 20013 (2008); arXiv:0903.0750
9. Holevo, A.S.: Probl. Inform. Transm. 43, 1 (2007)
10. Serafini, A., et al.: Phys. Rev. A 71, 012320 (2005)
11. Caruso, F., et al.: New Journal of Physics 8, 310 (2006); Caruso, F., Giovannetti, V.: Phys. Rev. A 74, 062307 (2006)
12. In particular, class C describes an attenuator for $0 < \tau < 1$ and an amplifier for $\tau > 1$. Class B_2 includes the ideal channel for $r = 0$
13. Cerf, N.J., et al.: Phys. Rev. Lett. 85, 1754 (2000)
14. A physical representation is a unitary dilation of the quantum channel where the environmental state ρ_E can be (generally) mixed [11] (see also Ref. [21]). It is *not unique* up to partial isometries, except when it coincides with a Stinespring dilation (i.e., ρ_E is pure)
15. The class B_2 is the unique class which is neither anti-degradable nor degradable [9]
16. Devetak, I., Shor, P.W.: Commun. Math. Phys. 256, 287 (2005)
17. Grosshans, F., et al.: Quant. Inf. and Comp. 3, 535 (2003)
18. In Fig. 2 the discontinuity of $\varepsilon^\blacktriangleleft = \varepsilon^\blacktriangleleft(\tau)$ at $\tau = 0$ is due to the limit $\mu \rightarrow +\infty$, taken for every finite and non-zero τ . For every *finite* μ , the curve converges to zero in a continuous way
19. Filip, R.: Phys. Rev. A 77, 032347 (2008)
20. Notice that, in order to be optimal in DR, the individual OGC attack ignores the measurement of the anticlone. It is not known if such a further measurement can be useful in the eavesdropping of the protocol in RR
21. Holevo, A.S.: Probl. Inform. Transm. Inform. 8, 63 (1972); Lindblad, G.: Commun. Math. Phys. 48, 116 (1976)

Universal Quantum Computation with a Non-Abelian Topological Memory

James R. Wootton, Ville Lahtinen, and Jiannis K. Pachos

School of Physics and Astronomy, University of Leeds,
Woodhouse Lane, Leeds LS2 9JT, UK

Abstract. An explicit lattice realization of a non-Abelian topological memory is presented. The correspondence between logical and physical states is seen directly by use of the stabilizer formalism. The resilience of the encoded states against errors is studied and compared to that of other memories. A set of non-topological operations are proposed to manipulate the encoded states, resulting in universal quantum computation. This work provides insight into the non-local encoding non-Abelian anyons provide at the microscopical level, with an operational characterization of the memories they provide.

1 Introduction

Anyons are quasiparticles with topological, and therefore non-local, properties [1,2], that may be realized on two-dimensional systems [3,4,5,6,7,8,9]. There has been a number anyon-based proposals for the storage and manipulation of quantum information. Many of these proposals deal with so-called Abelian anyons, encoding quantum information in quasiparticle occupancies [10,11,12] or ground state degeneracies [15]. Others utilize cluster state quantum computation [16]. In all cases one obtains a topologically protected quantum memory, but this protection does not extend to the processing of the stored information.

Non-Abelian anyon models possess quasiparticles with more complex behaviour than their Abelian counterparts [17]. Specifically, local measurements on two such quasiparticles cannot determine how they will behave if brought together as composite object. This non-local degree of freedom, known as the fusion channel of the two anyons, is ideal to encode quantum information, protecting against local errors as long as the nature of the anyons is not affected. The energy gap associated with the anyons ensures that there is a threshold error rate before this may occur. Furthermore, processing the information contained in non-Abelian anyons is possible while remaining within the energy gap, and so has the same advantages as adiabatic quantum computation [18].

Computational schemes with non-Abelian anyons are usually presented at an abstract level [13,14], while those using Abelian anyons are often more explicit [15,16]. This means that, though non-Abelian schemes provide the most promising proposals for fault-tolerant quantum computation, it is Abelian schemes that are better understood in terms of their underlying systems. Here we propose a

quantum memory using non-Abelian anyons of the $D(S_3)$ model, expressed explicitly in terms of the underlying spin lattice. This provides an opportunity to perform in-depth studies of the non-Abelian storage. Universal quantum computation is possible when the full $D(S_3)$ model is used [19,20], but we restrict ourselves to a non-universal sub-model. This is because the memory is our primary concern, which can be more thoroughly studied when less anyon types are considered. It also gives us an opportunity to consider how to achieve universality by non-topological operations [16,21,13,12], and to see how they these work in terms of the underlying spins.

1.1 The $D(S_3)$ Anyon Model

Stabilizer codes, strictly defined, are based on lattices of two level spins and the corresponding Pauli group of operators [22]. The quantum double models of anyons, proposed by Kitaev [17], use a generalization of this concept. Spins of higher dimensions are employed, with operators based upon group structures. Abelian groups give rise to Abelian anyons, while non-Abelian groups lead to non-Abelian anyons. Here we consider the simplest non-Abelian model, $D(S_3)$, whose explicit lattice realization was outlined in [20]. This provides the tools with which we build our computational scheme. The relevant aspects of the model are summarized below.

The $D(S_3)$ anyon model is defined on an oriented two-dimensional square lattice. On each edge there resides a six-level spin spanned by the states $|g\rangle$, where g is an element of S_3 , the permutation group of three objects. We express every element in terms of generators t and c , which satisfy $t^2 = c^3 = e$ and $tc = c^2t$. e denotes the trivial element. Using this notation the six elements are given by $S_3 = \{e, c, c^2, t, tc, tc^2\}$.

Define a vertex operator acting on vertex v by,

$$T_g(v) = R_g(e_1)R_g(e_2)L_{g^{-1}}(e_3)L_{g^{-1}}(e_4), \quad [T_g(v), T_h(v')] = 0, \quad (1)$$

where the e_i are the four edges connected to vertex v (see Fig. 1). Here $R_g(e)$ and $L_g(e)$ denote the right and left multiplication, respectively, of the local spin state on edge e by the element g . To be precise, they act as $R_g|h\rangle = |hg\rangle$ and

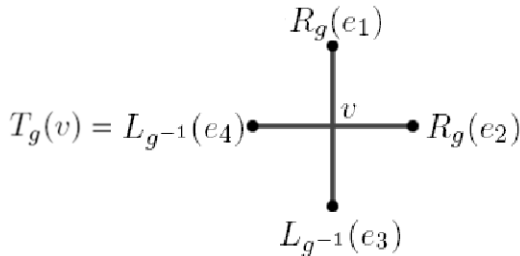


Fig. 1. A pictorial representation of the vertex operators $T_g(v)$

$L_g |h\rangle = |gh\rangle$. For the purposes of our topological memory, we consider only the so-called charge anyons associated with the vertices of the lattice. There are two non-trivial charges, which we call Λ and Φ , and the trivial vacuum charge, 1. When $|\Psi\rangle$ denotes a general state of the system, the presence of a charge of type A at vertex v is defined by $P_A |\Psi\rangle = |\Psi\rangle$, where the orthogonal projectors are given by,

$$\begin{aligned} P_1(v) &= \frac{1}{6}[T_e(v) + T_c(v) + T_{c^2}(v) + T_t(v) + T_{tc}(v) + T_{tc^2}(v)], \\ P_\Lambda(v) &= \frac{1}{6}[T_e(v) + T_c(v) + T_{c^2}(v) - T_t(v) - T_{tc}(v) - T_{tc^2}(v)], \\ P_\Phi(v) &= \frac{1}{3}[2T_e(v) - T_c(v) - T_{c^2}(v)]. \end{aligned}$$

Projectors are also defined for the states of flux anyons on plaquettes, but we need not give them here.

The stabilizer space consists of states with no anyons, i.e. those for which $P_1(v) |gs\rangle = |gs\rangle$ for all v , and a similar condition for the fluxes on plaquettes. The syndrome measurement is defined as a measurement of anyon occupancies, and so corresponds to the above projectors. A Hamiltonian may be defined to maintain the stabilizer space. This assigns energy to the states of the anyons, and thus suppresses their spontaneous creation. This may be expressed,

$$H = - \sum_v P_1(v) - \sum_p P_1(p). \quad (2)$$

Charge anyons are created from the stabilizer space by acting with the following operators on single spins,

$$W_\Lambda(e) = |e\rangle \langle e| + |c\rangle \langle c| + |c^2\rangle \langle c^2| - |t\rangle \langle t| - |tc\rangle \langle tc| - |tc^2\rangle \langle tc^2|, \quad (3)$$

$$W_\Phi(e) = 2|e\rangle \langle e| - |c\rangle \langle c| - |c^2\rangle \langle c^2|. \quad (4)$$

These create charges on the two vertices connected by the edge e . A protocol to create and move charges several edges apart is given in [20].

When charges of different type are brought to the same vertex, the possible outcomes are given by the fusion rules,

$$\Lambda \times \Lambda = 1, \quad \Lambda \times \Phi = \Phi, \quad \Phi \times \Phi = 1 + \Lambda + \Phi. \quad (5)$$

The last implies that the Φ charges have three possible fusion channels; a pair may fuse to the trivial charge 1, a Λ or a Φ . We may utilize the encoding of topological quantum computation [2], associating each possible outcome with a quantum state and hence using them to store quantum information. This information will be topologically protected due to the finite energy gap and the non-local encoding. However, the charges have trivial mutual statistics meaning that information processing by purely topological means is not possible. To

achieve universal quantum computation, we propose non-topological operations to harness the power of the underlying spin lattice. As stated in [13], abstract treatments of such quantum gates tend to be speculative. However, we have the means to study these gates explicitly in terms of spin operations.

2 The Computation with Λ Charges Alone

Though we are using a stabilizer code, the encoding described above is not within the stabilizer space. This allows similar protection from errors, yet easier manipulation. The basic principles of our scheme for universal quantum computation are first presented using the Λ charges alone. Topological protection is introduced later by encoding the Λ charges within the fusion channels of Φ 's, making the logical states indistinguishable by the stabilizer.

Consider two neighbouring vertices, v_1 and v_2 , connected by the edge, e_a (see Fig. 2(a)). The two vertices may be used to store a logical qubit a by identifying trivial charge or a pair of Λ charges at both v_1 and v_2 with the logical qubit states $|0\rangle_a$ and $|1\rangle_a$, respectively. Explicitly,

$$\begin{aligned} |0\rangle_a &= |\text{gs}\rangle, \\ |1\rangle_a &= W_\Lambda(e_a) |\text{gs}\rangle. \end{aligned} \quad (6)$$

These states are also expressed in Fig. 2(b).

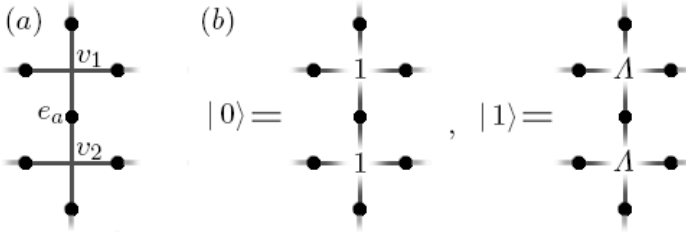


Fig. 2. (a) Two vertices use to store a logical qubit. (b) The logical states are stored by placing the trivial charge, 1, or the charge Λ at each vertex.

Measurement in the Z basis requires measurement of either vertex's occupancy, using the four-spin projectors of Eq.(2). The logical X is realized by $W_\Lambda(e_a)$, hence all operations diagonal in the X basis act on the spin e_a alone. The relation $|\pm\rangle\langle\pm| = (I \pm X)/2$ may be used to write the X basis projectors in terms of the lattice spins,

$$\begin{aligned} |+\rangle_a \langle+| &= \frac{I + W_\Lambda(e_a)}{2} = |e\rangle_{e_a} \langle e| + |c\rangle_{e_a} \langle c| + |c^2\rangle_{e_a} \langle c^2|, \\ |-\rangle_a \langle-| &= \frac{I - W_\Lambda(e_a)}{2} = |t\rangle_{e_a} \langle t| + |tc\rangle_{e_a} \langle tc| + |tc^2\rangle_{e_a} \langle tc^2|. \end{aligned} \quad (7)$$

Measurement in the X basis is therefore achieved by measuring the lattice spin in the above subspaces. Arbitrary phase gates in the X basis may then be written,

$$\begin{aligned} U_\theta(e_a) &= |+\rangle_a \langle +| + e^{i\theta} |-\rangle_a \langle -| \\ &= \left(|e\rangle_{e_a} \langle e| + |c\rangle_{e_a} \langle c| + |c^2\rangle_{e_a} \langle c^2| \right) \\ &\quad + e^{i\theta} \left(|t\rangle_{e_a} \langle t| + |tc\rangle_{e_a} \langle tc| + |tc^2\rangle_{e_a} \langle tc^2| \right). \end{aligned} \quad (8)$$

These may be easily performed with single spin rotations.

Entanglement with another logical qubit, b , stored on another pair of vertices with shared spin e_b , may be achieved by the phase-controlled-NOT gate. This is diagonal in the X basis of both qubits, and acts only on e_a and e_b . It may be expressed as follows,

$$K_{a,b} = |+\rangle_a \langle +| \otimes I_b + |-\rangle_a \langle -| \otimes X_b = I + W_\Lambda(e_a) + W_\Lambda(e_b) - W_\Lambda(e_b)W_\Lambda(e_a). \quad (9)$$

These operations form a universal gate set for quantum computation. For example, a Hadamard may be implemented on an arbitrary state $|\psi\rangle = \alpha|+\rangle_a + \beta|-\rangle_a$ of qubit a as follows. Firstly, qubit b is prepared in the state $|0\rangle_b$, and then entangled to a using $K_{a,b}$. The resulting state is,

$$\begin{aligned} \alpha|+0\rangle_{a,b} + \beta|-1\rangle_{a,b} &= \frac{1}{\sqrt{2}} \left(\alpha|00\rangle_{a,b} + \alpha|10\rangle_{a,b} + \beta|01\rangle_{a,b} - \beta|11\rangle_{a,b} \right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle_a (H|\psi\rangle_b) + |1\rangle_a (ZH|\psi\rangle_b) \right). \end{aligned} \quad (10)$$

Measuring qubit a in the Z basis then yields the state $H|\psi\rangle$ on qubit b , followed by a Z if the outcome of the measurement is $|1\rangle_a$. In the latter case the process may be repeated until the error is corrected and a Hadamard alone is implemented. With this Hadamard and the arbitrary phase gates in the X basis, arbitrary single qubit unitaries may be performed. With the entangling gate, this leads to universal quantum computation [23].

3 Fault-Tolerance Using Non-Abelian Charges

We will now extend the encoding by using Φ charges to hide the Λ 's. We first consider the most straightforward way of doing this, and then explore an alternative method.

Let us consider four neighbouring vertices, as shown in Fig. 3(a). Pairs of Φ charges carrying the trivial fusion channel may be created from the ground state with W_Φ (4). Applying this to spins $e_a^{1,4}$ and $e_a^{2,3}$ creates a pair carrying the trivial fusion channel on v_1 and v_4 , and another on v_2 and v_3 . This state is identified with the logical qubit state $|0\rangle_a$. By applying $W_\Lambda(e_a^{1,2})$, a Λ charge is

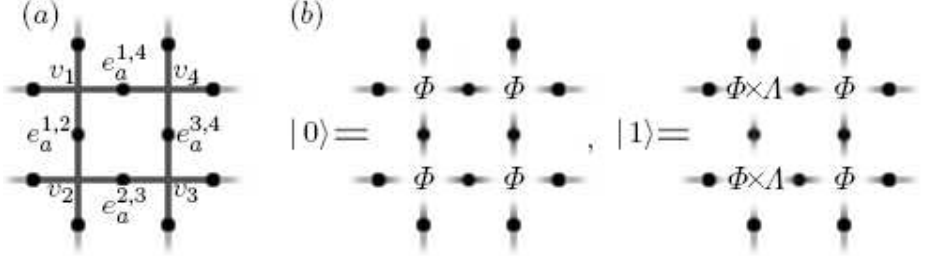


Fig. 3. (a) Four vertices use to store a logical qubit. These are labelled from v_1 to v_4 , starting from the top left and proceeding anticlockwise. The spin along the side connecting the vertices v_i and v_j is denoted $e_a^{i,j}$. (b) Both logical states use a Φ charge at each vertex. The only difference is that two of these are fused with a Λ charge in the $|1\rangle$ state. There is no local way to detect this, especially when the charges are separated.

fused with a Φ from each pair again resulting in two Φ pairs except that they now belong to the Λ fusion channel. This state is identified with the logical qubit state $|1\rangle_a$. Explicitly,

$$\begin{aligned} |0\rangle_a &= W_\Phi(e_a^{1,4})W_\Phi(e_a^{2,3})|gs\rangle, \\ |1\rangle_a &= W_\Phi(e_a^{1,4})W_\Phi(e_a^{2,3})W_\Lambda(e_a^{1,2})|gs\rangle. \end{aligned} \quad (11)$$

These states are also expressed in Fig. 3(b). Further logical qubits may be stored on other sets of four Φ charges. The syndrome measurements will see only the Φ charges and not the Λ charges they contain, making the logical states indistinguishable by local measurements alone, and degenerate under the Hamiltonian.

We observe that $W_\Lambda W_\Phi = W_\Phi$, implying,

$$W_\Lambda(e_a^{1,2})W_\Lambda(e_a^{1,4})W_\Phi(e_a^{1,4}) = W_\Lambda(e_a^{1,2})W_\Phi(e_a^{1,4}). \quad (12)$$

Here the left-hand side creates a Φ pair on v_1 and v_4 and fuses a Λ with the Φ on v_1 . The right-hand side does the same except that the Λ is fused with the Φ on v_4 . The equality between these shows that the resultant state does not depend upon which Φ the Λ was fused with, and holds even when they are well-separated, showing that the encoding of information in this way is indistinguishable by local operators alone.

Rather than keeping the Φ charges on neighbouring vertices, it is possible to move them apart. The single spins $e_a^{i,j}$ are then replaced by chains $C_a^{i,j}$ of l spins, where l is the new separation between the anyons. The logical states will be similar in form to those of Eq.(11) except that operations acting on spins $e_a^{i,j}$ will instead act on the chains $C_a^{i,j}$. The operations $W_\Phi[C_a^{i,j}]$ take the form,

$$W_\Phi[C_a^{i,j}] = \sum_{g_n \times \dots \times g_1 = c^k} (\omega^k + \omega^{-k}) |g_1, \dots, g_n\rangle \langle g_1, \dots, g_n|, \quad (13)$$

where $g_1, \dots, g_n$ are the states of the spins within the chain $C_a^{i,j}$ and $\omega = e^{i2\pi/3}$. The operations $W_\Lambda[C_a^{i,j}]$ are simply the product of W_Λ on each spin along a the chain. Just as in the previous section, this operation provides the logical X . Hence all X basis operations determined there still apply unchanged, except that they must now act on $O(l)$ spins to be realized. Measurement in the Z basis now requires the fusion of one or other of the Φ pairs and measurement of the result, the trivial charge implying $|0\rangle_a$ and Λ implying $|1\rangle_a$. These operations achieve universal quantum computation in the same way as before.

Errors in the encoding come from fusion with stray charges or braiding with stray fluxes. Both are suppressed by the stabilizer code, since regular measurements of the syndrome can detect these anyons and allow for their annihilation. They are also suppressed by the Hamiltonian, since the creation of the stray anyons costs energy. To see how well the errors are suppressed, we will now consider them individually. Errors in the X basis are caused by the creation of stray Λ charges and their fusion with a Φ from each pair. This requires a string of errors to occur on the l spins between the Φ 's, a process whose probability is suppressed by $O(e^{-l})$ [17,15]. Since the size of the logical operations only increases linearly with n , this is an efficient suppression of errors. Errors in the Z basis come from fusion with stray Φ 's, which can disrupt those used to encode and thus leave the logical information exposed to the stabilizer, and lose its degeneracy under the Hamiltonian. Z basis errors can also come from braiding with stray fluxes. Additional protection can be given to this basis by using a repetition code, in which two sets of n Φ charges are used to encode each qubit, rather than just two pairs [12]. The probability of errors will then be suppressed by $O(e^{-n})$.

It is possible to move the Φ charges using either multi-spin operations [20] or local potentials [11]. This gives the scheme a useful flexibility, since the charges may be moved apart to harness improved protection against errors and moved close so that logical operations may be performed on less spins.

3.1 Relation to Other Topological Memories

The Λ occupation of a vertex can be determined by measuring the observable $T_t(v)$, with the presence of the charge signalled by an outcome of -1 . This is true even when a Φ is present on the vertex, since the measurement can even detect those Λ 's fused with Φ 's. Consequently, making such a measurement on two Φ charges allows us to determine the number of Λ 's within the Φ pair. As one might expect, an even number will be found within any Φ pair that will fuse to vacuum, since the Λ 's will annihilate upon fusion. An odd number will be found within any Φ pair that will fuse to a Λ . The LOCC protocol of measuring $T_t(v)$ on each Φ and collecting the results is therefore sufficient to distinguish the logical states of Eq.(11). Note that since these measurements only act on the spins directly around each Φ , increasing their separation will not affect the complexity of the protocol.

Consider a modification to the syndrome measurement, in which the projectors $P_\Lambda(v)$ are replaced by $P'_\Lambda(v) = [T_e(v) + T_t(v)]/2$, and can therefore detect

the Λ 's within Φ 's. Since the syndrome measures each vertex and collects the results, it is able to count the number of Λ 's within each Φ pair, and thus distinguish the logical states. This shows that the encoding is equivalent to those in which Abelian anyons are stored in holes [16,12], since using the standard syndrome is equivalent to using the modified syndrome with the $P'_\Lambda(v)$ projections suppressed on any vertex holding a Φ . A exciting implication of this is that Abelian models may be used for quasi non-Abelian encodings, using the principles of non-Abelian anyons to enhance the power of their memories [24].

To see how a stronger encoding may be constructed, let us consider the single spin operation,

$$W'_\Phi = |c\rangle \langle c| - |c^2\rangle \langle c^2|. \quad (14)$$

Like W_Φ , this creates Φ charges on the vertices either side of the spin. However, measurements of $T_t(v)$ will give different results. An odd number of Λ 's will be found within a pair of Φ charges that fuse to vacuum, and an even number found within those that fuse to a Λ . This is opposite to what one would expect. The relative minus sign, coupled with the non-Abelian group multiplication underlying all operations on the spins, causes the $T_t(v)$'s to detect one more Λ within a pair than is actually present. Using this property, the logical states may be made indistinguishable to the $T_t(v)$ measurements, and any LOCC protocol, by using differently defined Λ pairs for the logical states. Explicitly,

$$\begin{aligned} |0\rangle_a &= W_\Phi(e_a^{1,4})W_\Phi(e_a^{2,3})|\text{gs}\rangle, \\ |1\rangle_a &= W'_\Phi(e_a^{1,4})W'_\Phi(e_a^{2,3})W_\Lambda(e_a^{1,2})|\text{gs}\rangle. \end{aligned} \quad (15)$$

With this encoding an even number of Λ 's is found within any pair, regardless of their fusion channel. They are then distinguishable only with non-local operations, such as the fusion of Φ 's. This is the true non-Abelian encoding, whose protection goes above and beyond that of Abelian encoding with holes.

Note that the huge operational difference between this encoding and that of Eq. (11) comes directly from the non-Abelian group multiplication underlying the model. It is only because of this that the relative minus sign in Eq. (14) has such an effect. Abelian group multiplication cannot provide tricks to fool the $T_t(v)$ observables in such a way.

The stronger encoding increases the complexity of the logical X operation. The fusion of a Φ 's with a Λ 's is no longer enough. The unitary operation,

$$U(v) = \frac{1}{3}T_e(v) - \frac{2}{3}[\omega T_c(v) + \omega^2 T_{c^2}(v)], \quad (16)$$

must be applied to any vertex on which a fusion takes place to rotate from W_Φ type Φ pairs to W'_Φ type, or vice-versa. Rather than single spin operations, logical operations on neighbouring Φ 's must then act on seven spins. For non-neighbouring Φ 's, operations must also act on six more spins than the previous requirement. Though the size of logical operations still scales with $O(l)$, and so still gives efficient suppression of errors, it is not as accessible to actual experimental realization.

4 Conclusions and Further Work

We have proposed a novel scheme for fault-tolerant quantum computation, utilizing a non-Abelian topological memory. As a result of this work, we have an explicit form for the logical states stored non-locally in terms of the physical states of the underlying lattice model, an understanding of what kinds of memories are possible and their relations to other topological memories. Specifically, we have found two means to encode qubits in the fusion channels of the model's anyons. Though both fault-tolerant and indistinguishable to local operations, these encodings have a crucial difference. One has states distinguishable to LOCC protocols, and is equivalent to encodings using Abelian anyons. The other has states distinguishable only to non-local operations. Hence, by showing exactly how these encodings differ, we have demonstrated the true difference between Abelian and non-Abelian anyons from a quantum information perspective.

Furthermore, we harness these states to give the non-topological operations required for universality while remaining below the energy gap. Our work allows the application of realistic error models and studies of how anyonic systems respond to practical experimental conditions [25]. There exist proposals on how to realize this and other lattice models in the laboratory [20,26,27,28,29]. This exercise is a step towards physical realizations of simple non-Abelian systems to demonstrate aspects of quantum computation.

We also note that the use of single spin measurements on highly entangled states bears a similarity to measurement based quantum computation [30]. It would be beneficial to unify these formalisms.

Acknowledgements

We would like to thank Gavin Brennen for inspiring conversations. This work was supported by the EU grants SCALA and EMALI, the EPSRC, the Finnish Academy of Science and the Royal Society.

References

1. Wilczek, F.: Phys. Rev. Lett. 49, 957 (1982)
2. Brennen, G.K., Pachos, J.K.: Proc. R. Soc. London, A 464, 2089 (2008); and references therein
3. Kalmeyer, V., Laughlin, R.B.: Phys. Rev. Lett. 59, 2095 (1987)
4. Read, N., Green, D.: Phys. Rev. B 61, 10267 (2000)
5. Freedman, M., Larsen, M., Wang, Z.: Commun. Math. Phys. 237, 605 (2002)
6. Wen, X.-G., Wilczek, F., Zee, A.: Phys. Rev. B 39, 11413 (1989)
7. Levin, M., Wen, X.-G.: Phys. Rev. B 71, 045110 (2005)
8. Fendley, P.: Ann. Phys. 323, 3113 (2007)
9. Wootton, J.R., Lahtinen, V., Wang, Z., Pachos, J.K.: Phys. Rev. B 78, 161102(R) (2008)
10. Lloyd, S.: Quant. Inf. Proc. 1, 1–2 (2002)
11. Pachos, J.K.: Int. J. Quant. Inf. 4, 947 (2006)

12. Wootton, J.R., Pachos, J.K.: 6th Workshop on Quantum Physics and Logic, arXiv:0904.4373 (2008)
13. Bravyi, S.: Phys. Rev. A 73, 042313 (2006)
14. Georgiev, L.S.: Phys. Rev. B 74, 235112 (2006)
15. Dennis, E., Kitaev, A., Landahl, A., Preskill, J.: J. Math. Phys. 43, 4452 (2002)
16. Raussendorf, R., Harrington, J., Goyal, K.: New J. Phys. 9, 199 (2007)
17. Kitaev, A.: Ann. Phys. 303, 2 (2003)
18. Farhi, E., Goldstone, J., Gutmann, S., Lapan, J., Lundgren, A., Preda, D.: Science 292, 472 (2001)
19. Mochon, C.: Phys. Rev. A 69, 032306 (2004)
20. Aguado, M., Brennen, G.K., Verstraete, F., Cirac, J.I.: Phys. Rev. Lett. 101, 260501; Aguado, M., Brennen, G.K., Cirac, J.I.: New J. Phys. 11, 053009 (2009)
21. Freedman, M., Nayak, C., Walker, K.: cond-mat/0512066 (2005)
22. Gottesman, D.: Phys. Rev. A 54, 1862 (1996)
23. Chuang, I.L., Nielsen, M.A.: Quantum Computation and Quantum Information, pp. 191–197. Cambridge University Press, Cambridge (2004)
24. Wootton, J.R., Lahtinen, V., Doucot, B., Pachos, J.K.: arXiv:0908.0708 (2009)
25. Iblisdir, S., Perez-Garcia, D., Aguado, M., Pachos, J.: Phys. Rev. B 79, 134303 (2009); Iblisdir, S., Perez-Garcia, D., Aguado, M., Pachos, J.: arXiv:0812.4975 (2008)
26. Doucot, B., Ioffe, L.B., Vidal, J.: Phys. Rev. B 69, 214501 (2004)
27. Pachos, J.K., Wieczorek, W., Schmid, C., Kiesel, N., Pohlner, R., Weinfurter, H.: New J. Phys. 11, 083010 (2009)
28. Lu, C.-Y., Gao, W.-B., Gühne, O., Zhou, X.-Q., Chen, Z.-B., Pan, J.-W.: Phys. Rev. Lett. 102, 030502 (2009)
29. Micheli, A., Brennen, G.K., Zoller, P.: Nat. Phys. 2, 341–347 (2006)
30. Raussendorf, R., Briegel, H.J.: Phys. Rev. Lett. 86, 5188 (2001)

Conditions for the Approximate Correction of Algebras

Cédric Bény

Centre for Quantum Technologies, National University of Singapore

Abstract. We study the approximate correctability of general algebras of observables, which represent hybrid quantum-classical information. This includes approximate quantum error correcting codes and subsystems codes. We show that the main result of [1] yields a natural generalization of the Knill-Laflamme conditions in the form of a dimension independent estimate of the optimal reconstruction error for a given encoding, measured using the trace-norm distance to a noiseless channel.

Slightly relaxing the requirement of perfect quantum error correction can allow for significantly larger quantum codes [2,3]. Here we focus on a quantification of the correction error based on the diamond norm distance, introduced below, which can be related to the worst case entanglement fidelity. (See [4] for the case of average entanglement fidelity). There exist results giving sufficient conditions for a code to be approximately correctable in that sense [5,6], however it is not known how general these conditions are. Instead we want to draw attention to results by Kretschmann *et al.* [1,7] who gave lower and upper bounds for the optimal reconstruction error for a given code in terms of the complementary channel's distance to a maximally forgetful channel. The present report can be seen partly as an advertisement of these results in a context where they are not widely known, or their meaning not recognized, namely as a providing a necessary and sufficient condition for approximate error correction. In addition we improve on these results by rendering the conditions more explicit, and generalizing them to the correction of general algebras.

The condition that we obtain (Theorem 1) can be understood as a perturbation of the exact Knill-Laflamme condition [8], or more generally its subsystem version [9], or full algebraic form [10]. We also give an essentially equivalent condition based on individual observables of the algebra (Theorem 2). The correctable algebra can be understood as representing a quantum system with superselection rules, or a hybrid quantum-classical memory [11], and can be shown to be the most general type of exactly correctable information in the sense of [12].

1 Preliminaries

A channel $\mathcal{N}$ is a completely positive trace-preserving map. It can always be written as

$$\mathcal{N}(\rho) = \sum_i E_i \rho E_i^\dagger$$

where the operators E_i are the channel elements and must only satisfy $\sum_i E_i^\dagger E_i = \mathbf{1}$. The dual $\mathcal{N}^\dagger$ is defined by the relation

$$\mathrm{Tr}(\mathcal{N}(\rho)A) = \mathrm{Tr}(\rho\mathcal{N}^\dagger(A))$$

for any state ρ and any operator A . This implies that

$$\mathcal{N}^\dagger(A) = \sum_i E_i^\dagger \rho E_i.$$

Physically, $\mathcal{N}$ is interpreted as evolving states, while $\mathcal{N}^\dagger$ evolves observables. Hence $\mathcal{N}^\dagger$ represents the Heisenberg picture for the evolution defined by the channel. To avoid confusion, we only call $\mathcal{N}$ a *channel*, while $\mathcal{N}^\dagger$ is its *dual*.

1.1 Complementary Channel

For any channel $\mathcal{N}$ we can find an isometry V ($V^\dagger V = \mathbf{1}$) such that

$$\mathcal{N}^\dagger(A) = V^\dagger(A \otimes \mathbf{1})V.$$

The isometry V amounts to adding an extra system; the “environment”, with a fixed pure initial state $|\phi_E\rangle$ and letting it interact unitarily with the system for a fixed amount of time, i.e. $V|\psi\rangle := U(|\psi\rangle \otimes |\phi_E\rangle)$ for some unitary operator U . This allows one to define a *complementary channel* $\widehat{\mathcal{N}}$ through

$$\widehat{\mathcal{N}}^\dagger(B) = V^\dagger(\mathbf{1} \otimes B)V.$$

The channel $\widehat{\mathcal{N}}$ maps the initial state of the system to the final state of the environment. The most important fact that we will use is that all complementary channels are equivalent up to a unitary transformation of their output, and eventual embedding into a larger environment, and that this property is stable under perturbation as shown in [1].

It is easy to relate a dilation with isometry V to channel elements E_i by introducing any orthonormal basis $|i\rangle$ of the environment as follows:

$$\mathcal{N}^\dagger(A) = V^\dagger(A \otimes \mathbf{1})V = \sum_i V^\dagger(A \otimes |i\rangle\langle i|)V = \sum_i V^\dagger(\mathbf{1} \otimes |i\rangle\langle i|)A(\mathbf{1} \otimes \langle i|)V$$

Hence we can use

$$E_i = (\mathbf{1} \otimes \langle i|)V$$

which is defined by

$$\langle \psi | E_i = (\langle \psi | \otimes \langle i |) V.$$

This implies that the complementary channel can be written in dual form as

$$\widehat{\mathcal{N}}^\dagger(B) = \sum_{ij} \langle i | B | j \rangle E_i^\dagger E_j.$$

1.2 Distance between Channels

Any operator A has a norm defined by

$$\|A\| := \sup_{|\psi\rangle} \frac{\|A|\psi\rangle\|}{\| |\psi\rangle \|}.$$

This norm on operators can be used to define a distance between dual channels as follows:

$$\|\mathcal{N}_1^\dagger - \mathcal{N}_2^\dagger\| := \sup_{A, \|A\| \leq 1} \|\mathcal{N}_1^\dagger(A) - \mathcal{N}_2^\dagger(A)\|.$$

However this distance can increase when the channels are tensored with the identity channel on an auxiliary space. Therefore we also define the *completely bounded* norm

$$\|\mathcal{N}_1^\dagger - \mathcal{N}_2^\dagger\|_{cb} := \|(\mathcal{N}_1^\dagger - \mathcal{N}_2^\dagger) \otimes \text{id}\|$$

where id is the identity channel on a Hilbert space of the same dimension as that of the source of the two channels. This distance is guaranteed to be stable under further trivial extension (See [13] for an introduction). It is equal to the *diamond norm* distance between the channels themselves:

$$\|\mathcal{N}_1^\dagger - \mathcal{N}_2^\dagger\|_{cb} = \|\mathcal{N}_1 - \mathcal{N}_2\|_\diamond$$

which is defined by

$$\begin{aligned} \|\mathcal{N}_1 - \mathcal{N}_2\|_\diamond &:= \|(\mathcal{N}_1^\dagger - \mathcal{N}_2^\dagger) \otimes \text{id}\|_1 \\ &= \sup_{\rho} \text{Tr}|(\mathcal{N}_1 - \mathcal{N}_2) \otimes \text{id}(\rho)|. \end{aligned}$$

where $\|\cdot\|_1$ is the trace norm. This distance is directly related to the worst case probability of failing to distinguish between the outputs of the two channels for any common initial state.

2 Exact Correctability of Algebras

We review here results on the exact correctability of algebras, as defined in [10]. A $\dagger$ -algebra (or algebra for short) is a set of operators closed under multiplication and which also contains the adjoint of all its elements. For instance, suppose that our Hilbert space $\mathcal{H}$ is divided into two subsystems: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, then consider the set $\mathcal{A}$ of operators of the form $A \otimes \mathbf{1}$, where A is an operator on $\mathcal{H}_A$ and $\mathbf{1}$ the identity on $\mathcal{H}_B$. It is trivial to show that $\mathcal{A}$ is an algebra. It represents all the local observables acting on $\mathcal{H}_1$. In fact this is close to being the most general form of a $\dagger$ -algebra. For any $\dagger$ -algebra $\mathcal{A}$ we can find a decomposition of the Hilbert space into orthogonal subspaces $\mathcal{H}_i$ which are left invariant by all elements of the algebra. Furthermore, when restricted to any of these invariant subspaces, the algebra has precisely the form described in the above example.

Hence the algebra defines a set of subsystems living in a family of orthogonal subspaces. This means that any element $A \in \mathcal{A}$ is of the form

$$A = \sum_i A_i \otimes \mathbf{1}_i$$

where $A_i \otimes \mathbf{1}_i$ is an operator supported on $\mathcal{H}_i$. Said differently, if P_i is the projector on $\mathcal{H}_i$ then $P_i A P_i = A_i \otimes \mathbf{1}_i$.

A useful tool that we will be using is the projector $\mathcal{P}_{\mathcal{A}}$ on this algebra, which we take to be orthogonal in terms of the Hilbert-Schmidt inner product between operators. This is a quantum channel satisfying $\mathcal{P}_{\mathcal{A}}^2 = \mathcal{P}_{\mathcal{A}} = \mathcal{P}_{\mathcal{A}}^\dagger$, whose range is precisely $\mathcal{A}$. It has the following explicit form:

$$\mathcal{P}_{\mathcal{A}}(\rho) = \sum_i \frac{1}{\text{Tr} P_i} \sum_{jk} (\mathbf{1}_i \otimes |j\rangle_i \langle k|_i) \rho (\mathbf{1}_i \otimes |k\rangle_i \langle j|_i) \quad (1)$$

where the vectors $|j\rangle_i$ for a fixed i are orthogonal and satisfies $\sum_k \mathbf{1}_i \otimes |k\rangle_i \langle k|_i = P_i$.

We say that an algebra $\mathcal{A}$ is correctable for the channel $\mathcal{N}$ if there exists a “correction” channel $\mathcal{R}$ such that for all $A \in \mathcal{A}$,

$$(\mathcal{R} \circ \mathcal{N})^\dagger(A) = A. \quad (2)$$

Note that $\mathcal{A}$ contains the spectral projectors of any observable $A \in \mathcal{A}$. Hence this definition implies that measuring A before the action of the channel $\mathcal{N}$ or after the correction will yield the same probabilities, no matter what the initial state was.

Clearly, Equ. 2 implies that $\mathcal{P}_{\mathcal{A}} \circ \mathcal{R} \circ \mathcal{N} = \mathcal{P}_{\mathcal{A}}$. Hence an equivalent formulation is to require the existence of a (possibly different) channel $\mathcal{R}$ such that

$$\mathcal{R} \circ \mathcal{N} = \mathcal{P}_{\mathcal{A}}. \quad (3)$$

It was shown in [10] that any algebra $\mathcal{A}$ is correctable if and only if its elements $A \in \mathcal{A}$ all satisfy

$$[A, E_i^\dagger E_j] = 0 \quad \text{for all } i, j \quad (4)$$

where E_i are the error operators, or elements of the channel $\mathcal{N}$ representing the interaction with the environment. What this means is that all the correctable algebras belong to the largest correctable algebra defined by the set of all operators commuting with the operators $E_i^\dagger E_j$, which is always a $\dagger$ -algebra. This condition shows that the correctability of an algebra is conditioned purely on the correctability of a family of generators (for instance two different Pauli operators if we are correcting a qubit).

We say that an observable A is correctable if the algebra $\text{Alg}(A)$ it generates is correctable. $\text{Alg}(A)$ is commutative and spanned by the spectral projectors of A . Any other observable in that algebra is just a coarse-graining of A . Clearly all the correctable observables are correctable by the same correction channel, namely the one correcting the full commutant of the operators $E_i^\dagger E_j$.

Equation 4 has a clear physical meaning if we note that the operators $E_i^\dagger E_j$ come from the complementary channel $\widehat{\mathcal{N}}^\dagger$. Indeed,

$$E_i^\dagger E_j = \widehat{\mathcal{N}}^\dagger(|i\rangle\langle j|).$$

Hence Equ. 4 can also be written as

$$[A, \widehat{\mathcal{N}}^\dagger(B)] = 0 \quad \text{for all } B. \quad (5)$$

The operators of the form $\widehat{\mathcal{N}}^\dagger(B)$ characterize the properties of the source system which are faithfully represented in the environment. Indeed, assuming that ρ is any arbitrary state of the source system, if B_i are elements of a POVM on the environment, then measuring $\{B_i\}$ yields probabilities $p_i = \text{Tr}(\widehat{\mathcal{N}}(\rho)B_i) = \text{Tr}(\rho\widehat{\mathcal{N}}^\dagger(B_i))$. These probabilities are precisely the probabilities that one would obtain by measuring the POVM with elements $A_i = \widehat{\mathcal{N}}^\dagger(B_i)$ on ρ . Hence the POVMs with elements of the form $\widehat{\mathcal{N}}^\dagger(B_i)$ for any POVM $\{B_i\}$ are observables of the source which represent information that is present in the environment. We say that these observables are *preserved* [14] by the channel $\widehat{\mathcal{N}}$. In particular the projective (sharp) observables (characterized by $A_i^2 = A_i$) which are preserved by a channel are the correctable observables for that channel [15].

Hence Equ. 5 means that the correctable observables are precisely those which are compatible with the observables preserved in the environment. Theorem 2 below shows how this fact generalizes in the approximate case.

Let $\mathcal{A}'$ be the commutant of $\mathcal{A}$, i.e. the algebra formed by the operators which commute with all the operators of $\mathcal{A}$. If $\mathcal{A}$ is the correctable algebra, then $\mathcal{A}'$ is the algebra generated by the operators $\widehat{\mathcal{N}}^\dagger(B)$ for any B , or equivalently by the operators $E_i^\dagger E_j$ for any i and any j .

The correctability condition expressed in Equ. 4 can also be written as

$$\widehat{\mathcal{N}} = \widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}. \quad (6)$$

Indeed, this means that $\widehat{\mathcal{N}}^\dagger = \mathcal{P}_{\mathcal{A}'} \circ \widehat{\mathcal{N}}^\dagger$, and hence any operator in the range of $\widehat{\mathcal{N}}^\dagger$ commutes with all elements of $\mathcal{A}$. If $\mathcal{P}_{\mathcal{A}}$ is given by Equ. 1 then one can show that $\mathcal{P}_{\mathcal{A}'}$ is given by

$$\mathcal{P}_{\mathcal{A}'}(\rho) = \sum_i \frac{1}{\text{Tr} P_i} \sum_{jk} (\widetilde{|j\rangle}_i \widetilde{\langle k|}_i \otimes \mathbf{1}_i) \rho (\widetilde{|k\rangle}_i \widetilde{\langle j|}_i \otimes \mathbf{1}_i). \quad (7)$$

where the vectors $\widetilde{|j\rangle}_i$ for a fixed i are orthogonal and satisfy $\sum_k \widetilde{|k\rangle}_i \widetilde{\langle k|}_i \otimes \mathbf{1}_i = P_i$.

Note that we have not mentioned any encoding, or code. The reason is that the encoding map can be considered to be included in the channel $\mathcal{N}$. For instance if the initial states are guaranteed to be encoded in a subspace $\mathcal{H}_C \subset \mathcal{H}$, i.e. the encoding is an isometry V (i.e. such that $VV^\dagger$ projects on $\mathcal{H}_C$), then we immediately see by replacing the channel elements E_i by $E_i V$ that an observable A is correctable under this assumption if and only if

$$[A, V^\dagger E_i^\dagger E_j V] = 0.$$

If we require that the algebra formed by these operators is the whole algebra of operators on the code spans $\mathcal{H}_C$ then we recover the Knill-Laflamme conditions [8], since this implies

$$V^\dagger E_i^\dagger E_j V \propto \mathbf{1}_C.$$

Similarly, if we only require the algebra to be that of all operators acting on a subsystem of the code we recover the conditions for subsystem error correction [16].

3 Approximate Correctability of Algebras

We will focus on the following approximate version of Equ. 3:

Definition 1. *We say that an algebra $\mathcal{A}$ is ϵ -correctable for the noise channel $\mathcal{N}$ if there exists a channel $\mathcal{R}$ such that*

$$\|\mathcal{R} \circ \mathcal{N} - \mathcal{P}_{\mathcal{A}}\|_{\diamond} \leq \epsilon.$$

We define the minimal reconstruction error to be

$$E_{\mathcal{A}}(\mathcal{N}) := \min_{\mathcal{R}} \|\mathcal{R} \circ \mathcal{N} - \mathcal{P}_{\mathcal{A}}\|_{\diamond}.$$

The following theorem gives a “necessary” and “sufficient” condition for approximate error correction of an algebra in the form of an estimate of the optimal correction error.

Theorem 1. *Let*

$$\delta_{\mathcal{A}}(\mathcal{N}) = \|\widehat{\mathcal{N}} - \widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \quad (8)$$

then

$$\frac{1}{4}\delta_{\mathcal{A}}^2(\mathcal{N}) \leq E_{\mathcal{A}}(\mathcal{N}) \leq 2\delta_{\mathcal{A}}^{\frac{1}{2}}(\mathcal{N}).$$

Note that $\delta_{\mathcal{A}}(\mathcal{N})$ is explicit apart from the diamond norm (see [17] or [13] for computation techniques).

Proof. These conditions follow from the exact condition (Equ. 6) and the main result of [1], namely that if

$$\|\mathcal{N}_1 - \mathcal{N}_2\|_{\diamond} \leq \epsilon$$

then for all channels $\widehat{\mathcal{N}}_1$ complementary to $\mathcal{N}_1$ there exists a channel $\widehat{\mathcal{N}}_2$ complementary to $\mathcal{N}_2$ such that

$$\|\widehat{\mathcal{N}}_1 - \widehat{\mathcal{N}}_2\|_{\diamond} \leq 2\sqrt{\epsilon}.$$

Suppose that for some channel $\mathcal{N}$,

$$\|\widehat{\mathcal{N}} - \widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq \epsilon.$$

We know from Equ. 6 that the algebra $\mathcal{A}$ is correctable for any channel $\mathcal{M}$ complementary to $\widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}$. In addition we can choose $\mathcal{M}$ such that

$$\|\mathcal{N} - \mathcal{M}\|_{\diamond} \leq 2\sqrt{\epsilon}$$

Let $\mathcal{R}$ be the correction channel for this choice of $\mathcal{M}$, i.e. $\mathcal{R} \circ \mathcal{M} = \mathcal{P}_{\mathcal{A}}$, then we have

$$\|\mathcal{R} \circ \mathcal{N} - \mathcal{P}_{\mathcal{A}}\|_{\diamond} = \|\mathcal{R} \circ \mathcal{N} - \mathcal{R} \circ \mathcal{M}\|_{\diamond} \leq \|\mathcal{R}\|_{\diamond} \|\mathcal{N} - \mathcal{M}\|_{\diamond} \leq 2\sqrt{\epsilon}.$$

Reciprocally, suppose that $\mathcal{A}$ is ϵ -correctable for $\mathcal{N}$, i.e. $\|\mathcal{R} \circ \widehat{\mathcal{N}} - \mathcal{P}_{\mathcal{A}}\|_{\diamond} \leq \epsilon$. Then by using again the result of [1] we have that $\widehat{\mathcal{R} \circ \mathcal{N}}$ is within $2\sqrt{\epsilon}$ to some channel $\mathcal{M}$ complementary to $\mathcal{P}_{\mathcal{A}}$. But since $\mathcal{A}$ is obviously correctable for the channel $\mathcal{P}_{\mathcal{A}}$, we know by the condition for exact correction (Equ. 6) that $\mathcal{M} = \mathcal{M} \circ \mathcal{P}_{\mathcal{A}'}$:

$$\|\widehat{\mathcal{R} \circ \mathcal{N}} - \mathcal{M} \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq 2\sqrt{\epsilon}.$$

Note that we can define a dilation of $\mathcal{R} \circ \mathcal{N}$ by the isometry $V = (V_{\mathcal{R}} \otimes \mathbf{1})V_{\mathcal{N}}$ where $V_{\mathcal{R}}$ (resp. $V_{\mathcal{N}}$) defines a dilation of $\mathcal{R}$ (resp. $\mathcal{N}$). In this product, the input of $V_{\mathcal{R}}$ is the output of $\mathcal{N}$. Hence the corresponding channel complementary to $\mathcal{R} \circ \mathcal{N}$ has two outputs, one from $V_{\mathcal{N}}$ and one from $V_{\mathcal{R}}$. If we trace out the output of $V_{\mathcal{R}}$ we obtain a channel complementary to $\mathcal{N}$, which we will call $\widehat{\mathcal{N}}$. Applying the same partial trace on $\mathcal{M} \circ \mathcal{P}_{\mathcal{A}'}$ yields a channel $\mathcal{M}' = \mathcal{M}' \circ \mathcal{P}_{\mathcal{A}'}$. Given that a partial trace cannot increase the diamond norm, we obtain

$$\|\widehat{\mathcal{N}} - \mathcal{M}'\|_{\diamond} = \|\widehat{\mathcal{N}} - \mathcal{M}' \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq 2\sqrt{\epsilon}$$

Hence also,

$$\|\widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'} - \mathcal{M}'\|_{\diamond} \leq \|\widehat{\mathcal{N}} - \mathcal{M}'\|_{\diamond} \|\mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq 2\sqrt{\epsilon}.$$

If we use these two inequalities together we obtain

$$\|\widehat{\mathcal{N}} - \widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq \|\widehat{\mathcal{N}} - \mathcal{M}'\|_{\diamond} + \|\mathcal{M}' - \widehat{\mathcal{N}} \circ \mathcal{P}_{\mathcal{A}'}\|_{\diamond} \leq 4\sqrt{\epsilon}. \quad \square$$

As an example let us show how the estimate (Equ. 8) looks like if we want to approximately correct a subspace, i.e. when the algebra $\mathcal{A}$ consists of the set of all operators acting on a code space $\mathcal{H}_C$, which we write $\mathcal{A} = \mathcal{B}(\mathcal{H}_C)$. Let V be the isometry embedding $\mathcal{H}_C$ into the physical Hilbert space $\mathcal{H}$. We also write the encoding channel as $\mathcal{E}(\rho) = V\rho V^{\dagger}$. In this case, the commutant $\mathcal{A}'$ is the trivial algebra containing only multiples of the identity on $\mathcal{H}_C$. Hence the corresponding projector is

$$\mathcal{P}_{\mathcal{A}}(\rho) = \text{Tr}(\rho) \frac{\mathbf{1}}{\text{Tr} \mathbf{1}}.$$

Let d be the dimension of the code Hilbert space $\mathcal{H}_C$, and

$$\lambda_{ij} := \langle i | \widehat{\mathcal{N} \circ \mathcal{E}}(\mathbf{1}/d) | j \rangle = \frac{1}{d} \text{Tr}(V^{\dagger} E_i^{\dagger} E_j V)$$

then direct computation shows that our estimate of the optimal recovery error is

$$\delta_{\mathcal{B}(\mathcal{H}_C)}(\mathcal{N} \circ \mathcal{E}) = \sup_{\|B\| \leq 1} \left\| \sum_{ij} (V^{\dagger} E_i^{\dagger} E_j V - \lambda_{ij} \mathbf{1}) \otimes B_{ij} \right\| \quad (9)$$

where B_{ij} are blocks of B , i.e. $B = \sum_{ij} |i\rangle\langle j| \otimes B_{ij}$. We see that the exact Knill-Laflamme conditions put this quantity to zero by imposing $V^{\dagger} E_i^{\dagger} E_j V - \lambda_{ij} \mathbf{1} = 0$ for all i, j .

3.1 Condition on Individual Operators

In the case of exact correction, the form of the condition expressed as a commutator (Equ. 5) is fundamental because it shows how different correctable algebras are related: namely that they are all in fact part of a largest correctable algebra. Here we show that a form of this condition still holds in the approximate case, however the consequences are weaker.

The following lemma will allow us to make this generalization.

Lemma 1. *Let $\mathcal{A}$ be a $\dagger$ -algebra and B any operator with $\|B\| \leq 1$, then*

$$\|B - \mathcal{P}_{\mathcal{A}'}(B)\| \leq \sup_{A \in \mathcal{A}, \|A\| \leq 1} \|[A, B]\| \leq 2\|B - \mathcal{P}_{\mathcal{A}'}(B)\|$$

Proof. The upper bound is straightforward:

$$\begin{aligned} \|[A, B]\| &= \|AB - A\mathcal{P}_{\mathcal{A}'}(B) + \mathcal{P}_{\mathcal{A}'}(B)A - BA\| \\ &\leq \|A\|\|B - \mathcal{P}_{\mathcal{A}'}(B)\| + \|\mathcal{P}_{\mathcal{A}'}(B) - B\|\|A\| \\ &\leq 2\|B - \mathcal{P}_{\mathcal{A}'}(B)\|. \end{aligned}$$

For the lower bound, note that the set of unitary operators in $\mathcal{A}$ forms a group with Haar measure μ . We assume that the measure is normalized to one. Note that the projector $\mathcal{P}_{\mathcal{A}'}$ can be computed by averaging over this group:

$$\mathcal{P}_{\mathcal{A}'}(B) = \int d\mu(U) U^\dagger B U$$

for all B . Indeed, it is clear that $\mathcal{P}_{\mathcal{A}'} = \mathcal{P}_{\mathcal{A}'}^\dagger$, and the fact that

$$U^\dagger \mathcal{P}_{\mathcal{A}'}(B) U = \mathcal{P}_{\mathcal{A}'}(B) \quad (10)$$

implies $\mathcal{P}_{\mathcal{A}'}^2 = \mathcal{P}_{\mathcal{A}'}$. In addition Equ. 10 also implies, $[\mathcal{P}_{\mathcal{A}'}(B), U] = 0$ for all $U \in \mathcal{A}$, which implies $\mathcal{P}_{\mathcal{A}'}(B) \in \mathcal{A}'$ for all B since the unitary operators span the algebra. But also, since all the unitary operators integrated over are in $\mathcal{A}$, it is clear that $\mathcal{P}_{\mathcal{A}'}(A) = A$ for all $A \in \mathcal{A}'$.

Using this expression for $\mathcal{P}_{\mathcal{A}'}$, we have

$$\begin{aligned} \|B - \mathcal{P}_{\mathcal{A}'}(B)\| &\leq \int d\mu(U) \|U^\dagger U B - U^\dagger B U\| \\ &\leq \int d\mu(U) \|U^\dagger\| \| [U, B] \| \\ &\leq \sup_{A \in \mathcal{A}, \|A\| \leq 1} \|[A, B]\| \quad \square \end{aligned}$$

We can now combine this lemma with Theorem 1 to obtain the following condition for approximate correctability:

Theorem 2. *If an algebra $\mathcal{A}$ is $\frac{1}{8}\epsilon^2$ -correctable then all its elements $A \in \mathcal{A}$ with $\|A\| \leq 1$ must approximately commute with all the observables preserved in the environment, i.e.*

$$\|[A \otimes \mathbf{1}, (\hat{\mathcal{N}}^\dagger \otimes \text{id})(B)]\| \leq \epsilon$$

for all operators $\|B\| \leq 1$, where $\mathbf{1}$ and id act on a Hilbert-space of dimension equal to that of the source of $\mathcal{N}$. Conversely, this condition guarantees that $\mathcal{A}$ is $2\sqrt{\epsilon}$ -correctable.

Proof. The estimate $\delta_{\mathcal{A}}(\mathcal{N})$ defined in Equ. 8 can be expressed in terms of the CB norm distance between the dual channels as

$$\delta_{\mathcal{A}}(\mathcal{N}) = \|\widehat{\mathcal{N}}^\dagger - \mathcal{P}_{\mathcal{A}'} \circ \widehat{\mathcal{N}}^\dagger\|_{cb}.$$

Theorem 1 then implies that if an algebra $\mathcal{A}$ is $\frac{1}{8}\epsilon^2$ -correctable, then for all $\|B\| \leq 1$,

$$\|(\widehat{\mathcal{N}}^\dagger \otimes \text{id})(B) - (\mathcal{P}_{\mathcal{A}'} \otimes \text{id})(\widehat{\mathcal{N}}^\dagger \otimes \text{id})(B)\| \leq \frac{1}{2}\epsilon.$$

Since $\mathcal{P}_{\mathcal{A}'} \otimes \text{id}$ is just the projector on the algebra $\mathcal{A} \otimes B(\mathcal{H})$, Lemma 1 implies that for all $A \in \mathcal{A}$,

$$\|[A \otimes \mathbf{1}, (\widehat{\mathcal{N}}^\dagger \otimes \text{id})(B)]\| \leq \epsilon.$$

Reciprocally, following the same steps in reverse, this condition implies via Lemma 1 that $\delta_{\mathcal{A}}(\mathcal{N}) \leq \epsilon$ which then implies via Theorem 1 that $\mathcal{A}$ is $2\sqrt{\epsilon}$ correctable. $\square$

We see that contrary to the exact case, the approximately correctable observables must not only approximately commute with the observables preserved by the complementary channel, but also with the observables preserved by its trivial extension on a larger space.

Also, unlike in the exact case, this condition does not guarantee that it is sufficient to test the commutativity condition on generators of the algebra. We can only rely on the convexity of the approximate condition. For instance this bound degrades with the number of products taken. If the norm one operators A_i , $i = 1, \dots, n$ satisfy $\|[A_i \otimes \mathbf{1}, (\widehat{\mathcal{N}}^\dagger \otimes \text{id})(B)]\| \leq \epsilon$, then we can only guarantee that $\|[A_1 A_2 \cdots A_n \otimes \mathbf{1}, (\widehat{\mathcal{N}}^\dagger \otimes \text{id})(B)]\| \leq n\epsilon$.

4 Outlook

In the exact case we know that there is only one maximal set of simultaneously correctable observables; the commutant of the operators $E_i^\dagger E_j$. We hope that the results presented in the last section can help understand the structure of—and the relation between—the sets of simultaneously approximately correctable observables, for a given error ϵ .

We focused here on the diamond norm distance between the corrected channel $\mathcal{R} \circ \mathcal{N}$ and a target channel $\mathcal{P}_{\mathcal{A}}$ because it allowed us to obtain a generalization of the condition expressed in terms of the commutation relation (Equ. 5). However, the same technique yields a much tighter estimate of the worst case entanglement fidelity. This is analyzed in a separate article in which we also address the problem of finding a good approximate correction channel [18].

Acknowledgements

Part of this work was done at the workshop QIP 2009. The author is grateful to the participants of the workshop TQC 2009 for feedback. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

1. Kretschmann, D., Schlingemann, D., Werner, R.F.: The information-disturbance tradeoff and the continuity of Stinespring's representation. *IEEE Transactions on Information Theory* 54(4), 1708–1717 (2008)
2. Leung, D.W., Nielsen, M.A., Chuang, I.L., Yamamoto, Y.: Approximate quantum error correction can lead to better codes. *Phys. Rev. A* 56(4), 2567–2573 (1997)
3. Crépeau, C., Gottesman, D., Smith, A.: Approximate quantum error-correcting codes and secret sharing schemes. In: Cramer, R. (ed.) *EUROCRYPT 2005*. LNCS, vol. 3494, pp. 285–301. Springer, Heidelberg (2005)
4. Barnum, H., Knill, E.: Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.* 43, 2097 (2002)
5. Schumacher, B., Westmoreland, M.D.: Approximate quantum error correction. *Quantum Information Processing* 1(1-2), 5–12 (2002)
6. Mandayam, P., Poulin, D.: Approximate quantum error correction. In: *First International Conference on Quantum Error Correction* (2007)
7. Kretschmann, D., Kribs, D.W., Spekkens, R.W.: Complementarity of private and correctable subsystems in quantum cryptography and error correction. *Physical Review A* 78, 032330 (2008)
8. Knill, E., Laflamme, R.: Theory of quantum error-correcting codes. *Phys. Rev. A* 55, 900–911 (1997)
9. Kribs, D., Laflamme, R., Poulin, D.: Unified and generalized approach to quantum error correction. *Physical Review Letters* 94(18), 180501 (2005)
10. Beny, C., Kempf, A., Kribs, D.W.: Generalization of quantum error correction via the Heisenberg picture. *Phys. Rev. Lett.* 98(10), 100502 (2007)
11. Kuperberg, G.: The capacity of hybrid quantum memory. *IEEE Transactions on Information Theory* 49(6), 1465–1473 (2002)
12. Blume-Kohout, R., Ng, H.K., Poulin, D., Viola, L.: The structure of preserved information in quantum processes (2007), arXiv:0705.4282
13. Johnston, N., Kribs, D.W., Paulsen, V.I.: Computing stabilized norms for quantum operations via the theory of completely bounded maps (2007), arXiv:0711.3636
14. Beny, C.: Unsharp pointer observables and the structure of decoherence (2008), arXiv:0802.0685
15. Beny, C.: Information flow at the quantum-classical boundary. PhD in Applied Mathematics, Department of Applied Mathematics, University of Waterloo, Waterloo, ON, N2L 3G1 (2008)
16. Kribs, D.W., Laflamme, R., Poulin, D., Lesosky, M.: Operator quantum error correction. *Quantum Information and Computation* 6, 382–399 (2006)
17. Watrous, J.: Semidefinite programs for completely bounded norms (2009), arXiv:0901.4709
18. Bény, C., Oreshkov, O.: General conditions for approximate quantum error correction and near-optimal recovery channels (2009), arXiv:0907.5391

Optimal State Merging without Decoupling

Jean-Christian Boileau¹ and Joseph M. Renes²

¹ Center for Quantum Information and Quantum Control, University of Toronto

² Institut für Angewandte Physik, Technical University of Darmstadt

Abstract. We construct an optimal state merging protocol by adapting a recently-discovered optimal entanglement distillation protocol [Renes and Boileau, Phys. Rev. A. 73, 032335 (2008)]. The proof of optimality relies only on directly establishing sufficient “amplitude” and “phase” correlations between Alice and Bob and not on usual techniques of decoupling Alice from the environment. This strengthens the intuition from quantum error-correction that these two correlations are all that really matter in two-party quantum information processing.

1 Introduction

Quantum state merging is an important primitive protocol in the hierarchy of quantum communication protocols, also known as the quantum information family tree. Given two parties Alice and Bob and a mixed bipartite state ψ^{AB} , the goal of state merging is simply for Alice to send her half of the state to Bob. One option, of course, is to compress ψ^A into as few qubits as possible and send it over a quantum channel. However, this ignores the information Bob has about the state in the form of ψ^B . Although it might seem that a quantum channel is essential for state merging to work, Bob’s side information can be such that only *classical* communication from Alice is required.

Reasoning about the protocol is made somewhat easier by considering the purification $|\psi\rangle^{ABR}$ of ψ^{AB} to a reference system R , that is $\psi^{AB} = \text{Tr}_R [\psi^{ABR}]$. The goal of state merging is then to arrange for Bob to hold the purification of R . In some cases quantum communication will clearly be required, for instance when $|\psi\rangle^{ABR} = |\Phi\rangle^{AR}|\xi\rangle^B$, where $|\xi\rangle$ is arbitrary while $|\Phi\rangle^{AR} = \frac{1}{\sqrt{d}} \sum_k |k, k\rangle^{AR}$ is the canonical maximally entangled state for a fixed basis $\{|k\rangle\}$ and d is the minimum dimension of A and R . Bob’s state is clearly irrelevant, and Alice must simply send her whole system, as it is incompressible. On the other hand, when Alice and Bob share $|\Phi\rangle^{AB}$, no communication is required at all! This is simply due to the fact that now the state of R is by itself pure, so neither Alice nor Bob hold its purification.

Horodecki, Oppenheim, and Winter [1,2] consider the asymptotic setting of many copies of ψ^{ABR} and show that classical communication suffices when the quantum conditional entropy $S(A|B) = S(AB) - S(B)$ is negative, where $S(A) = -\text{Tr} [\rho^A \log_2 \rho^A]$ is the von Neumann entropy. In fact, when $S(A|B) < 0$ their state merging protocol produces entangled pairs at the rate $-S(A|B)$ and uses classical communication at the rate $I(A:R)$, where $I(A:R) = S(A) + S(R) -$

$S(AR)$ is the quantum mutual information. These rates are also shown to be optimal. When $S(A|B) > 0$ on the other hand, any state merging protocol requires quantum communication at the rate $S(A|B)$, or equivalently consumes entangled pairs at this rate. This fact gives an operational meaning to the conditional entropy in terms of entanglement consumption or production, which due to its possible negativity is quite unlike its classical counterpart.

In this paper we construct a state merging protocol operating at the optimal rates by focusing on the classical information that Bob has about complementary observables “amplitude” and “phase” on Alice’s system and showing how classical communication is sufficient to transfer the necessary quantum correlations. This approach is substantially different from the original proof, which is based on the technique of decoupling Alice’s system from the reference system R [3], and follows our recent work on entanglement distillation (ED) quite closely [4]. Indeed, state merging is actually achieved in that protocol as well, but at the cost of too much classical communication. We rectify this problem here, showing that if Alice first compresses her system and then runs the ED protocol, a small modification suffices to make this an optimal state merging protocol.

The remainder of the paper is outlined as follows. We first review the known results for the state merging protocol in the next section, and then recapitulate the important parts of the proof of the ED protocol appearing in [4] in the following section. Section 4 contains the new contribution of this paper, showing how to modify the ED protocol to use only the minimum necessary classical communication. Finally, we conclude with a summary of the results and comment on the connections to the quantum noisy channel coding theorem.

2 State Merging Defined

As with most protocols in quantum information theory, we are concerned here with the rate at which Alice and Bob can transform an asymptotically-large number of copies of the state $|\psi\rangle^{ABR}$ into a good approximation of n copies in which Bob holds system A . To keep the accounting simple, we assume that any necessary quantum communication is performed by teleportation through pre-shared entangled pairs, so that the protocol uses only classical communication in any case, and either produces or consumes entanglement depending on the circumstances. We then define an (n, ϵ) state merging protocol for ψ^{ABR} to be a series of local operations involving only classical communication (LOCC operations) such that application to $|\Psi\rangle^{ABR} = (|\psi\rangle^{ABR})^{\otimes n}$ produces an output Υ^{DBR} in which Bob holds the system D such that $\|\Upsilon^{DBR} - \Psi^{DBR}\|_1 \leq \epsilon$. If there exists an (n, ϵ_n) protocol using K_n bits of classical communication and consuming E_n ebits of entanglement for every n such that $\lim_{n \rightarrow \infty} \epsilon_n = 0$, then the rates of communication and entanglement consumption of the protocol are given by

$$R_K = \lim_{n \rightarrow \infty} \frac{K_n}{n} \quad \text{and} \quad R_E = \lim_{n \rightarrow \infty} \frac{E_n}{n}. \quad (1)$$

Horodecki, Oppenheim, and Winter showed in [1,2] that

$$\inf R_K = I(A:R) \quad \text{and} \quad \inf R_E = S(A|B), \quad (2)$$

where a negative R_E indicates the amount of entanglement produced. The proof of these statements has two parts, the direct part showing the rates are achievable, and the converse part showing they cannot be surpassed. Here we will give a new proof of the direct part, borrowing our techniques from [4] which were used to give a new proof of the hashing inequality [5] on the achievable rate of entanglement distillation. In the next section we sketch the important parts of that proof.

3 Entanglement Distillation Revisited

A maximally entangled pair is one for which Bob can predict the measurement of either of the two observables, “amplitude” $Z^A = \sum_k (-1)^k |k\rangle\langle k|^A$ and its Fourier conjugate “phase” $X = \sum_k |k \oplus 1\rangle\langle k|$. Here we are assuming that Alice’s system has dimension 2, but what follows can be easily extended to higher dimensions. Since this is the desired output of the distillation procedure, the idea behind the protocol given in Theorem 6 of [4] is to determine what information Bob already has about these observables from his system B and then arrange for Alice to send him the rest. This is classical information, since it refers to the measurement outcomes, and therefore only classical communication will be required. However, since Alice needs to send information pertaining to both X and Z , one must ensure that both parts of her message simultaneously exist. This is achieved by measuring the X - and Z -type stabilizers of a Calderbank-Shor-Steane (CSS) code [6,7,8] to generate the message. The amount of information is governed by the “static” version of the Holevo-Schumacher-Westmoreland (HSW) theorem [9,10], which solves the problem of classical data compression with quantum side information [11] and which we review in the appendix.

Greatly simplified, the protocol starts by Alice picking a random CSS code of a given size for her Hilbert space. She then measures the stabilizers to obtain the syndromes α (for X) and β (for Z) and communicates them to Bob. The syndromes are such that he can find measurements $\Lambda_{\alpha,x}^B$ and $\Gamma_{\beta,z}^B$ on B which enable him to predict (with high probability) the outcome of measuring either X^A or Z^A , respectively. The existence of such measurements is guaranteed by the (static) HSW theorem, using Bob’s marginal states generated by Alice’s measurement as the ensemble and the code syndrome as the side information. It implies that the CSS code must have roughly $m_Z = nS(Z^A|B)$ Z -type syndromes and $m_X = nS(X^A|CB)$ X -type, where C is an additional quantum register containing a copy of Alice’s system in the Z basis, and $S(Z^A|B) = S(\bar{\psi}_Z^{AB}) - S(\psi^B)$ for $\bar{\psi}_Z^{AB}$ the shared state after Alice measures the observable Z . Once this process is complete, Bob can (in principle) predict either X^A or Z^A on each pair, and therefore can perform a quantum operation on his systems to create entangled pairs (to good approximation). Since Alice is left with only the code subspace

given by α and β , whose size is $n - m_X - m_X$, this is the number of entangled pairs they can create.

To see how this works in more detail, begin with the individual shared state $|\psi\rangle^{ABR}$ and write it as $|\psi\rangle^{ABR} = \sum \sqrt{p_k} |k\rangle^A |\varphi_k\rangle^{BR}$, where $|k\rangle$ is the eigenbasis of ψ^A and also defines the operator Z , the $|\varphi_k\rangle$ are a set of arbitrary orthonormal states, and p_k is a probability distribution. The n -fold version $|\Psi_0\rangle^{ABR} = (|\psi\rangle^{ABR})^{\otimes n}$ we write like so, using bold-faced symbols $\mathbf{k}$ to denote strings $(k_1, k_2, \dots, k_n)$:

$$|\Psi_0\rangle^{ABR} = \sqrt{p_{\mathbf{k}}} \sum_{\mathbf{k}} |\mathbf{k}\rangle^A |\varphi_{\mathbf{k}}\rangle^{BR}. \quad (3)$$

We'll also need to consider the associated state in which Bob has a copy of Alice's system in the Z basis:

$$|\psi_c\rangle^{ACBR} = \sum_k \sqrt{p_k} |k, k\rangle^{AC} |\varphi_k\rangle^{BR} = \frac{1}{\sqrt{2}} \sum_x |\tilde{x}\rangle^A |\vartheta_x\rangle^{CBR}.$$

Here $|\tilde{x}\rangle$ is an eigenstate of X and the $|\vartheta_x\rangle$ are again a arbitrary set of orthonormal states. Observe that $|\vartheta_0\rangle^{CBR} = |\psi\rangle^{CBR}$.

Denote the projections onto the stabilizers of the chosen CSS code by $\tilde{\Pi}_\alpha^A$ and Π_β^A , which commute by the CSS nature of the code. The result of Alice measuring the stabilizers and sending them to Bob is

$$|\Psi_1\rangle^{ABRP} = \sum_{\alpha, \beta} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\Psi_0\rangle^{ABR} |\alpha, \beta\rangle^P. \quad (4)$$

The system label P , for “public”, is shorthand for having arbitrarily many copies $P_1, P_2, \dots$ of the values α, β , and mimics the information being classically-transmitted. Given β , Bob can coherently perform the measurement $\Gamma_{\beta, \mathbf{k}}^B$ to extract the value of k in A to an auxiliary system C with high probability. One can show that this implies the state is very nearly identical to

$$|\Psi_2\rangle = \sum_{\alpha, \beta, \mathbf{k}} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\mathbf{k}\mathbf{k}\rangle^{AC} |\varphi_{\mathbf{k}}\rangle^{BR} |\alpha, \beta\rangle^P = \sum_{\alpha, \beta} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\Psi_c\rangle |\alpha, \beta\rangle^P. \quad (5)$$

Next, Bob can coherently measure $\Lambda_{\alpha, \mathbf{x}}^B$ to extract $\mathbf{x}$ in the conjugate basis of A to a further auxiliary system D , again with high probability. The resulting state is nearly identical to

$$|\Psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{\alpha, \beta, \mathbf{x}} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\tilde{\mathbf{x}}\rangle^A |\tilde{\mathbf{x}}\rangle^D |\vartheta_{\mathbf{x}}\rangle^{CBR} |\alpha, \beta\rangle^P. \quad (6)$$

Owing to the properties of X and Z and the two forms of $|\psi_c\rangle$, we have the relation $|\vartheta_{\mathbf{x}}\rangle^{CBR} = \sum_{\mathbf{k}} \sqrt{p_{\mathbf{k}}} \omega^{\mathbf{k} \cdot \mathbf{x}} |\mathbf{k}\rangle^C |\varphi_{\mathbf{k}}\rangle^{BR} = (Z^{\mathbf{x}})^C |\Psi_0\rangle^{CBR}$. Inserting this into equation 6 gives

$$|\Psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{\alpha, \beta, \mathbf{x}} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\tilde{\mathbf{x}}\rangle^A |\tilde{\mathbf{x}}\rangle^D (Z^{\mathbf{x}})^C |\Psi_0\rangle^{CBR} |\alpha, \beta\rangle^P. \quad (7)$$

Finally, a controlled- Z operation from D to C inverts the $Z^{\mathbf{x}}$ operator, leaving the desired output

$$|\Psi_4\rangle = \sum_{\alpha, \beta, \mathbf{x}} \tilde{\Pi}_\alpha^A \Pi_\beta^A |\Phi_n\rangle^{AD} |\alpha, \beta\rangle^P \otimes |\Psi_0\rangle^{CBR}, \quad (8)$$

where $|\Phi_n\rangle = |\Phi\rangle^{\otimes n}$. Observe that the purification of R is now solely in Bob's possession, so state merging has been accomplished. Furthermore, since $n[S(Z^A|B) + S(X^A|CB)]$ CSS stabilizers leave $n[1 - S(Z^A|B) - S(X^A|CB)]$ encoded logical operators, Alice and Bob share this many entangled pairs in systems A and D . In [4] it is shown that this equals $-nS(A|B)$, so provided this quantity is positive ($S(A|B) < 0$), the protocol achieves the rate R_E .

Of course, $|\Psi_4\rangle$ is not precisely the output of the protocol, since the two coherent measurement operations by Bob were not perfect. The details of the approximation are given in [4], the result being that if Alice chooses a random code having $n[S(Z^A|B) + \delta]$ Z -type stabilizers and $n[S(X^A|CB) + \delta]$ X -type stabilizers for some $\delta > 0$, then the output will be within $\exp(-O(n\delta^2))$ of $|\Psi_4\rangle$, as measured by the trace-distance.

If $S(A|B) > 0$, we can use the same trick as [1,2]. Adding $n[S(A|B) + 2\delta]$ entangled pairs, each of which has $S(A|B) = -1$, the conditional entropy of the overall state $|\Psi\rangle^{ABR} |\Phi_{n[S(A|B)+2\delta]}^{A'B'}$ is $-2n\delta$. Using this as the individual input into the above protocol accomplishes the state merging and outputs no entanglement. In this way R_E can be achieved when $S(A|B) > 0$.

The above protocol requires too much classical communication, however, $n[1 - S(A|B)]$ bits. This is generally greater than $I(A:E)$, and is only equal for $S(A) = 1$. The fact that the protocol is optimal when ψ^A is maximally mixed suggests that for a general input Alice should first compress her system and then run the protocol. However, the compression procedure will disturb the conjugate observable X and its eigenbasis, so there is no longer any guarantee that Bob's $\Lambda_{\alpha, \mathbf{x}}$ measurement will work as intended. The next section shows how to fix this problem.

4 Classical Communication Reduced

Fortunately, the ensemble of states $\vartheta_{\mathbf{x}}^{CB}$ which Bob would like to distinguish is invariant under the action of the group $(Z^{\mathbf{x}})^C$, which will enable us to adapt the original $\Lambda_{\alpha, \mathbf{x}}$ measurement for use after Alice compresses her state. This will reduce the number of X syndromes she needs to communicate to Bob to the optimal level.

The modified protocol begins as before with the state $|\Psi_0\rangle$. Alice then makes a measurement projecting her system onto the typical subspace $\mathcal{T}_\delta^n$, which is the subspace spanned by eigenvectors $|\mathbf{k}\rangle$ whose $\mathbf{k}$ are in the typical set $T_\delta^n = \{\mathbf{k} : |-\frac{1}{n} \log p_{\mathbf{k}} - S(\psi^A)| \leq \delta\}$ for a fixed $\delta > 0$ [12,13]. The probability $\mathcal{N}_\delta^n = \Pr[\mathbf{k} \in T_\delta^n]$ that $\mathbf{k}$ is typical is greater than $1 - 2^{-cn\delta^2} := 1 - \epsilon$, for some constant c [5] and

therefore the projection succeeds with probability exponentially close to unity; otherwise the protocol aborts. When it succeeds, it *prunes* the state $|\Psi_0\rangle$, leaving

$$|\Psi'_0\rangle^{ABR} = \frac{1}{\sqrt{\mathcal{N}_\delta^n}} \sum_{\mathbf{k} \in T_\delta^n} \sqrt{p_{\mathbf{k}}} |\mathbf{k}\rangle^A |\varphi_{\mathbf{k}}\rangle^{BR} = \sum_{\mathbf{k} \in T_\delta^n} \sqrt{p'_{\mathbf{k}}} |\mathbf{k}\rangle^A |\varphi_{\mathbf{k}}\rangle^{BR}, \quad (9)$$

where we have implicitly defined new probability weights $p'_{\mathbf{k}} = p_{\mathbf{k}}/\mathcal{N}_\delta^n$. Importantly, $D_\delta^n := \dim(\mathcal{T}_\delta^n) \leq 2^{n[S(\psi^A) + \delta]}$, and a simple calculation shows that $\langle \Psi_0 | \Psi'_0 \rangle = \sqrt{\mathcal{N}_\delta^n}$. This implies that two states are close in trace distance, $\|\Psi_0 - \Psi'_0\|_1 \leq \sqrt{\epsilon}$, using the relationship between fidelity and trace distance $\|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)^2}$ [14].

The protocol proceeds just as before, measuring X' - and Z' -type stabilizers of a random CSS code on the pruned state and communicating the results to Bob. Here Z' is the analog of Z for the typical subspace, and X' is its Fourier conjugate. Now, however, we have no direct way of setting the number of stabilizers, since the state is no longer i.i.d. and therefore the HSW theorem no longer applies. This is not really a problem for the Z' -type stabilizers, since the typical projection is done in the $|\mathbf{k}\rangle$ basis, the basis which generates the $\varphi_{\mathbf{k}}^B$. By design, the measurement constructed in the HSW theorem does not attempt to identify $\varphi_{\mathbf{k}}^B$ for nontypical $\mathbf{k}$, so Bob can just reuse it in this case. The probability of error will only decrease by *explicitly* rejecting nontypical $\mathbf{k}$. Hence $m_z \approx nS(Z^A|B)$ as before.

However, the original measurement will not work for the conjugate basis $|\mathbf{x}'\rangle$, the Fourier transform of the typical subspace basis, since the states $\vartheta_{\mathbf{x}'}^{CB}$ have no *a priori* relation to the original $\vartheta_{\mathbf{x}}^{CB}$. However, the former states stem from the related state

$$|\Psi'_c\rangle = \sum_{\mathbf{k} \in T_\delta^n} \sqrt{p'_{\mathbf{k}}} |\mathbf{k}\mathbf{k}\rangle^{AC} |\varphi_{\mathbf{k}}\rangle^{BR} = \frac{1}{\sqrt{D_\delta^n}} \sum_{\mathbf{x}'} |\tilde{\mathbf{x}}'\rangle^A |\vartheta_{\mathbf{x}'}^{CB}\rangle^{CBR}, \quad (10)$$

and this fact, coupled with the group covariance of both sets, gives us a means to transform $A_{\alpha, \mathbf{x}}^{CB}$ into a measurement $A_{\alpha, \mathbf{x}'}^{CB}$ suitable for distinguishing the $\vartheta_{\mathbf{x}'}^{CB}$.

To see how this works, it is easiest to go back to the proof of the HSW theorem, which for convenience is stated in the appendix. In the original i.i.d. case, the projectors $P_{\mathbf{x}}$ and P^{CB} onto the typical subspaces of $\vartheta_{\mathbf{x}}^{CB}$ and $\bar{\vartheta}^{CB} = \frac{1}{2^n} \sum_{\mathbf{x}} \vartheta_{\mathbf{x}}^{CB}$, respectively, fulfill the five conditions needed in the proof of the theorem, equations 17 through 21. Since $\vartheta_{\mathbf{x}}^{CB} = (Z^{\mathbf{x}})^C \Psi_0^{CB} (Z^{\mathbf{x}})^C$, the same holds for $P_{\mathbf{x}}^{CB}$, and the five conditions become

$$\text{Tr}[\bar{\vartheta}^{CB} (P^{CB} - P^{CB})] \leq \epsilon \quad (11)$$

$$\text{Tr}[\Psi_0^{CB} (P^{CB} - P_0^{CB})] \leq \epsilon \quad (12)$$

$$P_0^{CB} \leq r \cdot \Psi_0^{CB} \quad (13)$$

$$\sum_{\mathbf{x}} \vartheta_{\mathbf{x}}^{CB} \leq d \cdot \bar{\vartheta}^{CB} \quad (14)$$

$$\|P^{CB} \bar{\vartheta}^{CB} P^{CB}\|_{\infty} \leq \lambda, \quad (15)$$

with $\epsilon =$, $r = 2^{n[S(\psi^{CB})+\delta]}$, $d = 2^n$ (and the condition is an equality since all $\mathbf{x}$ are typical), $\lambda = 2^{-n[S(\vartheta^{CB})-\delta]}$. Our aim is now to find a set of new projectors $P_{\mathbf{x}}'^{CB}$ and P'^{CB} fulfilling these conditions for the states $\vartheta_{\mathbf{x}'}'^{CB}$ and $\bar{\vartheta}'^{CB} = \frac{1}{D_\delta^n} \sum_{\mathbf{x}'} \vartheta_{\mathbf{x}'}'^{CB}$.

To start, use the fact that $\text{Tr}[(\Psi_0'^{CB} - \Psi_0^{CB})P_0^{CB}] \leq \|\Psi_0'^{CB} - \Psi_0^{CB}\|_1 \leq \sqrt{\epsilon}$, since the trace distance is equal to the maximum of the lefthand side, maximized over all projectors [8]. Then we have

$$\text{Tr}[(- P_0^{CB})\Psi_0'^{CB}] \leq \text{Tr}[(- P_0^{CB})\Psi_0^{CB}] + \|\Psi_0'^{CB} - \Psi_0^{CB}\|_1 \leq \epsilon + \sqrt{\epsilon},$$

and so we can define $P_{\mathbf{x}'}'^{CB} = (Z'^{\mathbf{x}})^C P_0^{CB} (Z^{\mathbf{x}})^C$ to satisfy the first condition. The second condition follows analogously upon noting that $\bar{\vartheta}^{CB} = \sum_{\mathbf{k}} p_{\mathbf{k}} |\mathbf{k}\rangle \langle \mathbf{k}|^C \otimes \varphi_{\mathbf{k}}^B$ (and similarly for the pruned version) and therefore $\|\bar{\vartheta}' - \bar{\vartheta}\| \leq 2(1 - \mathcal{N}_\delta^n) \leq 2\epsilon$. The third condition remains as is, since we're using the same P_0 , and the fourth is an equality when $d = D_\delta^n$. For the fifth condition, observe that

$$\frac{1}{\mathcal{N}_\delta^n} \bar{\vartheta}^{CB} - \bar{\vartheta}'^{CB} = \frac{1}{\mathcal{N}_\delta^n} \sum_{\mathbf{k} \notin T_\delta^n} p_{\mathbf{k}} |\mathbf{k}\rangle \langle \mathbf{k}|^C \otimes \varphi_{\mathbf{k}}^B \geq 0.$$

Therefore, $P^{CB} \bar{\vartheta}'^{CB} P^{CB} \leq \frac{1}{\mathcal{N}_\delta^n} P^{CB} \bar{\vartheta}^{CB} P^{CB}$, which leads immediately to $\|P^{CB} \bar{\vartheta}'^{CB} P^{CB}\|_\infty \leq \lambda / \mathcal{N}_\delta^n \leq \lambda(1 + 2\epsilon)$.

We thus have all the ingredients needed to construct the required measurement, with $\epsilon' = 2\sqrt{\epsilon}$, $r' = r$, $d' = D_\delta^n$, and $\lambda' = \lambda(1 + 2\epsilon)$. The number of syndromes Bob needs from Alice is given by $m'_X \geq n[S(\psi^{AB}) + S(\psi^A) - S(\vartheta^{CB}) + 3\delta] + \log(1 + 2\epsilon)$, which works out to be $m'_X \approx n[S(\psi^R) - \sum_k p_k S(\varphi_k^R)]$. Since the pruned state is nearly identical to the original state, the remainder of the protocol goes through as before, outputting roughly $nS(A) - m_Z - m'_X$ entangled pairs. A simple calculation (along the lines of lemma 2 in [4]) gives $m'_X + m_Z = I(A:E)$ and $nS(A) - m'_X - m_Z = -S(A|B)$, and thus the protocol is optimal.

5 Conclusion

We have shown how to construct an optimal state merging protocol by following the intuition from quantum error-correction that what really matters in two-party quantum information processing is information about amplitude and phase measurements. Combining entanglement distillation with teleportation, our results also imply a new proof of the direct part of the noisy channel coding theorem [5], one not following the usual route of decoupling Alice's system from the purification R (e.g. all the fully fleshed-out proofs to date [15,16,17,18,19]). It would be interesting to apply these techniques to more protocols, and see how far this intuition about quantum information extends.

Acknowledgments. JMR received support from the European IST project SECOQC and JCB from Quantumworks and the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

1. Horodecki, M., Oppenheim, J., Winter, A.: *Nature* 436(7051), 673–676 (2005)
2. Horodecki, M., Oppenheim, J., Winter, A.: *Communications in Mathematical Physics* 269(1), 107–136 (2007)
3. Schumacher, B., Westmoreland, M.D.: *Quantum Information Processing*, vol. 1, pp. 5–12 (2002)
4. Renes, J.M., Boileau, J.-C.: *Physical Review A* 78(3), 032335–12 (2008)
5. Devetak, I., Winter, A.: *Proceedings of the Royal Society A* 461(2053), 207–235 (2053)
6. Calderbank, A.R., Shor, P.W.: *Physical Review A* 54(2), 1098 (1996)
7. Steane, A.: *Proceedings of the Royal Society A* 452(1954), 2551–2577 (1996)
8. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
9. Holevo, A.: *IEEE Transactions on Information Theory* 44(1), 269–273 (1998)
10. Schumacher, B., Westmoreland, M.D.: *Physical Review A* 56(1), 131 (1997)
11. Devetak, I., Winter, A.: *Physical Review A* 68(4), 042301 (2003)
12. Schumacher, B.: *Physical Review A* 51(4), 2738 (1995)
13. Cover, T.M., Thomas, J.A.: *Elements of Information Theory*, 2nd edn. Wiley-Interscience, Hoboken (2006)
14. Fuchs, C., van de Graaf, J.: *IEEE Transactions on Information Theory* 45(4), 1216–1227 (1999)
15. Devetak, I.: *IEEE Transactions on Information Theory* 51(1), 44–55 (2005)
16. Hayden, P., Horodecki, M., Winter, A., Yard, J.: *Open Systems & Information Dynamics* 15(1), 7–19 (2008)
17. Klesse, R.: *Open Systems & Information Dynamics* 15(1), 24–45 (2008)
18. Horodecki, M., Lloyd, S., Winter, A.: *Open Systems & Information Dynamics* 15(1), 47–69 (2008)
19. Hayden, P., Shor, P.W., Winter, A.: *Open Systems & Information Dynamics* 15(1), 71–89 (2008)
20. Carter, J.L., Wegman, M.N.: *Journal of Computer and System Sciences* 18(2), 143–154 (1979)
21. Hsieh, M., Devetak, I., Winter, A.: *IEEE Transactions on Information Theory* 54(7), 3078–3090 (2008)

A Static HSW Theorem

Here we are interested in the “static” setting of the HSW theorem, which is concerned with the following. Given n samples from an ensemble $\{p_k, \rho_k\}_{k=1}^d$ with average $\rho = \sum_k p_k \rho_k$, what is the smallest amount of side information $t = f(\mathbf{k})$ required in order to reliably construct a measurement $A_{t, \mathbf{k}}$ which will identify $\mathbf{k}$ from $\rho_{\mathbf{k}}$ with only a small probability of error? In order to match the setting in the main text, we can think of the ensemble as arising from the state $\psi^{AB} = \sum_k p_k |k\rangle \langle k|^A \otimes \rho_k^B$, a measurement of $|k\rangle$ (or Z^A) on A generating state ρ_k . For random CSS codes f is a random linear function, resulting from measuring the stabilizer observables on the state $|\mathbf{k}\rangle$. However, in what follows we will consider *universal hashing* [20], since it is no more difficult to do so. In universal (or 2-universal) hashing, the function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ generating

the side information is chosen at random from a universal family of hash functions in which the probability of collision $f(x) = f(y)$ but $x \neq y$ is the same as for random functions: $\Pr_f[f(x) = f(y)|x \neq y] \leq 1/2^m$.

In [4] we proved that for a fixed $\delta > 0$, choosing $m = n[S(Z^A|B) + 4\delta]$ is sufficient to guarantee the existence of a measurement having elements $\Lambda_{f(\mathbf{k}),\ell}$ such that the probability of error P_e is exponentially small (see also [11]):

$$P_e = \left\langle \sum_{\ell \neq \mathbf{k}} [\Lambda_{f(\mathbf{k}),\ell} \rho_{\mathbf{k}}] \right\rangle_{f,\mathbf{k}} \leq 6 \times 2^{-n\delta^2/2}. \quad (16)$$

A crucial step in the proof is to show the existence of projectors $Q_{\mathbf{k}}$ and Q such that

$$\text{Tr}[\langle \rho_{\mathbf{k}} \rangle_{\mathbf{k}} (-Q)] \leq \epsilon \quad (17)$$

$$\langle \text{Tr}[\rho_{\mathbf{k}} (-Q_{\mathbf{k}})] \rangle_{\mathbf{k}} \leq \epsilon \quad (18)$$

$$Q_{\mathbf{k}} \leq r \cdot \rho_{\mathbf{k}} \quad (19)$$

$$\sum_{\mathbf{k} \in T_{\delta}^n} \rho_{\mathbf{k}} \leq d \cdot \langle \rho_{\mathbf{k}} \rangle_{\mathbf{k}} \quad (20)$$

$$\|Q \langle \rho_{\mathbf{k}} \rangle_{\mathbf{k}} Q\|_{\infty} \leq \lambda, \quad (21)$$

after which it can be shown that $m \geq \lfloor \frac{1}{\gamma} \log r d \lambda \rfloor$ for $0 \leq \gamma \leq 1$ suffices to construct the measurement.¹ In the i.i.d. case of the HSW theorem, the $Q_{\mathbf{k}}$ and Q are projectors onto the typical subspaces of $\rho_{\mathbf{k}}$ (for typical $\mathbf{k}$) and $\rho^{\otimes n}$, respectively, for which $\epsilon = 2^{-cn\delta^2}$, $r = 2^{n[\sum_k p_k S(\rho_k) + \delta]}$, $d = 2^{n[H(p_k) + \delta]}$, and $\lambda = 2^{-n[S(\rho) - \delta]}$. Thus, one chooses $m \geq n[H(p_k) - S(\rho) + \sum_k p_k S(\rho_k) + 4\delta] = n[S(Z^A|B) + 4\delta]$.

¹ Breaking up the proof in this way is similar to the packing lemma of [21].

Optimal Trading of Classical Communication, Quantum Communication, and Entanglement

Min-Hsiu Hsieh¹ and Mark M. Wilde^{2,3}

¹ ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan

² Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

³ Science Applications International Corporation, Electronic Systems Division, 4001 North Fairfax Drive, Arlington, Virginia, USA 22203

Abstract. We provide a solution for the most general setting of information processing in the quantum Shannon-theoretic sense by giving optimal trade-offs between classical communication, quantum communication, and entanglement. We begin by showing that a combination of teleportation, superdense coding, and entanglement distribution is the optimal strategy for transmission of information when only the three noiseless resources of classical communication, quantum communication, and entanglement are available. Next, we provide a solution for the scenario where a large number of copies of a noisy bipartite state are available (in addition to consumption or generation of the above three noiseless resources). The coding strategy is an extension of previous techniques in the quantum Shannon-theoretic literature. We finally provide a solution to the scenario where a large number of uses of a noisy quantum channel are available in addition to the consumption or generation of the three noiseless resources. The coding strategy here is the classically-enhanced father protocol, a protocol which we discussed in a previous paper. Our results are of a “multi-letter” nature, meaning that there might be room for improvement in the coding strategies presented here.

Keywords: Quantum Shannon theory, triple trade-off, resource inequalities, quantum communication, entanglement, and channel capacity.

1 Introduction

The recent development of quantum information theory marks an improved understanding of information processing systems. Three resources are essential in any quantum information processing system: the classical bit, the quantum bit, and the entangled bit—we abbreviate these respective resources as the *cbit*, the *qubit*, and the *ebit*. Shannon developed an informational notion of a bit that measures the uncertainty of a classical register [1]. Much later, Schumacher followed with an analogous informational notion of a quantum bit [2]. The Schumacher qubit measures how much quantum information a given quantum register possesses. Finally, in a seminal paper, several authors developed an informational

notion of strong quantum correlations, known as entanglement, that two quantum systems in a pure state can share [3]. These three noiseless resources are the most crucial for basic quantum information processing tasks such as superdense coding [4], teleportation [5], and more complicated schemes involving noisy resources [6].

Shannon developed classical information theory in order to quantify the amount of information in a classical system and to determine how one might optimally convert resources between two non-local classical systems [1]. The interconversion problems fall into one of two categories: *static* or *dynamic*. Suppose that two spatially separated parties possess a correlated noisy resource described by random variables X and Y with joint probability density $p_{X,Y}(x,y)$ (one party possesses X and the other possesses Y). The static problem considers how they might transform the noisy resource to perfectly correlated uniform random variables X and Y with joint probability distribution $\frac{1}{d}\delta(x,y)$ where d is the dimension of both random variables [7]. The two parties can then exploit these noiseless correlations in later classical information processing protocols. Suppose next that a noisy channel, described by the conditional probability density $p_{Y|X}(y|x)$, connects two spatially separated parties. That is, the channel outputs a random variable Y to the receiver if the sender inputs a random variable X to it. The goal in the dynamic setting is to transform the noisy dynamic resource $p_{Y|X}(y|x)$ to a noiseless dynamic resource by employing a clever coding strategy [1]. The two parties can then use the channel for reliable classical communication. The above static and dynamic protocols represent a broad class of information interconversions for the classical setting of information processing.

Quantum information theory attempts to solve interconversion problems between non-local quantum systems just as classical information theory does [6]. Though, there is a significant increase of noiseless resources, from cbits in the classical setting to cbits, qubits, and ebits in the quantum setting. This increase implies that a general theory for the static and dynamic case in the quantum setting should be richer than it is in the classical setting. The static noisy resource that the sender Alice and receiver Bob may share is a shared noisy bipartite state ρ^{AB} , described mathematically as a unit trace, positive linear operator acting on the tensor product of two Hilbert spaces A and B [8]. The dynamic noisy resource is a noisy quantum channel $\mathcal{N}^{A' \rightarrow B}$ that connects Alice to Bob, described mathematically by a linear superoperator that acts on the space of density operators [8]. Both of these resources are natural quantum extensions of their classical counterparts given in the previous paragraph. Ref. [6] provides an excellent, up-to-date summary of progress in quantum Shannon theory.

Our understanding of quantum interconversion problems, as of Ref. [6], is limited to optimal trade-offs that involve only one or two noiseless resources, together with one noisy static or dynamic resource. In this paper, we push the results of Ref. [6] further by attacking the full triple trade-off problems for both the static and dynamic setting—that is, we give the trade-offs between the three fundamental noiseless resources when a sender and receiver possess either a static or dynamic noisy resource. This work is the most general scenario considered so

far, when the protocol consists of a single sender and a single receiver, and the quantum state or channel is independent and identically distributed (IID). Previous results from Ref. [6] are all special cases of the present work. We appeal to the asymptotic setting where a large number of independent copies or uses of the respective static or dynamic noisy resource are available. For both the static and dynamic scenarios, we assume that the sender and receiver either consume or generate noiseless classical communication, noiseless quantum communication, and noiseless entanglement in addition to the consumption of the noisy resource. The result is a three-dimensional capacity region that gives the optimal trade-offs for the three noiseless resources in both the static and dynamic scenarios. The rate of a noiseless resource is negative if a protocol consumes the corresponding resource and its rate is positive if a protocol generates the resource. The present paper’s full solution for the static and dynamic scenarios contains both negative and positive rates.

Our current formulas characterizing the triple trade-off capacity regions are alas of a “multi-letter” nature, a problem that plagues many results in quantum Shannon theory. A multi-letter formula is one that involves an intractable optimization over an arbitrary number of uses of a channel or a state, as opposed to a more desirable “single-letter” formula that involves a tractable optimization over a single use of a channel or state. In principle, a multi-letter characterization is an optimal solution, but the multi-letter nature of our characterization of the capacity region implies that there may be a slight room for improvement in the formulas when considering an optimization over a finite number of uses—sometimes suboptimal protocols can lead to an optimal characterization of a capacity region when taking the limit over an arbitrary number of uses of a channel or a state. It is part of our ongoing investigation to find examples of channels or states that admit a single-letter characterization and give further credence to the suggestion that our formulas given here are indeed optimal.

We structure this paper as follows. We first consider communication involving the three noiseless resources only. The result is that the optimal strategy is a combination of teleportation, super-dense coding, and entanglement distribution (defined in the next section). Then we give the triple trade-off solution for the static case and follow with that for the dynamic case. The full proofs for the theorems in this article are available as a preprint [9].

2 The Triple Trade-Off between Unit Resources

We first establish some notation for the rest of the paper. The three fundamental noiseless resources are noiseless classical communication, noiseless quantum communication, and noiseless entanglement. Let $[c \rightarrow c]$ denote the resource of one *cbit* of noiseless forward classical communication, let $[q \rightarrow q]$ denote the resource of one *qubit* of noiseless forward quantum communication, and let $[qq]$ denote the resource of one *ebit* of shared noiseless entanglement. The ebit is a maximally entangled state $|\Phi^+\rangle^{AB} \equiv (|00\rangle^{AB} + |11\rangle^{AB})/\sqrt{2}$. The ebit $[qq]$ is a unit static resource and both the cbit $[c \rightarrow c]$ and the qubit $[q \rightarrow q]$ are unit dynamic resources.

We now consider what rates are achievable when there is no noisy resource—the only resources available are noiseless classical communication, noiseless quantum communication, and noiseless entanglement. The result is a three-dimensional “unit resource” capacity region in a three-dimensional space whose points are rate triples (R, Q, E) . R represents the rate of classical communication, Q the rate of quantum communication, and E the rate of entanglement consumption or generation.

Three important protocols relate the three fundamental noiseless resources. These protocols are teleportation (TP) [5], super-dense coding (SD) [4], and entanglement distribution (ED) [10]. We can express these three protocols as resource inequalities. The resource inequality for teleportation is

$$2[c \rightarrow c] + [qq] \geq [q \rightarrow q], \quad (1)$$

where the meaning of the resource inequality is that the protocol consumes the resources on the left in order to produce the resource on the right. Super-dense coding corresponds to the following inequality:

$$[q \rightarrow q] + [qq] \geq 2[c \rightarrow c], \quad (2)$$

and entanglement distribution is as follows:

$$[q \rightarrow q] \geq [qq]. \quad (3)$$

In any trade-off problem, we have the achievable region and the capacity region. The achievable region is the set of all rate triples that one can achieve with a specific, known protocol. The capacity region divides the line between what is physically achievable and what is not—there is no method to achieve any point outside the capacity region. We define it with respect to a given quantum information processing task. In our development below, we consider the achievable region and the capacity region of the three unit resources of noiseless classical communication, noiseless quantum communication, and noiseless entanglement.

Definition 1. Let $\tilde{C}_U$ denote the unit resource achievable region. It consists of all the rate triples (R, Q, E) obtainable from linear combinations of the above protocols: TP, SD, and ED.

We can further show that the achievable region $\tilde{C}_U$ in the above definition is equivalent to all rate triples satisfying the following inequalities [9]:

$$R + Q + E \leq 0, \quad Q + E \leq 0, \quad \frac{1}{2}R + Q \leq 0. \quad (4)$$

Definition 2. The unit resource capacity region C_U is the closure of the set of all points (R, Q, E) in the R, Q, E space satisfying the following resource inequality:

$$0 \geq R[c \rightarrow c] + Q[q \rightarrow q] + E[qq]. \quad (5)$$

The above notation may seem confusing at first glance until we establish the convention that a resource with a negative rate implicitly belongs on the left-hand side of the resource inequality.

Theorem 1 below gives the optimal three-dimensional capacity region for the three unit resources.

Theorem 1. *The unit resource capacity region C_U is equivalent to the unit resource achievable region $\tilde{C}_U$: $C_U = \tilde{C}_U$.*

The complete proof is available in Ref. [9]. It involves several proofs by contradiction that apply to each octant of the (R, Q, E) space, using the postulates that ebits alone cannot generate cbits or qubits and cbits alone cannot generate ebits or qubits.

3 Direct Static Trade-Off

The main result of this section provides a solution to the scenario when a noisy static resource is available in addition to the three noiseless resources. We give a three-dimensional “direct static” capacity region with the full trade-off between the three fundamental noiseless resources.

Definition 3. *The direct static capacity region $C_{DS}(\rho^{AB})$ of a noisy bipartite state ρ^{AB} is a three-dimensional region in the (R, Q, E) space. It is the closure of the set of all points (R, Q, E) satisfying the following resource inequality:*

$$\langle \rho^{AB} \rangle \geq R[c \rightarrow c] + Q[q \rightarrow q] + E[qq]. \quad (6)$$

The rates R , Q , and E can either be negative or positive with the same interpretation as in the previous section. We first introduce a new protocol that we name “classically-assisted quantum state redistribution.” It proves to be useful in determining the achievable region for the static case.

Theorem 2. *The following “classically-assisted quantum state redistribution” resource inequality holds*

$$\begin{aligned} \langle \rho^{AB} \rangle + \frac{1}{2} I(A'; E|E'X)_\sigma [q \rightarrow q] + I(X; E|B)_\sigma [c \rightarrow c] \\ \geq \frac{1}{2} (I(A'; B|X)_\sigma - I(A'; E'|X)_\sigma) [qq] \end{aligned} \quad (7)$$

for a static resource ρ^{AB} and for any remote instrument $\mathcal{T}^{A \rightarrow A'X}$. In the above resource inequality, the state $\sigma^{XA'BEE'}$ is defined by $\sigma^{XA'BEE'} \equiv \tilde{\mathcal{T}}(\psi^{ABE})$, where $|\psi\rangle\langle\psi|^{ABE}$ is some purification of ρ^{AB} and $\tilde{\mathcal{T}}^{A \rightarrow A'X}$ is an isometric extension of $\mathcal{T}^{A \rightarrow A'X}$.

The above quantities $I(A'; E|E'X)_\sigma$, $I(X; E|B)_\sigma$, and $I(A'; B|X)_\sigma - I(A'; E'|X)_\sigma$ are entropic quantities that are taken with respect to the state

$\sigma^{XA'BEE'}$. These quantities give the rates of resource consumption or generation in the above protocol. We refer the reader to Refs. [6,11] for definitions of the above entropic quantities and the definition of a “quantum instrument.” The above protocol generalizes the mother protocol [6], noisy teleportation [6], noisy super-dense coding [6], the entanglement distillation protocol [12], and the grandmother protocol [6].

Definition 4. *The classically-assisted state redistribution “one-shot” achievable region $\tilde{C}_{\text{CASR}}^{(1)}(\rho^{AB})$ is as follows:*

$$\bigcup_{\tilde{T}} \left(-I(X; E|B)_\sigma, -\frac{1}{2}I(A'; E|E'X)_\sigma, \frac{1}{2}(I(A'; B|X)_\sigma - I(A'; E'|X)_\sigma) \right),$$

where σ is defined as above and the union is over all instruments $\tilde{T}$. The classically-assisted state redistribution achievable region $\tilde{C}_{\text{CASR}}(\rho^{AB})$ is the following multi-letter regularization of the one-shot region:

$$\tilde{C}_{\text{CASR}}(\rho^{AB}) \equiv \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \tilde{C}_{\text{CASR}}^{(1)}((\rho^{AB})^{\otimes k})}. \quad (8)$$

Theorem 3. *The classically-assisted state redistribution capacity region $C_{\text{CASR}}(\rho^{AB})$ is equivalent to the classically-assisted state redistribution achievable region $\tilde{C}_{\text{CASR}}(\rho^{AB})$: $C_{\text{CASR}}(\rho^{AB}) = \tilde{C}_{\text{CASR}}(\rho^{AB})$.*

A full proof is in Ref. [9].

Below we state this section’s main theorem, the direct static capacity theorem.

Theorem 4. *The direct static capacity region $C_{\text{DS}}(\rho^{AB})$ is equivalent to the direct static achievable region $\tilde{C}_{\text{DS}}(\rho^{AB})$: $C_{\text{DS}}(\rho^{AB}) = \tilde{C}_{\text{DS}}(\rho^{AB})$. The direct static achievable region $\tilde{C}_{\text{DS}}(\rho^{AB})$ is the set addition of the classically-assisted state redistribution achievable region $\tilde{C}_{\text{CASR}}$ and the unit resource achievable region $\tilde{C}_{\text{U}}$: $\tilde{C}_{\text{DS}}(\rho^{AB}) \equiv \tilde{C}_{\text{CASR}}(\rho^{AB}) + \tilde{C}_{\text{U}}$. The “set addition” operation between two regions A and B is defined as*

$$A + B \equiv \{a + b : a \in A, b \in B\}.$$

The complete proof is available in Ref. [9]. The meaning of the theorem is that it is possible to obtain all achievable points in the direct-static capacity region by combining only four protocols: classically-assisted state redistribution, SD, TP, and ED.

4 Direct Dynamic Trade-Off

The main result of this section is a three-dimensional “direct dynamic” capacity region that gives the full trade-off between the three fundamental noiseless resources when a noisy dynamic resource is available.

Definition 5. The direct dynamic capacity region $C_{\text{DD}}(\mathcal{N})$ of a noisy channel $\mathcal{N}^{A' \rightarrow B}$ is a three-dimensional region in the (R, Q, E) space defined by the closure of the set of all points (R, Q, E) satisfying the following resource inequality:

$$\langle \mathcal{N} \rangle \geq R[c \rightarrow c] + Q[q \rightarrow q] + E[qq]. \quad (9)$$

We first recall a few theorems concerning the classically-enhanced father protocol [11] because this protocol proves useful in determining the achievable region for the dynamic case. Briefly, the classically-enhanced father protocol is an optimal protocol for the simultaneous transmission of classical and quantum information with an entanglement-assisted quantum channel.

Theorem 5. The following classically-enhanced father resource inequality holds

$$\langle \mathcal{N} \rangle + \frac{1}{2}I(A; EE'|X)_\sigma[qq] \geq \frac{1}{2}I(A; B|X)_\sigma[q \rightarrow q] + I(X; B)_\sigma[c \rightarrow c], \quad (10)$$

for a noisy dynamic resource $\mathcal{N}^{A' \rightarrow B}$. In the above resource inequality, the state $\sigma^{XABEE'}$ is defined as follows

$$\sigma^{XABEE'} \equiv \sum_x p(x) |x\rangle \langle x|^X \otimes U_{\mathcal{N}}(\psi_x^{AA'E'}), \quad (11)$$

where the states $\psi_x^{AA'E'}$ are pure and $U_{\mathcal{N}}^{A' \rightarrow BE}$ is an isometric extension of $\mathcal{N}$.

The classically-enhanced father protocol generalizes the father protocol [6], classically-enhanced quantum communication [13], entanglement-assisted classical communication [14], classical communication [15,16], and quantum communication [17,18,19].

Definition 6. The “one-shot” classically-enhanced father achievable region $\tilde{C}_{\text{CEF}}^{(1)}(\mathcal{N})$ is as follows:

$$\tilde{C}_{\text{CEF}}^{(1)}(\mathcal{N}) \equiv \bigcup_{\sigma} \left(I(X, B)_\sigma, \frac{1}{2}I(A; B|X)_\sigma, -\frac{1}{2}I(A; EE'|X)_\sigma \right),$$

where σ is defined in (11). The classically-enhanced father achievable region $\tilde{C}_{\text{CEF}}(\mathcal{N})$ is the following multi-letter regularization of the one-shot region:

$$\tilde{C}_{\text{CEF}}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \tilde{C}_{\text{CEF}}^{(1)}(\mathcal{N}^{\otimes k})}.$$

Theorem 6. The classically-enhanced father capacity region $C_{\text{CEF}}(\mathcal{N})$ is equivalent to the classically-enhanced father achievable region: $C_{\text{CEF}}(\mathcal{N}) = \tilde{C}_{\text{CEF}}(\mathcal{N})$.

We now state this section’s main theorem, the direct dynamic capacity theorem.

Theorem 7. *The direct dynamic capacity region $C_{\text{DD}}(\mathcal{N})$ is equivalent to the direct dynamic achievable region $\tilde{C}_{\text{DD}}(\mathcal{N})$: $C_{\text{DD}}(\mathcal{N}) = \tilde{C}_{\text{DD}}(\mathcal{N})$. The direct dynamic achievable region $\tilde{C}_{\text{DD}}(\mathcal{N})$ is the set addition of the classically-enhanced father achievable region and the unit resource achievable region:*

$$\tilde{C}_{\text{DD}}(\mathcal{N}) \equiv \tilde{C}_{\text{CEF}}(\mathcal{N}) + \tilde{C}_{\text{U}}. \quad (12)$$

The complete proof is available in Ref. [9]. The meaning of the theorem is that it is possible to obtain all achievable points in the direct-dynamic capacity region by combining only four protocols: the classically-enhanced father protocol, super-dense coding, teleportation, and entanglement distribution.

5 Conclusion

We have provided a unifying treatment of many of the important results in quantum Shannon theory. Our first result is a solution of the unit resource capacity region—the optimal strategy mixes super-dense coding, teleportation, and entanglement distribution. Our next result is the full triple trade-off for the static scenario where a sender and receiver share a noisy bipartite state. The optimal strategy combines classically-assisted state redistribution with the three unit protocols. Our last result is a solution of the direct dynamic capacity theorem—the scenario where a sender and receiver have access to a large number of independent uses of a noisy quantum channel. The optimal strategy combines the classically-enhanced father protocol with the three unit protocols. Our formulas are of a multi-letter nature, implying that the coding strategies may have room for improvement.

Acknowledgements

The authors thank I. Devetak, P. Hayden, and D. Leung for initial discussions during the development of this project. M.M.W. acknowledges support from the National Research Foundation & Ministry of Education, Singapore and support from a grant of SAIC.

References

1. Shannon, C.E.: A mathematical theory of communication. Bell System Technical Journal 27, 379–423, 623–656 (1948)
2. Schumacher, B.: Quantum coding. Physical Review A 51, 2738–2747 (1995)
3. Bennett, C.H., Bernstein, H.J., Popescu, S., Schumacher, B.: Concentrating partial entanglement by local operations. Physical Review A 53, 2046–2052 (1996)
4. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters 69, 2881–2884 (1992)
5. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters 70, 1895–1899 (1993)

6. Devetak, I., Harrow, A.W., Winter, A.: A resource framework for quantum shannon theory. *IEEE Transactions on Information Theory* 54(10), 4587–4618 (2008)
7. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography – part II: Cr-capacity. *IEEE Transactions on Information Theory* 44, 225–240 (1998)
8. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, New York (2000)
9. Hsieh, M.-H., Wilde, M.M.: Trading classical communication, quantum communication, and entanglement in quantum shannon theory. *arXiv:0901.3038* (2009)
10. Devetak, I., Harrow, A.W., Winter, A.J.: A family of quantum protocols. *Physical Review Letters* 93, 239503 (2004)
11. Hsieh, M.-H., Wilde, M.M.: The classically-enhanced father protocol. *arXiv:0811.4227* (2008)
12. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Woiters, W.K.: Mixed state entanglement and quantum error correction. *Physical Review A* 54, 3824–3851 (1996)
13. Devetak, I., Shor, P.W.: The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics* 256(2), 287–303 (2005)
14. Shor, P.W.: The classical capacity achievable by a quantum channel assisted by limited entanglement (2004), *quant-ph/0402129*
15. Holevo, A.S.: The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory* 44, 269–273 (1998)
16. Schumacher, B., Westmoreland, M.D.: Sending classical information via noisy quantum channels. *Physical Review A* 56, 131–138 (1997)
17. Lloyd, S.: The capacity of a noisy quantum channel. *Physical Review A* 55, 1613–1622 (1997)
18. Shor, P.W.: The quantum channel capacity and coherent information. In: *MSRI workshop on quantum computation* (2002)
19. Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory* 51(1), 44–55 (2005)

On the Power of the PPT Constraint in the Symmetric Extensions Test for Separability

Miguel Navascués¹, Masaki Owari^{1,2}, and Martin B. Plenio^{1,2,3}

¹ Institute for Mathematical Sciences, 53 Prince's Gate, Imperial College London, London SW7 2PG, UK

² QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, UK

³ Institut für Theoretische Physik, Universität Ulm, D-89081 Ulm, Germany

Abstract. In this paper, we analyze the efficiency of entanglement criteria based on symmetric extensions and PPT symmetric extensions to solve the weak membership problem of separability $WEMP(S)$. We observe that the set of states admitting an N -PPT symmetric extension converges to the set of all separable states quadratically faster than the set of states admitting a general N -symmetric extension. As a result, we show that the PPT constraint in the symmetric extensions criterion reduces the dominant factor on time complexity from $(k_1/\delta)^{6d_B}$ to $(k_2/\delta)^{4d_B}$, where δ is the accuracy parameter of $WEMP(S)$.

1 Introduction

The separability problem is the problem of determining whether a given quantum state is entangled or separable. This problem is one of the central topics of quantum information theory, and a great effort has been devoted to find efficient ways to solve it [1,2,3,4,5,6]. In particular, Computer Science-based approaches to this problem have attracted attention in recent years, the proof of the NP hardness of separability problem being one of the most astounding achievements in this direction [7,8,9].

There are several different ways to state the separability problem as a computational problem. Among them, we will focus on a promise problem called the weak membership problem of separability ($WMEM(S)$). In $WMEM(S)$, the goal is to determine the separability of a given state with admissible error δ . More specifically, for a given state ρ , we have to assert either that ρ is in the δ -neighbor of a set of all separable states, or that there is an entangled state in the δ -neighbor of ρ .

Several different algorithms are known for $WMEM(S)$ [9,10,11,12]. Among them, those with shorter running time are the Semidefinite Programming (SDP)-based symmetric extensions criterion by Doherty et al. [11,12], a large SDP method by Perez-García et al., and an interior-point cutting-plane algorithm by Ioannou et al. [9]. The last two algorithms are based on an entanglement-witness search that uses an ϵ -net of the set of all pure states. Among these three, the algorithm based on the symmetric extension test may be the most well known and most popular algorithm, since it is easy to implement and also physically intuitive. This is thus the algorithm we will study in this paper.

In [11,12], Doherty et al. predicted that we may accelerate the symmetric extension test by adding the so called Positive Partial Transpose (PPT) constraint. But so far no one has succeeded in proving this fact. Even though Ioannou derived in [9] an upper bound on the time-complexity of the symmetric extensions test by means of the finite Quantum de Finetti theorem [13,14], no better upper bound is known for the PPT symmetric extension test. Actually, by adding the PPT constraint, the main matrix of the SDP becomes quadratically larger than the original one. Since a larger matrix constraint may be a factor that contributes towards slowing down the algorithm, it is a highly non-trivial problem whether this constraint indeed accelerates the algorithm.

In this paper, we analyze the performance of the test based on symmetric extensions with and without the PPT constraint. As a result, we derive an upper bound on the time-complexity for the PPT symmetric extensions test that outperforms the corresponding upper bound for the method based on plain symmetric extensions. Moreover, concerning the latter test, we improve the upper bound derived by Ioannou.

The structure of this paper is as follows: after introducing WMEM(S) and the (PPT) symmetric extension in Section 2, we derive a lemma characterizing the noise needed to destroy the entanglement of a state admitting an N symmetric extension (Lemma 1). This lemma allows us to calculate an upper bound on the time-complexity of the method based on plain symmetric extensions. In Section 3, we extend this lemma for the PPT symmetric extensions test (Lemma 2) and derive an upper bound on its time-complexity. Finally, in section 4, we present the conclusions of this paper.

2 The Weak Membership Problem of Separability and the Symmetric Extensions Test

At the beginning of this section, we give some remarks about notation. In this paper, we will be mainly concerned with a finite dimensional bipartite Hilbert space $\mathcal{H} \stackrel{\text{def}}{=} \mathcal{H}_A \otimes \mathcal{H}_B$. We define d_A and d_B as $d_A \stackrel{\text{def}}{=} \dim \mathcal{H}_A$ and $d_B \stackrel{\text{def}}{=} \dim \mathcal{H}_B$, respectively. We will use the term *state* in order to refer to normalized non-negative operators on $\mathcal{H}$. The set of all quantum states on $\mathcal{H}$ will be called Q . The set of all separable states on $\mathcal{H}$ will be call S .

There are several different ways to describe the separability problem as a computational problem [9]. In this paper, we chose to focus our attention in an approximated separability problem called the *weak membership problem of separability*. This “*promise*” problem (as opposed to a “*decision*” problem) roughly consists on deciding the separability of a given state, but allowing an uncertainty parameterized by δ .

More properly, the “*In-biased*” weak membership problem is defined as follows [9]:

(Weak membership problem of the separability (WMEM(S)))

Given a bipartite quantum state $\rho \in Q$ and rational $\delta > 0$, assert either that

$$\rho \in S(\delta) \text{ or} \tag{1}$$

$$\rho \notin S, \quad (2)$$

where $S(\delta)$ is a δ neighbor of S , i.e., $S(\delta) = \{\sigma \in Q : \exists \tilde{\sigma} \in S \subset Q, \|\tilde{\sigma} - \sigma\|_1 \leq \delta\}$.

In the above definition, $\|\omega\|_1 = \text{Tr}(\sqrt{\omega\omega^\dagger})$, the trace norm of the operator ω , although, in principle, we could have chosen other norms or distance measures as an accuracy parameter.

WMEM(S) is, thus, an approximation of the conventional separability problem in the sense that an algorithm solving WMEM(S) may assert equation (1) for a state ρ_{AB} having just a small amount of entanglement. This approximated formalism is more practical than a non-approximated or exact formalism like EXACT-QSEP [9], because of the inevitable errors we incur in both numerical and experimental studies, that should somehow be accounted for in our analysis of separability. A fair amount of effort has been devoted to the study of the time complexity of WMEM(S), the most remarkable result being that, if $d_A \geq d_B$, then WMEM(S) is NP-hard whenever $1/\delta$ increases exponentially [7] or polynomially [8] with respect to d_B .

Several different algorithms are known [9] to solve WMEM(S). Among them, we will focus on algorithms based on the symmetric extensions criterion and the PPT symmetric extensions criterion (we will call them DPS criteria). In the symmetric extensions criterion, we have to decide whether a given bipartite state ρ_{AB} is in the set S^N of N -symmetrically extendible states. We say that ρ_{AB} belongs to S^N iff there exists a state $\rho_{AB^N} \in \mathcal{H}_A \otimes \mathcal{H}_B^{\otimes N}$ that satisfies the following three conditions:

1. $\rho_{AB^N} \geq 0$.
2. $\text{Tr}_{B^{N-1}}(\rho_{AB^N}) = \rho_{AB}$.
3. ρ_{AB^N} is Bose symmetric in $\mathcal{H}_B^{\otimes N}$, i.e., $\rho_{AB^N}(A \otimes P_{\text{sym}}^N) = \rho_{AB^N}$, where P_{sym}^N denotes the projector onto the symmetric subspace $\mathcal{H}_{\text{sym}}^N$ of $\mathcal{H}_B^{\otimes N}$.

Similarly, in the PPT symmetric extension criterion, we have to decide if a given bipartite state ρ is in the set S_p^N of N -PPT symmetrically extendible states, and we say that $\rho_{AB} \in S_p^N$ iff there exists a state ρ_{AB^N} fulfilling 1-3 and the additional constraint:

4. ρ_{AB^N} has a Positive Partial Transpose (i.e., it is PPT) [16] w.r.t. the bipartition $AB^{[N/2]}|B^{[N/2]}$.

Doherty et al. [12] proved that both sequences $\{S^N\}_{N=1}^\infty$ and $\{S_p^N\}_{N=1}^\infty$ converge to S from the outside:

$$S_{(p)}^1 \supset S_{(p)}^2 \supset S_{(p)}^3 \supset \dots \supset S, \text{ with } \lim_{N \rightarrow \infty} S_{(p)}^N = S. \quad (3)$$

Moreover, as all these sets are defined through linear matrix inequalities, the problem of determining whether a given state belongs to one of them can be cast as a semidefinite program (SDP) [15]. For a given δ , there exists a natural number $N(\delta)$ such that $S_{(p)}^{N(\delta)} \subset S(\delta)$. Checking if $\rho_{AB} \in S_{(p)}^{N(\delta)}$, we can thus

solve $\text{WMEM}(S)$ with a precision parameter δ . Thus, the DPS criterion gives an algorithm for $\text{WMEM}(S)$ that can be formulated as a semidefinite program.

We will now proceed to evaluate the time complexity of $\text{WMEM}(S)$ when solved through the DPS criterion. First, following the discussion of Doherty et al. [12], S^N can be characterized by a semidefinite program with $\left((\dim \mathcal{H}_{\text{sym}}^N)^2 - d_B^2\right) d_A^2$ free variables and a matrix of size $(\dim \mathcal{H}_{\text{sym}}^N) d_A$ on which we will impose the positivity constraint. On the other hand, for S_p^N , the PPT constraint implies demanding positivity from an additional matrix of size $(\dim \mathcal{H}_{\text{sym}}^{N/2})^2 d_A$. Since the time-complexity of an SDP with m variables and of matrix size n is $O(m^2 n^2)$ (with a small extra cost coming from an iteration of algorithms), the dominant factors for the asymptotic time-complexity of these tests can be written as

$$\text{Symmetric} : d_A^6 (\dim \overline{\mathcal{H}_{\text{sym}}^{N_{\text{sym}}}})^6 \quad (4)$$

$$\text{PPT symmetric} : d_A^6 (\dim \overline{\mathcal{H}_{\text{sym}}^{N_{\text{ppt}}}})^4 (\dim \overline{\mathcal{H}_{\text{sym}}^{N_{\text{ppt}}/2}})^4, \quad (5)$$

where $\overline{N_{\text{sym}}}$ and $\overline{N_{\text{ppt}}}$ are the sizes of the extensions needed to achieve a given accuracy parameter δ :

$$\overline{N_{\text{sym}(\text{ppt})}} \stackrel{\text{def}}{=} \min_{n \in \mathbb{N}} \left\{ n \mid S_{(p)}^n \subset S(\delta) \right\}. \quad (6)$$

By definition, $S_p^N \subset S_p^N$, and so S_p^N will approximate S better than S^N . However, at this stage, there still remains the possibility that the algorithm based on the sets $\{S_p^N\}$ is slower than the one based on the sets $\{S^N\}$, because of the increase in time complexity that arises from imposing positivity on the partially transposed operator. In other words, the scalings of $\overline{N_{\text{sym}}}$ and $\overline{N_{\text{ppt}}}$ actually determine which algorithm is the faster. The aim of this paper is to suggest that the additional PPT constraint actually accelerates the algorithm by deriving upper bounds for $\overline{N_{\text{sym}}}$ and $\overline{N_{\text{ppt}}}$.

3 Analysis of the Symmetric Extensions Criterion without the PPT Constraint

In [9], Ioannou derived an upper bound on $\overline{N_{\text{sym}}}$ by invoking the finite quantum de Finetti theorem [13,14]. Here, we derive an improved upper bound on $\overline{N_{\text{sym}}}$ that improves the previous bound by approximately a constant factor 2. This improvement is accomplished by means of a characterization of the amount of local noise sufficient to induce separability on states in S^N .

Lemma 1. *For any state $\rho_{AB} \in S^N$, the state $\tilde{\rho}_{AB}$ defined as*

$$\tilde{\rho}_{AB} = \frac{N}{N + d_B} \rho_{AB} + \frac{1}{N + d_B} \rho_A \otimes \mathbb{I}_B \quad (7)$$

is separable.

From the above lemma, we can derive an upper bound of $\overline{N_{\text{sym}}}$ as follows:

Theorem 1. *For all $N \in \mathbb{N}$, we have $S^N \subseteq S(\delta)$ with*

$$\delta = \frac{2(d_B - 1)}{N + d_B - 1}. \quad (8)$$

In other words,

$$\overline{N_{\text{sym}}} \leq \left\lceil \frac{(2 - \delta)(d_B - 1)}{\delta} \right\rceil. \quad (9)$$

(Proof of Theorem 1)

Let $\rho \in S^N$. Then Lemma 1 implies that there exists $\tilde{\rho} \in S$, with $\tilde{\rho}_A = \rho_A$, such that:

$$\rho - \tilde{\rho} = \frac{d_B - 1}{N + d_B - 1} \rho - \frac{1}{N + d_B - 1} (\rho_A \otimes_{B} \tilde{\rho}). \quad (10)$$

Using the triangle inequality, we have that

$$\begin{aligned} \|\rho - \tilde{\rho}\|_1 &\leq \frac{d_B - 1}{N + d_B - 1} \|\rho\|_1 + \frac{1}{N + d_B - 1} \|(\rho_A \otimes_{B} \tilde{\rho})\|_1 \\ &= \frac{2(d_B - 1)}{N + d_B - 1}, \end{aligned} \quad (11)$$

where in the last step we used the fact that $\rho_A \otimes_{B} \tilde{\rho}$ is separable (and, therefore, positive). $\square$

Before we go into the proof Lemma 1, we will give some remarks about the notation used in this section and the next one. Given a unitary operator U , by $|U\rangle$ we will denote the state $U|0\rangle$. dU will be understood as the Haar measure over $\text{SU}(d_B)$. Also, for any permutation $\pi \in P_N$, $V_\pi \in B(\mathcal{H}^{\otimes N})$ will represent the corresponding permutation operator. V alone will denote the SWAP operator acting over a bipartite system $\mathcal{H}^{\otimes 2}$, i.e.,

$$V = \sum_{i,j=0}^{d_B} |i\rangle |j\rangle \langle j| \langle i|. \quad (12)$$

Now, we go into the proof of Lemma 1.

(Proof of Lemma 1)

For $\rho_{AB} \in S^N$, we define a state $\tilde{\rho}_{AB}$ as follows:

$$\tilde{\rho}_{AB} = \frac{\int dU \text{Tr}_{B^N} \left(A \otimes |U\rangle \langle U|^{\otimes N+1} \rho_{AB^N} \otimes_{B} \right)}{\int dU \text{Tr}(|U\rangle \langle U|^{\otimes N} \rho_{B^N})}. \quad (13)$$

By the definition, $\tilde{\rho}_{AB}$ is clearly a separable state.

To evaluate the integrals in Eq.(13) it is enough to notice that

1. For any operator C ,

$$\int dU U^{\otimes N} C (U^\dagger)^{\otimes N} = \sum_{\pi \in P_N} c_\pi V_\pi, \quad (14)$$

for some coefficients c_π . In particular,

$$\begin{aligned} \int dU |U\rangle \langle U|^{\otimes N} &= \frac{(d-1)! N! P_{\text{sym}}^N}{(N+d-1)!} \\ &= \frac{(d-1)! \sum_{\pi \in P_N} V_\pi}{(N+d-1)!}. \end{aligned} \quad (15)$$

2. Due to the fact that ρ_{AB^N} acts over $\mathcal{H}_A \otimes \mathcal{H}_{\text{sym}}^N$, for any $\pi \in P_{N+1}$,

$$\begin{aligned} \text{Tr}_{B^N} \{ (\rho_{AB^N} \otimes I_A) V_\pi \} &= \\ &= \begin{cases} \rho_A \otimes I_B, & \text{if } \pi(N+1) = N+1; \\ \rho_{AB}, & \text{otherwise.} \end{cases} \end{aligned} \quad (16)$$

Finally, we arrive at the expression Eq.(7) □

It is natural to wonder if the above bounds are indeed optimal. We will argue that at least the scaling of the upper bounds for the accuracy of the approximation of S by S^N is correct with respect to N ; hence, it should be $O(1/N)$. For this purpose, it is convenient to introduce an entanglement measure called the *robustness of entanglement* of a state ρ is defined as the minimum amount of separable noise needed to destroy the entanglement of such a state [17]:

$$R(\rho) \stackrel{\text{def}}{=} \min_{\lambda} \{ \lambda : \exists \sigma \in S, \text{ s.t. } \frac{\rho + \lambda \sigma}{1 + \lambda} \in S \}. \quad (17)$$

Then, from Lemma 1, it is straightforward to see that $\rho_{AB} \in S^N$ satisfies the inequality

$$R(\rho) \leq \frac{d_B - 1}{N}, \quad (18)$$

which may be accepted as a counterpart of Theorem 1 in term of the robustness of entanglement. We will see this inequality (18) is actually tight with respect to N .

To see this fact, let $N = 2K - 1$, and consider the $N + 1$ bipartite state given by

$$|\Psi_{AB^N}\rangle \equiv \frac{1}{C_K} \sum_{\text{perm}} \left| \overbrace{0 \cdots 0}^K \overbrace{1 \cdots 1}^K \right\rangle, \quad (19)$$

where C_K is a normalization factor. Define now $\rho_{AB} \equiv \text{Tr}_{B^{N-1}}(|\Psi_{AB^N}\rangle\langle\Psi_{AB^N}|)$. Clearly, $\rho_{AB} \in S^N$. Now, it can be shown that

$$\begin{aligned} \rho_{AB} = & \frac{K-1}{2(2K-1)}(|00\rangle\langle 00| + |11\rangle\langle 11|) + \\ & + \frac{K}{2(2K-1)}(|01\rangle + |10\rangle)(\langle 01| + \langle 10|). \end{aligned} \quad (20)$$

The partially transposed operator $\rho_{AB}^{T_B}$ has a negative eigenvalue $-1/2(2K-1)$ corresponding to the eigenvector $(|00\rangle - |11\rangle)/\sqrt{2}$, whose maximum Schmidt coefficient is $1/\sqrt{2}$. According to [17], this implies that $R(\rho_{AB}) = 1/(2K-1) = 1/N$. The bound (18) is, therefore, tight for $d_A = d = 2$. Since for any pair of Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ of dimensions greater than 1 we can embed the previous family of states in $B(\mathcal{H}_A \otimes \mathcal{H}_B)$, it follows that the optimal upper bound on the entanglement robustness of partial traces of Bose symmetric extensions must scale as $O(1/N)$.

4 Analysis of the PPT Symmetric Extensions Criterion

In this section, we will analyze how fast the set of states admitting a PPT symmetric extension S_p^N converges to the set of all separable states S . As a result, we will derive an upper bound of $\overline{N_{\text{ppt}}}$ which is quadratically better than the upper bound Eq.(9) of $\overline{N_{\text{sym}}}$ derived in the previous section.

The following lemma, a counterpart of Lemma 1 in terms of S_p^N , estimates the amount of local noise necessary to induce separability on states in S_p^N .

Lemma 2. *For any state $\rho_{AB} \in S_p^N$, the state $\tilde{\rho}_{AB}$ defined as*

$$\tilde{\rho}_{AB} \equiv (1 - \frac{d_B}{2(d_B-1)}g_N)\rho_{AB} + \frac{1}{2(d_B-1)}g_N\rho_A \otimes \rho_B \quad (21)$$

is separable. In the above equation, g_N (or $g_N^{(d_B)}$ in case d_B is ambiguous) is defined as

$$\begin{aligned} g_N = & \min\{1 - x : P_{N/2+1}^{(d_B-2,0)}(x) = 0\} \text{ for } N \text{ even,} \\ & \min\{1 - x : P_{(N+1)/2}^{(d_B-2,1)}(x) = 0\} \text{ for } N \text{ odd,} \end{aligned} \quad (22)$$

with $P_n^{(\alpha,\beta)}(x)$ being the Jacobi Polynomials [18].

Notice that, in the above lemma, g_N is defined in terms of the greatest root of Jacobi polynomials. The properties of the roots of Jacobi polynomials have been studied for a long time [18]. This allows us to derive an expression for the asymptotic behavior of g_N :

$$g_N \approx 2 \left(\frac{j_{d-2,1}}{N} \right)^2, \text{ for } N \gg 1,$$

$$\approx 2 \left(\frac{d_B + 1.856d_B^{1/3} + O(d_B^{-1/3})}{N} \right)^2, \quad \text{for } N \gg d_B \gg 1, \quad (23)$$

where $j_{n,1}$ is the first positive zero of the Bessel function $J_n(y)$.

From the above lemma, using the same techniques that allowed to derive Theorem 1, we arrive at:

Theorem 2. *For all $N \in \mathbb{N}$, we have $S_p^N \subseteq S(\delta)$ with*

$$\delta = g_N \approx 2 \left(\frac{d}{N} \right)^2, \quad (24)$$

In other words,

$$\overline{N_{\text{ppt}}} \lesssim \frac{\sqrt{2}j_{d_B-2,1}}{\sqrt{\delta}} \approx \frac{\sqrt{2}d_B}{\sqrt{\delta}}. \quad (25)$$

Comparing this theorem with Theorem 1, we observe that the upper bounds for S_p^N converge quadratically faster than those for S^N . In other words, if the bounds for S^N were optimum, then we would have proven that the additional PPT constrain gives the DPS criterion a quadratic speed-up. Actually, as we saw in the last section, the bound $O(1/N)$ on the robustness of entanglement of states in S^N is tight. On the other hand, from Lemma 2, we can derive a bound $R(\rho) \leq \frac{g_N}{2 - \frac{d}{d-1}g_N} \approx \left(\frac{d}{N}\right)^2$ for $\rho \in S_p^N$. This bound guarantees that the corresponding value for S_p^N at least scales as $O(1/N^2)$, i.e., Lemma 2 allows to derive an upper bound for the entanglement robustness that decreases asymptotically faster than the optimal upper bound in the general Bose symmetric case.

After substituting Eq. (9) and Eq. (25) to Eq. (4) and Eq. (5), using the Stirling formula, and doing straightforward arithmetic, we obtain upper bounds on the time complexity of WMEM(S) when attacked via the symmetric extensions criterion and the PPT symmetric extensions criterion. Respectively:

$$\begin{aligned} & O \left(d_A^6 \left[\frac{2e}{\delta} \right]^{6d_B} \right), \quad \text{for } S^N \\ & O \left(d_A^6 \left[\frac{e^2}{\delta} \right]^{4d_B} \right), \quad \text{for } S_p^N, \end{aligned} \quad (26)$$

where we just wrote the dominant (exponential) terms and omitted all polynomially growing terms. Note that the scaling law derived for the non PPT DPS criterion is valid as long as the optimal bounds on the trace distance to the set of separable states scale as d_B/N . We conjecture that such is the case, although all our attempts to derive an analytical proof have failed so far. Under this assumption, the above formula thus shows that the criterion based on PPT BSEs indeed requires less steps than the one based on plain BSEs in order to solve WMEM(S) for a given accuracy δ .

Now, we proceed to the proof of Theorem 2,

(Proof of Theorem 2)

First, for even N , we define states $|\phi_N\rangle \in \mathcal{H}_B^{\otimes N}$ depending on coefficients $\{c_n\}_{n=0}^{N/2}$:

$$|\phi_N\rangle \stackrel{\text{def}}{=} \sum_{n=0}^{N/2} c_n |\psi_n\rangle; \quad |\psi_n\rangle \stackrel{\text{def}}{=} |00\rangle^{\otimes n} |\Psi^+\rangle^{\otimes N/2-n}, \quad (27)$$

where $|\Psi^+\rangle \stackrel{\text{def}}{=} \sum_i |ii\rangle$ is proportional to a maximally entangled state.

When N is even, we define $\tilde{\rho}_{AB}$ for $\rho_{AB} \in S_p^N$ as follows:

$$\tilde{\rho}_{AB} = \frac{\int dU \text{Tr}_{B^N} \left[I_A \otimes (U^{\otimes N} |\phi_N\rangle \langle \phi_N|^{T_{B'}} U^{\dagger \otimes N} \cdot \rho_{AB^N}) \right] \otimes |U\rangle \langle U|}{\int dU \text{Tr}_{B^N} \left[(U^{\otimes N} |\phi_N\rangle \langle \phi_N|^{T_{B'}} U^{\dagger \otimes N} \cdot \rho_{B^N}) \right]}, \quad (28)$$

where $T_{B'}$ is a partial transposition with respect to $N/2$ copies of $\mathcal{H}_B$, that is, with respect to the partition $AB^{N/2}|B^{N/2}$. The PPT condition of $\rho_{AB^N} \in S_p^N$ guarantees the separability of $\tilde{\rho}_{AB}$.

A fast way to perform the integral in Eq.(28) is to notice that, for $m > n$,

$$|\psi_n\rangle \langle \psi_m|^{T_{B'}} = |00\rangle \langle 00|^{\otimes n} \otimes (|0\rangle \langle 0|)^{\otimes m-n} \otimes V^{\otimes N/2-m}. \quad (29)$$

Therefore, there exists a pair of permutations $\pi, \pi' \in P_N$ such that

$$V_\pi |\psi_n\rangle \langle \psi_m|^{T_{B'}} V_{\pi'}^\dagger = |0\rangle \langle 0|^{\otimes m+n} \otimes |0\rangle \langle 0|^{\otimes N-m-n}. \quad (30)$$

But $A \otimes V_\pi^\dagger \rho_{AB^N} = \rho_{AB^N} A \otimes V_\pi = \rho_{AB^N}$, so

$$\begin{aligned} \text{Tr}_{B^N} (\rho_{AB^N} A \otimes U^{\otimes N} |\psi_n\rangle \langle \psi_m|^{T_{B'}} (U^\dagger)^{\otimes N}) &= \\ = \text{Tr}_{B^N} (\rho_{AB^N} A \otimes |U\rangle \langle U|^{\otimes m+n} \otimes |0\rangle \langle 0|^{\otimes N-m-n}). \end{aligned} \quad (31)$$

In the end, we have that

$$\tilde{\rho}_{AB} = \left(1 - d_B \frac{\mathbf{c}^\dagger \tilde{A} \mathbf{c}}{\mathbf{c}^\dagger \tilde{B} \mathbf{c}} \right) \rho_{AB} + \frac{\mathbf{c}^\dagger \tilde{A} \mathbf{c}}{\mathbf{c}^\dagger \tilde{B} \mathbf{c}} \rho_A \otimes \rho_B, \quad (32)$$

where $\tilde{A}$ and $\tilde{B}$ are square matrices given by

$$\tilde{B}_{nm} = \frac{(n+m)!}{(n+m+d_B-1)!}, \quad \tilde{A}_{nm} = \frac{(n+m)!}{(n+m+d_B)!}, \quad n, m = 0, 1, \dots, N/2. \quad (33)$$

In case of odd N , we use the following definition of $\tilde{\rho}_{AB}$ instead of Eq.(28):

$$\begin{aligned} &\tilde{\rho}_{AB} \\ &= \frac{\int dU \text{Tr}_{B^N} \left[I_A \otimes (U^{\otimes N} |\phi_{N-1}\rangle \langle \phi_{N-1}|^{T_{B'}} \otimes |0\rangle \langle 0| U^{\dagger \otimes N} \cdot \rho_{AB^N}) \right] \otimes |U\rangle \langle U|}{\int dU \text{Tr}_{B^N} \left[(U^{\otimes N} |\phi_{N-1}\rangle \langle \phi_{N-1}|^{T_{B'}} \otimes |0\rangle \langle 0| U^{\dagger \otimes N} \cdot \rho_{B^N}) \right]}, \end{aligned}$$

After the appropriate computations, we again arrive at expression (32), but the form of $\tilde{A}$ and $\tilde{B}$ changes to:

$$\tilde{B}_{nm} = \frac{(n+m+1)!}{(n+m+d_B)!}, \tilde{A}_{nm} = \frac{(n+m+1)!}{(n+m+d_B+1)!},$$

$$n, m = 0, 1, \dots, (N-1)/2. \quad (34)$$

Obviously, in order to guarantee that ρ_{AB} is close to $\tilde{\rho}_{AB}$, it is in our interest to minimize the quantity

$$f_N(\mathbf{c}) \equiv \frac{\mathbf{c}^\dagger \tilde{A} \mathbf{c}}{\mathbf{c}^\dagger \tilde{B} \mathbf{c}} \quad (35)$$

over all possible vectors $\mathbf{c}$. Details on how to calculate the minimum of (35), together with the expression of the optimal $\mathbf{c}$ can be found in Appendix A. The result is:

$$\min_{\mathbf{c}} f_N(\mathbf{c}) = \frac{1}{2(d_B - 1)} g_N. \quad (36)$$

This concludes the proof of Theorem 2. $\square$

5 Conclusion

In this paper, we have studied the weak membership problem of separability in term of the DPS criterion. We showed that, while the minimal amount of noise necessary to turn an arbitrary state in S^N into a separable state decreases as $O(1/N)$, the corresponding amount of noise needed to disentangle states in S_p^N decreases at least as $O(1/N^2)$. Thus, S_p^N converges to S quadratically faster than S^N with respect to N . By means of these expressions, we showed that the PPT constraint in the DPS criterion reduces the dominant factor of the upper bound on the time complexity from $(k_1/\delta)^{6d_B}$ to $(k_2/\delta)^{4d_B}$, where δ is the accuracy parameter of $WMEM(S)$. We concluded that the PPT condition is worth imposing provided that the *optimal* bounds on the speed of convergence of the method based on plain BSEs scale as $O(d_B/N)$, as our own bounds suggest. We therefore hope to have shed some light on the question of how much the DPS criterion owes its strength to the PPT condition.

We note that a full version of this post proceedings is also available [19]. There one can find an extension of the theory to multi-partite systems, and its applications to derive approximate algorithms to solve the state estimation problem and compute the maximum output purity and the geometric measure of entanglement of arbitrary quantum channels and states. We also note that a new complete Separability criterion can be derived based on Lemma 1 and Lemma 2 [20].

Acknowledgements

The authors thank Animesh Datta and Fernando G. S. L. Brandão for useful discussions. This work is part of the EPSRC QIP-IRC and is supported by EPSRC grant EP/C546237/1, the Royal Society, the EU Integrated Project QAP and an Institute for Mathematical Sciences postdoc fellowship.

References

1. Plenio, M.B., Virmani, S.: Quant. Inf. Comp. 7, 1 (2007)
2. Bruss, D.: J. Math. Phys. 43, 4237 (2002)
3. Terhal, B.: J. Theor. Comp. Sci. 287, 313 (2002)
4. Sen, A., Sen, U., Lewenstein, M., Sanpera, A.: Ch. 8. In: Brus, D., Leuchs, G. (eds.) Lectures on Quantum Information
5. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Rev. Mod. Phys. 81, 865 (2009)
6. Gühne, O., Tóth, G.: Physics Reports 474, 1 (2009)
7. Gurvits, L.: Proceedings of the third fifth ACM symposium on Theory of computing, vol. 10. ACM Press, New York (2003)
8. Gharibian, S.: e-print arXiv:0810.4507
9. Ioannou, L.M.: Quant. Inf. Comp. 7, 335 (2007)
10. Spedalieri, F.M.: Phys. Rev. A 76, 032318 (2007)
11. Doherty, A.C., Parrilo, P.A., Spedalieri, F.M.: Phys. Rev. Lett. 88, 187904 (2002)
12. Doherty, A.C., Parrilo, P.A., Spedalieri, F.M.: Phys. Rev. A. 69, 022308 (2004)
13. König, R., Renner, R.: J. Math. Phys. 46, 122102 (2005)
14. Christandl, M., König, R., Mitchison, G., Renner, R.: Commun. Math. Phys. 273, 473 (2007)
15. Vandenberghe, L., Boyd, S.: SIAM Review 38, 49 (1996)
16. Peres, A.: Phys. Rev. Lett. 77, 1413 (1996)
17. Vidal, G., Tarrach, R.: Phys. Rev. A 59, 141 (1999)
18. Abramowitz, M., Stegun, I.A.: Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables. Dover Publications, New York (1972)
19. Navascués, M., Owari, M., Plenio, M.B.: e-print arXiv:0906.2731
20. Navascués, M., Owari, M., Plenio, M.B.: Phys. Rev. Lett. 103, 160404 (2009)

A Minimization of Eq.(35)

Take N even. Then it can be checked that

$$\begin{aligned}\tilde{A}_{mn} &= \int_0^1 x^{m+n} \cdot \frac{(1-x)^{d_B-1}}{(d_B-1)!} dx, \\ \tilde{B}_{mn} &= \int_0^1 x^{m+n} \cdot \frac{(1-x)^{d_B-2}}{(d_B-2)!} dx.\end{aligned}\tag{37}$$

Combining this relation with (35), it follows that

$$f(\mathbf{c}) = \frac{1}{d_B-1} \frac{\int_0^1 |\sum_{n=0}^{N/2} c_n x^n|^2 (1-x)(1-x)^{d_B-2} dx}{\int_0^1 |\sum_{n=0}^{N/2} c_n x^n|^2 (1-x)^{d_B-2} dx}.\tag{38}$$

That way, we can see the minimization of $f(\mathbf{c})$ as a minimization over the set of all polynomials $Q_{N/2}(x) = \sum c_n x^n$ of degree $N/2$. Making the change of coordinates $y = 2x - 1$ we find that the above minimization is equivalent to

$$\min_{Q_{N/2}} \frac{1}{2(d_B - 1)} \frac{\int_{-1}^1 |Q_{N/2}(y)|^2 (1 - y)^{d_B - 1} dy}{\int_{-1}^1 |Q_{N/2}(y)|^2 (1 - y)^{d_B - 2} dy}, \quad (39)$$

where $Q_{N/2}(y)$ is an arbitrary polynomial of order $N/2$. This problem can be solved by means of the *Jacobi polynomials*.

The Jacobi polynomials $P_n^{(\alpha, \beta)}(y)$ are a complete set of functions orthogonal upon integration in the interval $[-1, 1]$ under the weight $(1 + y)^\beta (1 - y)^\alpha$ [18]. Now, define the *normalized Jacobi polynomials* $p_n(y)$ as

$$p_n(y) \equiv \frac{P_n^{(d_B - 2, 0)}(y)}{\|P_n^{(d_B - 2, 0)}\|}, \quad (40)$$

with

$$\|P_n^{(d_B - 2, 0)}\| = \sqrt{\int_{-1}^1 |P_n^{(d_B - 2, 0)}(y)|^2 (1 - y)^{d_B - 2} dy}. \quad (41)$$

It is clear that we can express any $Q_{N/2}(y)$ as a linear combination of normalized Jacobi polynomials of order less or equal than $N/2$. That is,

$$Q_{N/2}(y) = \sum_{n=0}^{N/2} e_n p_n(y), \quad (42)$$

for some coefficients e_n . Because of the orthogonality of the p_n 's, when we input this expression in the integral of the denominator, we end up with

$$\int_{-1}^1 |Q_{N/2}(y)|^2 (1 - y)^{d_B - 2} dy = \sum_n |e_n|^2. \quad (43)$$

To calculate the integral on the numerator, we can make use of the recurrence relation

$$(1 - y)p_n(y) = \alpha_n p_n(y) + \beta_n p_{n+1}(y) + \gamma_n p_{n-1}(y), \quad (44)$$

that holds for some coefficients $\alpha_n, \beta_n, \gamma_n$, with $\gamma_0 = 0$ and $\gamma_{n+1} = \beta_n$ [18]. Invoking again the orthogonality of the Jacobi polynomials, we have that

$$\min_{\mathbf{c}} f(\mathbf{c}) = \min_{|\mathbf{e}|^2=1} \frac{1}{2(d_B - 1)} \mathbf{e}^\dagger \tilde{C} \mathbf{e}, \quad (45)$$

where $\tilde{C}$ is an $(N/2 + 1) \times (N/2 + 1)$ tridiagonal hermitian matrix given by

$$\begin{aligned} \tilde{C}_{m,n} = & \alpha_n, \text{ if } m = n, \\ & \beta_n, \text{ if } m = n + 1, \\ & \gamma_n, \text{ if } m = n - 1, \\ & 0 \text{ elsewhere.} \end{aligned} \quad (46)$$

Now we will proceed to diagonalize $\tilde{C}$.

Let λ be an eigenvalue of $\tilde{C}$. This means that there exists a vector $\{v_i\}_{i=0}^{N/2+1}$ such that

$$(\alpha_n - \lambda)v_n + \beta_n v_{n+1} + \gamma_n v_{n-1} = 0, \quad (47)$$

with $v_{N/2+1} = 0$.

Choose a real number y_0 and try the ansatz $v_n = p_n(y_0)$. From (44), it is clear that v_n will satisfy (47), provided that

$$\begin{aligned} \lambda &= 1 - y_0, \\ p_{N/2+1}(y_0) &= 0. \end{aligned} \quad (48)$$

That is, any root of the polynomial $p_{N/2+1}(y)$ corresponds to an eigenvalue of $\tilde{C}$.

But $p_{N/2+1}(y)$ has $N/2 + 1$ *simple* roots [18], so all the eigenvalues of $\tilde{C}$ are obtained using this strategy. It follows that

$$\min_{\mathbf{c}} f_N(\mathbf{c}) = \frac{1}{2(d_B - 1)} \min\{1 - x : P_{N/2+1}^{(d_B-2,0)}(x) = 0\}. \quad (49)$$

The expression for the case of odd N can be derived in an analogous way taking into account that, this time,

$$\begin{aligned} \tilde{A}_{mn} &= \int_0^1 x^{m+n} \cdot \frac{x(1-x)^{d_B-1}}{(d_B-1)!} dx, \\ \tilde{B}_{mn} &= \int_0^1 x^{m+n} \cdot \frac{x(1-x)^{d_B-2}}{(d_B-2)!} dx. \end{aligned} \quad (50)$$

Author Index

Bény, Cédric	66	Odaira, Takanori	33
Boileau, Jean-Christian	76	Owari, Masaki	94
Braunstein, Samuel L.	47		
Browne, Dan E.	20	Pachos, Jiannis K.	56
		Pirandola, Stefano	47
Campbell, Earl T.	20	Plenio, Martin B.	94
Cosme, Carlos M.M.	1	Portugal, Renato	1
Gonçalves, Demerson N.	1	Renes, Joseph M.	76
Hsieh, Min-Hsiu	85	van Dam, Wim	10
Koshiba, Takeshi	33		
		Wilde, Mark M.	85
Lahtinen, Ville	56	Wootton, James R.	56
Lloyd, Seth	47		
Navascués, Miguel	94	Yuan, Qingqing	10