TQC2015

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

May 20–22, Université Libre de Bruxelles, Belgium

Wednesday May 20 6

Invited talk: *Majorana particles with noise: problems with braiding anyons*
David DiVincenzo 6

Area law for fixed points of rapidly mixing dissipative quantum systems
Fernando G.S.L. Brandão, Toby Cubitt, Angelo Lucia, Spyridon Michalakis and David Perez Garcia 7

The spin-2 AKLT state on the square lattice is universal for measurement-based quantum computation
Tzu-Chieh Wei and Robert Raussendorf 9

Computation in generalised probabilistic theories
Ciaran Lee and Jonathan Barrett 11

Local hidden variable models for entangled quantum states using finite shared randomness
Joseph Bowles, Flavien Hirsch, Marco Túlio Quintino and Nicolas Brunner 12

The resource theory of steering
Rodrigo Gallego and Leandro Aolita 13

Sampling quantum nonlocal correlations with high probability
Carlos E. González-Guillén, C. Hugo Jiménez, Carlos Palazuelos and Ignacio Villanueva 15

On the closure of the completely positive semidefinite cone and linear approximations to quantum colorings
Sabine Burgdorf, Monique Laurent and Teresa Piovesan 16

Implementing unitary 2-designs using random diagonal-unitary matrices
Yoshifumi Nakata, Christoph Hirche, Ciara Morgan and Andreas Winter . 17

Quantum Circuits for Isometries
Raban Iten, Roger Colbeck, Ivan Kukuljan, Jonathan Home and Matthias Christandl 19

Thursday May 21 21

Invited talk: *Quantum property testing: A survey and one new result*
Ronald de Wolf 21

Hierarchy of efficiently computable and faithful lower bounds to quantum discord
Marco Piani 22

Quantum capacity can be greater than private information for arbitrarily many uses
David Elkouss and Sergii Strelchuk 24

Round elimination in exact communication complexity
Jop Briet, Harry Buhrman, Debbie Leung, Teresa Piovesan and Florian Speelman 26

Rate-loss analysis of an efficient quantum repeater architecture
Saikat Guha, Hari Krovi, Christopher Fuchs, Zachary Dutton, Joshua Slater, Christoph Simon and Wolfgang Tittel 27

Renormalising entanglement distillation
Stephan Waeldchen, Janina Gertis, Earl T. Campbell and Jens Eisert . . 29

Invited talk: *Unbounded entanglement can be needed to achieve the optimal success probability*
Laura Mančinska 31

Quantum enhancement of randomness distribution
Raul Garcia-Patron Sanchez, William Matthews and Andreas Winter . . 32

Semidefinite programs for randomness extractors
Mario Berta, Omar Fawzi and Volkher Scholz 34

Interferometric versus projective measurement of anyons
Michael Freedman and Claire Levaillant 35

Qudit (Gauge) Colour Codes in All Spatial Dimensions
Fern Watson, Earl Campbell, Hussain Anwar and Dan Browne 36

Thermalization and decoherence in open Majorana systems
Earl Campbell 38

Friday May 22 40

Invited talk: *A quantum algorithm for computing the unit group of an arbitrary degree number field*
Sean Hallgren 40

Oracles with Costs
Shelby Kimmel, Cedric Yen-Yu Lin and Han-Hsuan Lin 41

A universal adiabatic quantum query algorithm
Mathieu Brandeho and Jérémie Roland 42

On the Robustness of Bucket Brigade Quantum RAM
Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca and Priyaa Varshinee Srinivasan 43

New constructions for Quantum Money
Marios Georgiou and Iordanis Kerenidis 44

Making Existential-Unforgeable Signatures Strongly Unforgeable in the Quantum Random-Oracle Model
Edward Eaton and Fang Song 46

Posters 48

1. *A Quantum Key Distribution Protocol for quNits with better noise resistance*
Zoé Amblard and Francois Arnault 48

2. *Quantum control based on SU(2) decomposition of n-partite two level quantum systems*
Francisco Delgado 50

3. *Area laws and efficient descriptions of quantum many-body states*
Yimin Ge and Jens Eisert 52

4. *Efficient Implementation of Quantum Walk Based Search Algorithms*
András Gilyén 53

5. *Dealing with loss in a quantum computer*
Mercedes Gimeno-Segovia, Pete Shadbolt, Dan Browne and Terry Rudolph 55

6. *A linear condition for a wide range of exact quantum algorithms*
Sebastian Grillo and Franklin Marquezino 56

7. *Bidirectional quantum controlled teleportation by using EPR states and entanglement swapping*
Shima Hassanpour and Monireh Houshmand 58

8. *Bounds on quantum non-locality via partial transposition*
Karol Horodecki and Glaucia Murta 60

9. *Trotterization in universal quantum simulators under faulty control*
George Knee and William Munro 62

10. *Grover's search with faults on some marked elements*
Dmitry Kravchenko, Nikolajs Nahimovs and Alexander Rivosh 64

11. *A Generalized Quantum Inspired Evolutionary Algorithm for Signature - based Intrusion Detection Systems*
Monisha Loganathan 65

12. *Dynamical Quantum Steering Ellipsoids in Non-Markovian Spin Chains*
Ruari McCloskey, Tony Apollaro and Mauro Paternostro 66

13. *Computing many-party quantum correlations - analytical results*
Leiba Rodman, Ilya M. Spitkovsky, Arleta Szkola and Stephan Weis . . . 68

14. *Moments of Coinless Quantum Walks on Lattices*
Raqueline A. M. Santos, Renato Portugal and Stefan Boettcher 70

15. *Degradable Channels From Products of Pure States*
Vikesh Siddhu and Robert Griffiths 72

16. *Classical Simulation of Quantum Walks on Clusters of Computers*
David Souza, Franklin Marquezino and Alexandre A. B. Lima 74

17. *Quantum Adiabatic Evaluation of Trees*
Luís Tarrataca 76

18. *Secrecy in prepare-and-measure CHSH games with a qubit bound*
Erik Woodhead and Stefano Pironio 78

19. *On the breakdown of quantum search with spatially distributed marked vertices*
Thomas Wong 80

Majorana particles with noise: problems with braiding anyons

David DiVincenzo

RWTH Aachen & FZ Jlich

Abstract. It is believed that branched semiconductor nanowires can provide a realization of Kitaev's 1D model of Majorana quasiparticles [1], and the means of braiding these Ising anyons to achieve topologically protected quantum computation. We have identified a solvable model of the Kitaev chain, in the form of a "T" junction, coupled to a thermal environment. Using a Markovian treatment employed successfully in recent work of Bravyi and Haah [2], and an error correction protocol related to current work on other anyonic systems by [3] and [4], we determine the coherence of a qubit coded in four Majorana particles [5] both at rest and in the course of a sequence of moves that accomplish quasiparticle braiding. As anticipated by Kitaev, error correction is highly effective in suppressing loss of fidelity for stationary Majoranas in long wires. However, error correction is fundamentally ineffective at protecting coherence during (braiding) gate operations. We identify single quantum-jump events that cause qubit failure, which cannot be repaired by quantum error correction.
Work performed with Dr. Fabio Pedrocchi.

References

1. A. Y. Kitaev, Phys.-Usp. 44, 131 (2001).
2. S. Bravyi and J. Haah Phys. Rev. Lett. 111, 200501 (2013)
3. Courtney G. Brell, Simon Burton, Guillaume Dauphinais, Steven T. Flammia, and David Poulin Phys. Rev. X 4, 031058 (2014).
4. James R. Wootton, Jan Burri, Sofyan Iblisdir, and Daniel Loss Phys. Rev. X 4, 011051 (2014) .
5. J. Alicea, Y. Oreg, G. Refael, F. von Oppen, M. P. A. Fisher, Nat. Phys. 7, 412417 (2011).

Area law for fixed points of rapidly mixing dissipative quantum systems

arXiv:1505.02776

Fernando G. S. L. Brandão[1,2], Toby S. Cubitt[3], Angelo Lucia[4], Spyridon Michalakis[7], and David Perez-Garcia[4,5,6]

[1] Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA, U. S. A.
[2] Department of Computer Science, University College London, U. K.
[3] DAMTP, University of Cambridge, U. K.
[4] Departamento de Análisis Matemático, Universidad Complutense de Madrid, Spain
[5] IMI, Universidad Complutense de Madrid, Spain
[6] ICMAT, C/ Nicolás Cabrera, Campus de Cantoblanco, 28049 Madrid
[7] Institute for Quantum Information and Matter, Caltech, U. S. A.

Abstract. We prove an area law for the mutual information for fixed points of local dissipative quantum system satisfying a rapid mixing condition, under either of the following assumptions: the fixed point is pure, or the system is frustration free.

Recently, the quantum information community has been focusing its attention on the class of states that can be obtained as fixed points of (local) dissipative processes – more formally, fixed points of semigroups of trace preserving, completely positive linear maps. The motivation is twofold: on the one hand, such processes model most of the different types of noise that can be found in nature, and therefore provide a realistic model for physical systems – since in practice no system will be completely isolated. On the other hand, proposals have been made to artificially engineer such dissipative interactions in order to have a determined quantum state as a fixed point, making them effectively "dissipative machines" to produce useful/interesting quantum states [4, 7]. This dissipative state engineering has been experimentally shown to be a robust mechanism to maintain coherence [5, 1].

A natural question then arises: is there in this context an area law – a scaling of entanglement entropy of a subregion as the volume of the boundary of the region, instead of its volume? First of all, we must notice that since fixed points of dissipative evolutions are generically not pure, we must consider another measure of entanglement or correlations, and we will focus on the *mutual information* [8].

For area laws in Hamiltonian systems, the main assumption that is usually made is the presence of a spectral gap, a non-vanishing separation between the two lowest energy levels of the Hamiltonian. In the dissipative setting, instead of spectral assumptions, it is more natural to make assumptions on the speed of convergence of the dissipation towards its fixed point (a quantity that is not controlled by the spectrum alone [6]), or equivalently on the so-called *mixing time*. In this work we restrict to systems for which the mixing time scales logarithmically with the system size, a property we called *rapid mixing*[2].

Under such assumption we prove the following two results:

1. if the system satisfies rapid mixing and the fixed point is pure, then it satisfies an area law (for the entanglement entropy);
2. if the system satisfies rapid mixing and is frustration free, then its fixed point satisfies an area law for the mutual information.

In both cases, the area law obtained will have a logarithmic correction.

We will compare these bounds with the ones obtained in [3].

References

1. J. T. Barreiro, P. Schindler, O. Gühne, T. Monz, M. Chwalla, C. F. Roos, M. Hennrich, and R. Blatt. Experimental multiparticle entanglement dynamics induced by decoherence. *Nature Physics*, 6:943–946, December 2010.
2. Toby S. Cubitt, Angelo Lucia, Spyridon Michalakis, and David Perez-Garcia. Stability of local quantum dissipative systems, 2013.
3. Michael J Kastoryano and Jens Eisert. Rapid mixing implies exponential decay of correlations. *Journal of Mathematical Physics*, 54(10):102201, 2013.
4. B. Kraus, H. P. Büchler, S. Diehl, A. Kantian, A. Micheli, and P. Zoller. Preparation of entangled states by quantum Markov processes. *Phys. Rev. A*, 78(4), October 2008.
5. Hanna Krauter, Christine A. Muschik, Kasper Jensen, Wojciech Wasilewski, Jonas M. Petersen, J. Ignacio Cirac, and Eugene S. Polzik. Entanglement generated by dissipation and steady state entanglement of two macroscopic objects. *Phys. Rev. Lett.*, 107:080503, August 2011.
6. Oleg Szehr, David Reeb, and Michael M Wolf. Spectral convergence bounds for classical and quantum markov processes, 2013.
7. F. Verstraete, M. M. Wolf, and J. I. Cirac. Quantum computation and quantum-state engineering driven by dissipation. *Nature Physics*, 5(9):633–636, 2009.
8. Michael M. Wolf, Frank Verstraete, Matthew B. Hastings, and J. Ignacio Cirac. Area laws in quantum systems: Mutual information and correlations. *Phys. Rev. Lett.*, 100:070502, February 2008.

The spin-2 AKLT state on the square lattice is universal for measurement-based quantum computation

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

[1] C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, State University of New York at Stony Brook, Stony Brook, NY 11794-3840, USA

[2] Department of Physics and Astronomy, University of British Columbia, Vancouver, British Columbia, V6T 1Z1, Canada

Abstract. We show that the spin-2 Affleck-Kennedy-Lieb-Tasaki state on the square lattice can be used as a resource state for performing universal quantum computation with only local measurements. The proof is done by finding local measurements that convert the AKLT state to random planar graph states, whose graphs are in the supercritical phase of percolation.

1 Motivation

One-way quantum computation was first invented using the cluster state [1]. Since then graph states, the generalization of the cluster state, were investigated and understood when they would enable such a measurement-based approach for quantum computation (MBQC). Are there any other family of states, i.e., states with different entanglement structures, that can also serve as the universal resource for quantum computation? Recent study shows that the spin-3/2 Affleck-Kennedy-Lieb-Tasaki (AKLT) state [2] on the honeycomb lattice also provides a useful source [3, 4]. It then triggers the question: are there other states in the AKLT family that are universal for MBQC? If so, what properties are essential for the universality?

2 Result

Here, we show that the spin-2 AKLT state on the square lattice is a universal resource for measurement-based quantum computation. We employ a local POVM on all sites that convert the local 5-level system to 2-level, and the post-POVM state is a graph state, whose graph is in general non-planar. We then follow with another round of local measurement to

recover the planarity of the graphs by thinning. The resultant typical graphs are shown to reside in the supercritical phase of percolation via Monte Carlo simulations. This means that the associated graph states are universal, implying the AKLT state is also universal. The details are described in our preprint [5].

One difference between the spin-3/2 and the spin-2 is the POVM. For the latter, three additional elements are needed to fulfill the completeness relation. Hence, the probability weight for the POVM outcomes are different. The most pronounced difference between the spin-3/2 and spin-2 probability weights is that for spin 3/2 all possible combinations of POVM outcomes do indeed occur with non-zero probability (except when the lattice is not bi-colorable, i.e., due to geometric frustration). This arisesas a consequence of the bi-colorability of the underlying honeycomb lattice. For the spin-2 case, certain combinations of POVM outcomes do not occur, i.e., have probability zero.

Our result here adds a missing piece to a series of study [3, 4, 6, 7] and gives rise to the following emerging picture that advances our understanding of the quantum computational universality in the valence-bond family. AKLT states involving spin-2 and other lower spin entities are universal if they reside on a two-dimensional frustration-free regular lattice with any combination of spin-2, spin-3/2, spin-1 and spin-1/2 (consistent with the lattice). Furthermore, geometric frustration can, but not necessarily, be a hinderance to the quantum computational universality, and a frustrated lattice can be decorated (by adding additional spins) such that the resultant AKLT state is universal.

References

1. R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
2. I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Phys. Rev. Lett. **59**, 799 (1987); Comm. Math. Phys. **115**, 477 (1988). T. Kennedy, E. H. Lieb, and H. Tasaki, J. Stat. Phys. **53**, 383 (1988).
3. T.-C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).
4. A. Miyake, Ann. Phys. (Leipzig) **326**, 1656 (2011).
5. T.-C. Wei and R. Raussendorf, arXiv:1501.07571
6. T.-C. Wei, Phys. Rev. A **88**, 062307 (2013).
7. T.-C. Wei, P. Haghnegahdar, R. Raussendorf, Phys. Rev. A **90**, 042333, (2014).

Computation in generalised probabilistic theories

Ciarán M. Lee* and Jonathan Barrett

University of Oxford, Department of Computer Science, Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

From the general difficulty of simulating quantum systems using classical systems, and in particular the existence of an efficient quantum algorithm for factoring, it is likely that quantum computation is intrinsically more powerful than classical computation. At present, the best upper bound known for the power of quantum computation is that **BQP** $\subseteq$ **AWPP**, where **AWPP** is a classical complexity class (known to be included in **PP**, hence **PSPACE**). This work investigates limits on computational power that are imposed by simple physical, or information theoretic, principles. To this end, we define a circuit-based model of computation in a class of operationally-defined theories more general than quantum theory, and ask: what is the minimal set of physical assumptions under which the above inclusions still hold? We show that given only an assumption of tomographic locality (roughly, that multipartite states and transformations can be characterised by local measurements), efficient computations are contained in **AWPP**. This inclusion still holds even without assuming a basic notion of causality (where the notion is, roughly, that probabilities for outcomes cannot depend on future measurement choices). Following Aaronson, we extend the computational model by allowing post-selection on measurement outcomes. Aaronson showed that the corresponding quantum complexity class, **PostBQP**, is equal to **PP**. Given only the assumption of tomographic locality, the inclusion in **PP** still holds for post-selected computation in general theories. Hence in a world with post-selection, quantum theory is optimal for computation in the space of all operational theories. We then consider whether one can obtain relativised complexity results for general theories. It is not obvious how to define a sensible notion of a computational oracle in the general framework that reduces to the standard notion in the quantum case. Nevertheless, it is possible to define computation relative to a 'classical oracle'. Then, we show there exists a classical oracle relative to which efficient computation in any theory satisfying the causality assumption does not include **NP**. This provides some degree of evidence that **NP**-complete problems cannot be solved efficiently in any theory satisfying tomographic locality and causality.

*Electronic address: ciaran.lee@cs.ox.ac.uk

Local hidden variable models for entangled quantum states using finite shared randomness

Joseph Bowles[1], Flavien Hirsch[1], Marco Túlio Quintino[1], and Nicolas Brunner[1]

1 **Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland**

Abstract

The statistics of local measurements performed on certain entangled states can be reproduced using a local hidden variable (LHV) model. While all known models make use of an infinite amount of shared randomness—the physical relevance of which is questionable—we show that essentially all entangled states admitting a LHV model can be simulated with finite shared randomness. Our most economical model simulates noisy two-qubit Werner states using only 3.58 bits of shared randomness. We also discuss the case of POVMs, and the simulation of nonlocal states with finite shared randomness and finite communication. Our work represents a first step towards quantifying the cost of LHV models for entangled quantum states.

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The resource theory of steering

Rodrigo Gallego[1] and Leandro Aolita[1]

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

Steering, as Schrödinger named it [1], is an exotic quantum effect by which ensembles of quantum states can be remotely prepared by performing local measurements at a distant lab. It allows [2, 3] to certify the presence of entanglement between a user with an untrusted measurement apparatus, Alice, and another with a trusted quantum-measurement device, Bob. It constitutes a fundamental notion between quantum entanglement [4], whose certification requires quantum measurements on both sides, and Bell non-locality [5], where both users possess untrusted black-box devices. Steering can be detected through simple tests analogous to Bell inequalities [6], and has been verified in a variety of remarkable experiments [7]. Apart from its fundamental relevance, steering has been identified as a resource for one-sided device-independent quantum key-distribution (QKD), where only one of the parts has an untrusted apparatus while the other ones possess trusted devices [8, 9]. There, the experimental requirements for unconditionally secure keys are less stringent than in fully (both-sided) device-independent QKD [10].

In this work, we present a formal operational framework for steering as a physical resource, i.e., we develop a *resource theory* of steering. The basic component of a resource theory is the identification of resource non-increasing operations, i.e., a set physical operations that map the set of states without the resource into itself. With this, one can define measures of the resource or study conversion rates between resourceful states, for example. Entanglement theory [4] is the most popular and best understood example of a resource theory [11], being local operations assisted by classical communication (LOCCs) the corresponding non-increasing operations.

Our results can be (item-like) summarized by the following list:

– We show that local operations and one-way classical communication from Bob to Alice (1W-LOCCs) are a valid set of steering non-increasing operations. Furthermore, we show its relevance as the natural set of operations employed in information protocols where steering is a useful resource; namely, one-sided device-independent quantum key distribution and randomness.

– We introduce the notion of convex steering monotones as axiomatic quantifiers of steering.
– As an example, we present the relative entropy of steering. In addition, we show that two other recently proposed measures, the steerable weight [12] and the robustness of steering [13], are also convex steering monotones.
– To end up with, we study steering conversion under 1W-LOCCs. On the one hand, we establish necessary and sufficient conditions for pure-state steering conversions under stochastic 1W-LOCCs. On the other hand, we prove, for minimal-dimensional systems, the non-existence of *steering bits*, i.e., measure-independent maximally steerable states from which all states can be obtained by means of the free operations.

References

1. E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).
2. H. M. Wiseman, S. J. Jones and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
3. M. D. Reid *et al.*, Rev. Mod. Phys. **81**, 1727 (2009).
4. R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. of Mod. Phys. **81**, 865 (2009).
5. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
6. E. G. Cavalcanti, S. J. Jones, H. M. Wiseman and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).
7. Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992); W. P. Bowen, R. Schnabel, and P. K. Lam, Phys. Rev. Lett. **90**, 043601 (2003); D.-H. Smith et al., Nat. Commun. **3**, 625 (2012); D. J. Saunders *et al.*, Nat. Phys. **6**, 845 (2010); A. J. Bennet *et al.*, Phys. Rev. X **2**, 031003 (2012); V. Händchen *et al.*, Nat. Phot. **6**, 598 (2012); B. Wittmann *et al.*, New J. Phys. **14**, 053030 (2012); S. Steinlechner *et al.*, Phys. Rev. A **87**, 022104 (2013).
8. C. Branciard *et al., P*hys. Rev. A **85**, 010301(R) (2012).
9. Q. Y. He and M. D. Reid, Phys Rev Lett. **111**, 250403 (2013).
10. A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).
11. V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
12. P. Skrzypczyk, M. Navascués, and D. Cavalcanti, arXiv: 1311.4590.
13. M. Piani and J. Watrous, arXiv:1406.0530 (2014).

Sampling quantum nonlocal correlations with high probability

Carlos González-Guillén[1,2], C. Palazuelos[3,4], and I. Villanueva[2,3]

[1] Universidad Politécnica de Madrid
[2] Instituto de Matemática Interdisciplinar IMI
[3] Universidad Complutense de Madrid
[4] Instituto de Ciencias Matemáticas ICMAT

Abstract. t is well known that quantum correlations for bipartite dichotomic measurements are those of the form $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$, where the vectors u_i and v_j are in the unit ball of a real Hilbert space. In this work we study the probability of the nonlocal nature of these correlations as a function of $\alpha = \frac{m}{n}$, where the previous vectors are sampled according to the Haar measure in the unit sphere of $\mathbf{R}^m$. In particular, we prove the existence of an $\alpha_0 > 0$ such that if $\alpha \leq \alpha_0$, γ is nonlocal with probability tending to 1 as $n \to \infty$, while for $\alpha > 2$, γ is local with probability tending to 1 as $n \to \infty$.

On the closure of the completely positive semidefinite cone and linear approximations to quantum colorings

Sabine Burgdorf[1], Monique Laurent[1,2], and Teresa Piovesan[2]

[1] Centrum Wiskunde & Informatica (CWI), The Netherlands
[2] Tilburg University, The Netherlands

We investigate structural properties of the completely positive semidefinite cone $\mathcal{CS}_+^n$, consisting of all the $n \times n$ symmetric matrices that admit a Gram representation by positive semidefinite matrices of any size. This cone has been introduced to model quantum graph parameters as conic optimization problems. Recently it has also been used to characterize the set $\mathcal{Q}$ of bipartite quantum correlations, as projection of an affine section of it. We have two main results concerning the structure of the completely positive semidefinite cone, namely about its interior and about its closure. On the one hand we construct a hierarchy of polyhedral cones which covers the interior of $\mathcal{CS}_+^n$, which we use for computing some variants of the quantum chromatic number by way of a linear program. On the other hand we give an explicit description of the closure of the completely positive semidefinite cone, by showing that it consists of all matrices admitting a Gram representation in the tracial ultraproduct of matrix algebras.

Implementing unitary 2-designs using random diagonal-unitary matrices

Yoshifumi Nakata[1,2], Christoph Hirche[2], Ciara Morgan[2], and Andreas Winter[3]

[1] Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan
[2] Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover, Germany
[3] ICREA & Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain

Abstract Unitary 2-designs are random unitary matrices which have a wide range of applications in quantum information science and, in contrast to their Haar-distributed counterparts, have been shown to be efficiently realized by quantum circuits. Here we prove that unitary 2-designs can be implemented approximately using random *diagonal*-unitaries.

Quantum Shannon theory is concerned with the evolution of quantum systems and so-called Haar random unitaries are one of the important primitives. While a Haar random unitary is a powerful tool, the number of gates required to achieve their implementation grows exponentially in the system size. Unitary designs represent finite approximations of Haar random unitaries and, unitary 2-designs in particular, have been shown to be suitable for replacing Haar random unitaries in many protocols. Unitary 2-designs can be implemented efficiently using Clifford circuits [1] and random quantum circuits [2] and among the most notable results is the recent breakthrough of Cleve *et al.* [3] demonstrating a "near linear" implementation of an exact unitary 2-design.

This motivates the question of how simply unitary 2-designs can be achieved. In this work [4], we show that unitary 2-designs can be realized to arbitrary precision by alternately applying random Z- and X-diagonal unitaries. Here, a random W-diagonal unitary D^W $(W = X, Z)$ is a random variable taking a value in a set of unitaries diagonal in the Pauli-W basis according to a probability measure D_W induced by a uniform probability measure on the parameter space $[0, 2\pi)^d$. Our main result is that $D[\ell] := D^Z_{\ell+1} D^X_\ell D^Z_\ell \cdots D^X_2 D^Z_2 D^X_1 D^Z_1$, where D^W_i $(i = 1, \ldots, \ell + 1,\ W = X, Z)$ are independent random W-diagonal unitaries, quickly approaches a unitary 2-design with increasing ℓ.

Theorem 1. *A random unitary matrix $D[\ell]$ on an N-qubit system is an ϵ-approximate unitary 2-design for $\ell \geq 2 + \frac{1}{N}(1 + \log 1/\epsilon)$. Conversely, $D[\ell]$ cannot be an ϵ-approximate unitary 2-design if $\ell \leq \frac{1}{N} \log 1/\epsilon$.*

The key component of the proof is a map given by $\mathcal{R} := \mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X} \circ \mathcal{G}^{(2)}_{D^Z}$, where $\mathcal{G}^{(2)}_U(X) := \mathbb{E}_U[U^{\otimes 2} X U^{\dagger \otimes 2}]$ for any $X \in \mathcal{B}(\mathcal{H}^{\otimes 2})$ and $\mathbb{E}_U$ represents an expectation over a random unitary matrix U. We show that this map strongly, but not completely, scrambles the symmetric and the antisymmetric subspaces in $\mathcal{H}^{\otimes 2}$. This scrambling property of $\mathcal{R}$ makes $D[\ell]$ approach a unitary 2-design very quickly.

Combining Theorem 1 with the result in Ref. [5], we also provide a simple quantum circuit that efficiently achieves a unitary 2-design. The circuit consists of repeating three steps; single-qubit phase gates on all qubits, the controlled-Z gates acting on every pair of qubits with probability $1/2$, and the Hadamard gates on all qubits. The total number of gates is at most $3N(N + \frac{1}{2} \log 1/\epsilon) + O(N)$, which is as efficient as most of the previous unitary 2-designs [1,2] but is worse than the recent one [3].

Along with theoretical interest, the significance of our result lies in its simple implementation. Indeed, all the gates in the first two steps of the circuit are commuting, and they can be applied, in principle, simultaneously. As the non-commuting part of the circuit is depth $O(1)$, this leads to a vast reduction in the execution time of the overall circuit.

Acknowledgement– YN is a JSPS Research Fellow and is supported by JSPS Postdoctoral Fellowships for Research Abroad. CH and CM acknowledge support from the EU grants SIQS and QFTCMPS and by the cluster of excellence EXC 201 Quantum Engineering and Space-Time Research. AW is supported by the European Commission (STREP "RAQUEL"), the European Research Council (Advanced Grant "IRQUAT"), the Spanish MINECO, projects FIS2008-01236 and FIS2013-40627-P, with the support of FEDER funds, as well as by the Generalitat de Catalunya, CIRIT project no. 2014 SGR 966.

References

1. D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory, 48:580, 2002; C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A, 80:012304, 2009.
2. A. W. Harrow and R. A. Low, Commun. Math. Phys., 291:257, 2009. I. T. Diniz and D. Jonathan, Commun. Math. Phys., 304:281, 2011.
3. R. Cleve, D. Leung, L. Liu, and C. Wang, arXiv:1501.04592, 2015.
4. Y. Nakata, C. Hirche, C. Morgan, and A. Winter, arXiv: 1502.0751, 2015.
5. Y. Nakata, M. Koashi, and M. Murao, New J. Phys., 16:053043, 2014.

Quantum Circuits for Isometries

Raban Iten[1], Roger Colbeck[2], Ivan Kukuljan[3], Jonathan Home[4], and Matthias Christandl[5]

1 **M.Sc. student of Physics at ETH Zürich, Department of Physics, Switzerland**
`itenr@student.ethz.ch`
2 **Department of Mathematics, University of York, UK**
3 **M.Sc. student of mathematical physics at the University of Ljubljana, Faculty of Mathematics and Physics, Slovenia**
4 **Institute for Quantum Electronics, ETH Zürich, Switzerland**
5 **Department of Mathematical Sciences, University of Copenhagen, Denmark**

Abstract

Every quantum operation can be decomposed into a sequence of single-qubit and Controlled-NOT (C-NOT) gates [1]. In many experimental architectures, the C-NOT gate is relatively 'expensive' and hence it is desirable to keep the number of these as low as possible. Previous work has looked at C-NOT-efficient synthesis of arbitrary unitaries and state preparation (see for example [5, 4] and references therein). Here we consider the generalization to arbitrary isometries from m qubits to n qubits. We derive a theoretical lower bound on the number of C-NOT gates required to decompose an isometry for arbitrary m and n, and give an explicit gate decomposition that achieves this bound up to a factor of about two in the leading order. We also perform some bespoke optimizations in the case of small m and n. In addition, we show how to apply our result for isometries to give a decomposition scheme for an arbitrary quantum operation via Stinespring's theorem, and derive a lower bound on the number of C-NOTs in this case too.

1 Summary of our Technical Version (arXiv:1501.06911)

We introduce a decomposition scheme for an arbitrary isometry V from m to n qubits that uses about twice as many C-NOT gates as required by the theoretical lower bound for large n. A factor of two between the upper and lower bounds is also known to be achievable using the best known decompositions for arbitrary quantum gates [5] and for state preparation [2, 4] (cf. Table 1). Thinking of V in terms of its $2^n \times 2^m$ matrix representation, our decomposition generates the isometry column by column. We can alternatively represent our isometry in terms of a $2^n \times 2^n$ unitary matrix $G^\dagger$ by writing $V = G^\dagger I_{2^n \times 2^m}$, where $I_{2^n \times 2^m}$ denotes the first 2^m columns of the $2^n \times 2^n$ identity matrix. Note that $G^\dagger$ is not unique (unless $m = n$). Physically, we can think of a system, where $n - m$ qubits start in the basis state $|0\rangle$ and the state of the other m qubits is arbitrary and whose evolution is described by the unitary $G^\dagger$.

We decompose a gate of the form $G^\dagger$ in terms of C-NOTs and single-qubit gates. Since a C-NOT gate is inverse to itself and the inverse of a single-qubit gate is another single-qubit gate, this is equivalent to an analogous decomposition of a quantum gate G satisfying $I_{2^n \times 2^m} = GV$. Our technique works by constructing a sequence of unitary matrices that when applied to V successively bring it closer to $I_{2^n \times 2^m}$. We do one column at a time, first choosing a sequence of quantum gates, corresponding to G_0 that get the first column right, i.e., $G_0 V|0\rangle^{\otimes m} = I_{2^n \times 2^m}|0\rangle^{\otimes m} = |0\rangle^{\otimes n}$. We then use G_1 to get the second column right without affecting the first, i.e., $G_1 G_0 V(|0\rangle^{\otimes(m-1)} \otimes |1\rangle) = I_{2^n \times 2^m}(|0\rangle^{\otimes(m-1)} \otimes |1\rangle) = |0\rangle^{\otimes(n-1)} \otimes |1\rangle$ and $G_1 G_0 V|0\rangle^{\otimes m} = G_1|0\rangle^{\otimes n} = |0\rangle^{\otimes n}$, and so on. For the first column a decomposition scheme for state preparation can be used (in reverse). However, this idea does not work for the second column, since the operator performing the inverse of state preparation on the second column wouldn't act trivially on $|0\rangle^{\otimes n}$ in general. We therefore introduce a modified

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

	State preparation	$1 \leqslant m \leqslant n-2$ to n Iso. (CCD)	$n-1$ to n Iso. (CSD)	Arbitrary n-qubit gate
#C-NOT	$\frac{23}{24}2^n - 2 \cdot 2^{\frac{n}{2}} + \frac{5}{3}$, n even [4] $\frac{23}{24}2^n - \frac{3}{2}2^{\frac{n+1}{2}} + \frac{4}{3}$, n odd	$2^{m+n} - \frac{1}{24}2^n + \mathcal{O}\left(n^2\right)2^m$	$\frac{23}{64}4^n - \frac{5}{4}2^n + 1$	$\frac{23}{48}4^n - \frac{3}{2}2^n + \frac{4}{3}$ [5]
LB	$\lceil \frac{1}{2}\left(2^n - n - 1\right) \rceil$ [4]	$\lceil \frac{1}{2}2^{m+n} - \frac{1}{4}\left(2^{2m} + 2n + m + 1\right) \rceil$	$\lceil \frac{3}{16}\left(4^n - 4n\right) \rceil$	$\lceil \frac{1}{4}\left(4^n - 3n - 1\right) \rceil$ [6]

Table 1 Best known C-NOT counts for m to n isometries for large n and lower bounds. As is to be expected, the number of required C-NOT gates increases if m increases. Or in other words, the cost of the computation is found to be lower when more of the input data is fixed. Abbreviations: LB: Lower bound; CCD: Column by Column Decomposition of an isometry (our first technique); CSD: Decomposition of an isometry using the Cosine-Sine Decomposition (our second technique).

technique that takes this into account while only slightly increasing the number of C-NOT gates needed over that required for state preparation on each column. This technique borrows a decomposition scheme for uniformly controlled gates from [2]. We describe this technique in our work and give a rigorous proof that it works for arbitrary isometries in the Appendix. This proof can also be seen as an alternative way [1] to prove the universality of the gate library containing single-qubit and C-NOT gates.

Remark: In the cases $m = n$ and $m = n - 1$, it turns out that there is a more efficient decomposition based on the Cosine-Sine Decomposition. In the case $m = n$, this is exactly the decomposition used in [5] for arbitrary gate synthesis. For $m = n - 1$ an adaptation of this technique can be used to give a lower C-NOT count than our first method. This is also displayed in Table 1.

2 Applications and Future Work

Experimental groups strive to demonstrate their ability to control a small number of qubits, and the ultimate demonstration would be the ability to do any quantum operation on them. Since any such operation can be implemented via an isometry followed by partial trace (using Stinespring's theorem), our decomposition scheme for isometries points towards an efficient way to synthesize quantum operations, and could also be used in the construction of arbitrary POVMs. In fact, we derive a theoretical lower bound on the number of C-NOT gates required to implement an arbitrary completely positive trace-preserving map in the quantum circuit model and show that we can achieve this bound up to a factor of four in leading order using our decomposition scheme for isometries. Alternative methods for the implementation of quantum channels are described in [7] and [3], which allow for additional classical randomness to implement the channel. In future work we will investigate how to use our approach in an alternative model that allows either measurements or classical randomness as additional resources, in order to further improve the C-NOT counts.

References

1 A. Barenco et al. *Physical Review A*, 52(5):3457–3467, November 1995.
2 Ville Bergholm et al. *Phys. Rev. A*, 71:052330, May 2005.
3 Marco Piani et al. *Phys. Rev. A*, 84:032304, Sep 2011.
4 Martin Plesch and Časlav Brukner. *Physical Review A*, 83(3):032302, March 2011.
5 Vivek V. Shende, Stephen S. Bullock, and Igor L. Markov. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(6):1000–1010, June 2006.
6 Vivek V. Shende et al. *Physical Review A*, 69(6):062321, June 2004.
7 Dong-Sheng Wang et al. *Phys. Rev. Lett.*, 111:130504, Sep 2013.

Quantum property testing: A survey and one new result

Ronald de Wolf

CWI, Amsterdam

Abstract. "Property testers" are algorithms that can efficiently handle very large amounts of data: given a large object that either has a certain property or is somehow far from having that property, a tester should efficiently distinguish between these two cases. In this talk we describe recent results obtained for quantum property testing. This area naturally falls into three parts. First, we may consider quantum testers for properties of classical objects. We survey the main examples known where quantum testers can be much more efficient than classical testers. We also describe one new result: a quantum algorithm for testing whether a given n-bit Boolean function f is a k-junta (i.e., depends on only k of the n input bits) using roughly $\sqrt{k}$ queries to f, which is quadratically faster than the best classical testers. Second, we may consider classical testers of quantum objects. This is the situation that arises for instance when one is trying to determine if untrusted quantum states or operations are what they are supposed to be, based only on classical input-output behavior. Finally, we may also consider quantum testers for properties of quantum objects, such as whether two states or unitaries are equal, whether a state is separable, etc.
This is based on joint work with Ashley Montanaro (survey arXiv:1310.2035) and with Andris Ambainis, Aleksanders Belovs, and Oded Regev (k-junta testing).

Hierarchy of efficiently computable and faithful lower bounds to quantum discord

Marco Piani[1,2]

[1] Department of Physics & Astronomy and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
[2] SUPA and Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK

Abstract. Quantum discord expresses a fundamental non-classicality of correlations more general than quantum entanglement, but its evaluation is challenging. We combine the no-local-broadcasting theorem, semidefinite-programming characterizations of quantum fidelity and quantum separability, and a recent breakthrough result of Fawzi and Renner about quantum Markov chains to provide a hierarchy of computationally efficient lower bounds to quantum discord. Such a hierarchy converges to the surprisal of measurement recoverability introduced by Seshadreesan and Wilde, and provides a faithful lower bound to quantum discord already at the lowest non-trivial level. Furthermore, the latter constitutes by itself a valid discord-like measure of the quantumness of correlations.

Quantum discord was introduced in terms of the minimum amount of correlations, as quantified by mutual information, that is necessarily lost in a local quantum measurement of a bipartite quantum state [1, 2] (see below for exact definitions). Standard quantum discord is not easily computed even in simple cases, and general easily computable *lower* bounds to it are similarly not known. In this paper we provide a family of lower bounds for the standard quantum discord which can reliably be computed numerically. On the other hand, all the bounds have physical meaning, since they are based on 'impossibility features' (i.e., no-go theorems) related to the local manipulation of quantum correlations; in particular, they are based on the no-local-broadcasting theorem [3, 4]. Furthermore, such lower bounds satisfy the basic requests that should be imposed on any meaningful measure of quantum correlations [5, 6], hence making each quantifier in the hierarchy a valid discord-like quantifier in itself.

The hierarchy of lower bounds that we introduce exploits ideas used in the characterization and detection of entanglement via semidefinite programming [7–9]. Semidefinite programming optimization techniques [10] have found many other significant applications in quantum information (see, e.g., [11–19]), and, in recent times, they have been used also in the

quantification of steering [20, 21]. Here we extend the use of semidefinite programming for the study of quantum correlations to quantum discord.

References

1. Ollivier, H., Zurek, W.H.: Quantum discord: a measure of the quantumness of correlations. Physical review letters **88**(1) (2001) 017901
2. Henderson, L., Vedral, V.: Classical, quantum and total correlations. Journal of physics A: mathematical and general **34**(35) (2001) 6899
3. Piani, M., Horodecki, P., Horodecki, R.: No-local-broadcasting theorem for multipartite quantum correlations. Physical review letters **100**(9) (2008) 090502
4. Luo, S., Sun, W.: Decomposition of bipartite states with applications to quantum no-broadcasting theorems. Physical Review A **82**(1) (2010) 012338
5. Brodutch, A., Modi, K.: Criteria for measures of quantum correlations. Quantum Information and Computation **12** (2012) 0721
6. Piani, M.: Problem with geometric discord. Physical Review A **86**(3) (2012) 034101
7. Doherty, A.C., Parrilo, P.A., Spedalieri, F.M.: Distinguishing separable and entangled states. Phys. Rev. Lett. **88** (Apr 2002) 187904
8. Doherty, A.C., Parrilo, P.A., Spedalieri, F.M.: Complete family of separability criteria. Phys. Rev. A **69** (Feb 2004) 022308
9. Doherty, A.C.: Entanglement and the shareability of quantum states. Journal of Physics A: Mathematical and Theoretical **47**(42) (2014) 424004
10. Boyd, S., Vandenberghe, L.: Convex optimization. Cambridge University Press (2009)
11. Nowakowski, M.L., Horodecki, P.: A simple test for quantum channel capacity. Journal of Physics A: Mathematical and Theoretical **42**(13) (2009) 135306
12. Jain, R., Ji, Z., Upadhyay, S., Watrous, J.: QIP = PSPACE. Journal of the ACM (JACM) **58**(6) (2011) 30
13. Kempe, J., Regev, O., Toner, B.: Unique games with entangled provers are easy. SIAM Journal on Computing **39**(7) (2010) 3207–3229
14. Navascués, M., Pironio, S., Acín, A.: Bounding the set of quantum correlations. Phys. Rev. Lett. **98** (2007) 010401
15. Watrous, J.: Semidefinite programs for completely bounded norms. Theory of Computing **5** (2009)
16. Johnston, N., Kribs, D.W.: A family of norms with applications in quantum information theory. Journal of Mathematical Physics **51**(8) (2010) 082202
17. Eisert, J., Brandao, F., Audenaert, K.: Quantitative entanglement witnesses. New Journal of Physics **9**(3) (2007) 46
18. Eisert, J., Hyllus, P., Gühne, O., Curty, M.: Complete hierarchies of efficient approximations to problems in entanglement theory. Physical Review A **70**(6) (2004) 062317
19. Moroder, T., Bancal, J.D., Liang, Y.C., Hofmann, M., Gühne, O.: Device-independent entanglement quantification and related applications. Physical review letters **111**(3) (2013) 030501
20. Skrzypczyk, P., Navascués, M., Cavalcanti, D.: Quantifying einstein-podolsky-rosen steering. Phys. Rev. Lett. **112** (2014) 180404
21. Piani, M., Watrous, J.: Necessary and Sufficient Quantum Information Characterization of Einstein-Podolsky-Rosen Steering. Phys. Rev. Lett. **114** (2015) 060404

Quantum capacity can be greater than private information for arbitrarily many uses

(arXiv:1502.05326)

David Elkouss[1] and Sergii Strelchuk[2]

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

2 **Department of Applied Mathematics and Theoretical Physics,**
University of Cambridge, Cambridge CB3 0WA, U.K.
ss870@cam.ac.uk

Abstract

The quantum capacity of a quantum channel is always smaller than the capacity of the channel for private communication. However, both quantities are given by the infinite regularization of respectively the coherent and the private information. Here, we construct a family of channels for which the private and coherent information can remain strictly superadditive for unbounded number of uses. We prove this by showing that the coherent information is strictly larger than the private information of a smaller number of uses of the channel. It turns out that even though the quantum capacity is upper bounded by the private capacity, the non-regularized quantities can be interleaved. From an operational point of view, the private capacity can be used for gauging the practical value of quantum channels for secure communication and, consequently, for key distribution. We thus show that in order to evaluate the interest a channel for this task it is necessary to optimize the private information over an unlimited number of uses of the channel.

How well is it possible to characterize the resources available to transmit information? In classical information theory, this proves to be fully within our computational abilities: given a description of a channel, answering the question about its capacity to convey information to the receiver is straightforward. To compute a number of different types of capacity of the quantum channel, defined as regularized quantities, it is necessary to perform an unbounded optimization over the number of the copies of the channel.

From the above expressions it follows that one might have to optimize over an *infinite* number of copies of the channel in order to compute its capacity. Do we have to resort to the regularized expression in order to compute the capacity of a quantum channel? It has recently been shown that at least in the case of the quantum capacity this is unavoidable even when we attempt to answer the question whether the channel has any capacity at all. For the classical capacity, which is known to be superadditive for two uses of the channel, there is some evidence that ultimately the regularization might not be required.

Arguably, the biggest practical success of quantum information theory to date is the possibility of quantum key distribution (QKD). QKD allows two distant parties to agree on a secret key independent of any eavesdropper. The required assumptions are: access to a quantum channel with positive private capacity and the validity of quantum physics[1]. On

[1] In order to characterize the channel and to implement a specific QKD protocol one might need a public authentic classical channel or a small preshared secret.

the other hand, key distribution is a primitive that can only be implemented with classical resources if one is willing to constrain the power of the eavesdropper. Even though there exist practical QKD schemes which enable secure communication over large distances with high key rates, some of the fundamental questions about the capacity to transmit secure correlations remain unanswered.

The private capacity $\mathcal{P}$ of a channel is used to describe the ability of the channel to send secure messages to the receiver. It has a clear operational interpretation as the maximum rate at which the sender, Alice, can send private *classical* communication to the receiver, Bob. It is defined as follows:

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}). \tag{1}$$

The private capacity is given by the regularization of $\mathcal{P}^{(1)}(\mathcal{N})$, the private information of the channel, which is given by $\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B) - I(X;E)$, where $\mathcal{R}$ is the set of c-q states. One can view private capacity as the optimal rate of reliable communication keeping Eve in a product state with Alice and Bob.

Here we show that private information can be strictly superadditive for an arbitrarily large number of uses of the channel. We construct a family of channels for which the private and coherent information can remain strictly superadditive any number of uses of the channel. We are able to prove this result by showing that the private information of k uses of the channel is smaller than the coherent information of $k+1$ uses. It turns out that both quantities can be interleaved use after use for the first n uses of the channel. This shows that even though the quantum capacity is upper bounded by the infinite regularization of the private information, the quantum capacity can be larger than a finite regularization of the private information. We proved that in order to compute the private capacity it is necessary to consider regularized expressions (1).

More precisely, we prove the following theorem:

▶ **Theorem 1.** *For any n there exists a triple (n,p,d) and a quantum channel $\mathcal{N}_{n,p,d}$ such that for $n > k \geq 1$:*

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}) < \frac{1}{k+1}\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k+1}). \tag{2}$$

This proves that entangled inputs increase the private information of a quantum channel and this effect persists for an *arbitrary* number of channel uses. Also, we show that the coherent information may be greater than the private information and this effect exists for arbitrary many uses of the channel. As a bonus, we obtain a qualitatively different proof for the unbounded superadditivity of the coherent information proved in arXiv:1408.5115.

Round elimination in exact communication complexity

Jop Briët[1], Harry Buhrman[2], Debbie Leung[3], Teresa Piovesan[2], and Florian Speelman[2]

[1] Courant Institute, New York University, USA.
[2] Centrum Wiskunde & Informatica (CWI), The Netherlands.
[3] University of Waterloo, Canada.

We study two basic graph parameters, the chromatic number and the orthogonal rank, in the context of classical and quantum exact communication complexity. In particular, we consider two types of communication problems that we call *promise equality* and *list* problems. For both of these, it was already known that the one-round classical and one-round quantum complexities are characterized by the chromatic number and orthogonal rank of a certain graph, respectively.

In a promise equality problem, Alice and Bob must decide if their inputs are equal or not. We prove that classical protocols for such problems can always be reduced to one-round protocols with no extra communication. In contrast, we give an explicit instance of a promise problem that exhibits an exponential gap between the one- and two-round exact quantum communication complexities. Whereas the chromatic number thus captures the complete complexity of promise equality problems, the hierarchy of "quantum chromatic numbers" (starting with the orthogonal rank) giving the quantum communication complexity for every fixed number of communication rounds thus turns out to enjoy a much richer structure.

In a list problem, Bob gets a subset of some finite universe, Alice gets an element from Bob's subset, and their goal is for Bob to learn which element Alice was given. The best general lower bound (due to Orlitsky) and upper bound (due to Naor, Orlitsky, and Shor) on the classical communication complexity of such problems differ only by a constant factor. We exhibit an example showing somewhat surprisingly that the four-round protocol used in the bound of Naor et al. can in fact be optimal, and that the constant-factor gap cannot be closed in the general. Finally, we pose a conjecture on the orthogonality rank of a certain graph whose truth would imply an intriguing impossibility of *round elimination* in quantum protocols for list problems, something that works trivially in the classical case.

Rate-loss analysis of an efficient quantum repeater architecture

Saikat Guha[1], Hari Krovi[1], Christopher A. Fuchs[1,2], Zachary Dutton[1], Joshua A. Slater[3,4], Christoph Simon[4], and Wolfgang Tittel[4]

[1] Raytheon BBN Technologies, 10 Moulton Street, Cambridge, MA USA 02138
[2] University of Massachusetts Boston, 100 Morrissey Blvd., Boston, MA USA 02125
[3] Faculty of Physics, University of Vienna, 1090 Vienna, Austria
[4] Department of Physics and Astronomy, University of Calgary, Alberta, T2N 1N4

We analyze an entanglement-based quantum key distribution (QKD) architecture that uses a linear chain of quantum repeaters employing photon-pair sources, spectral multiplexing, probabilistic Bell-state measurements, multi-mode quantum memories and classical-only error correction, i.e., no quantum error correction or purification. Assuming sources with zero multi-photon emission probability, we find an *exact* analytical description of how the density operator of the end-to-end shared entangled state evolves through the repeater chain, the secret-key rate (if that shared entanglement is consumed for QKD), entanglement-distillation rate, and fidelity [1]. We show via an explicit calculation, that this multiplexing based protocol achieves a secret key rate that surpasses the TGW bound [2]—a recently-found fundamental limit to the rate-vs.-loss scaling achievable by any QKD protocol over a direct optical link—thereby providing one of the first rigorous proofs of the efficacy of a quantum repeater protocol. We extend our theoretical analysis to encompass sources with non-zero two-pair-emission probability $p(2)$, using an efficient exact numerical evaluation of the quantum state propagation and measurements. When all the multi-photon events—resulting either from non-zero $p(2)$, or from detector noise such as dark click probability P_d—are zero, then quantum error correction or purification add no value to a repeater protocol, since the average rate at which (perfect) EPR pairs are heralded by Alice and Bob translates to the key rate. However, when the multi-photon events are non-zero, the heralded states are impure, and when such impurity surpasses a certain threshold, repeater purification and quantum error correction at the repeaters could perform better.

Our main results are: (a) an exact evaluation of the evolving noisy shared-entangled state and a recursive description of the QBER through concatenated stages, (b) an achievable key rate of the form $A\eta^s$ bits/mode, $s < 1$, which beats the TGW scaling limit of $s = 1$, (c) that P_d does not have an effect on the rate-loss envelope until it crossed a certain threshold

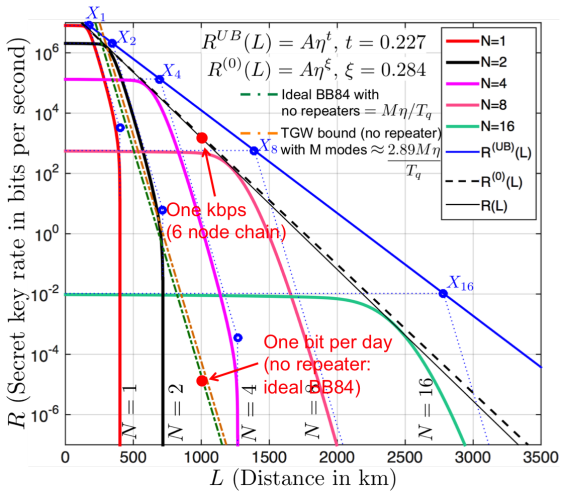


Fig. 1. Key rates as a function of range for $N = 1, 2, 4, \ldots, 16$ elementary links. The rate envelope outperforms what is theoretically achievable by any repeater-less QKD protocol that uses the same time-slot length (T_q) and number of frequency channels (M). Also shown is the *exact* zero-dark-click-probability rate-distance envelope, $R^{(0)}(L) = A\eta^\xi$, where $\xi = 0.284$ for the chosen parameters, which are: $P_d = P_r = P_e = 3 \times 10^{-5}$, $\eta_d = \eta_r = \eta_e = 0.9$, $\lambda_m = 1$ dB (memory loading-readout efficiency), $M = 1000$ (frequency modes), $\alpha = 0.15$ dB/km (fiber loss), $T_q = 50$ ns.

that is significantly high for practical detectors (even through the individual rate curves for some finite number of links become zero at deminishing P_d-dependent maximum ranges), and that (d) non-zero source $p(2)$ determines $N_{\max}$, a maximum number of links concatenating beyond which brings down the rate sharply to zero. The main result relies on an exact solution of a variant of the *logistic map*, solutions to which in general are known to be chaotic. For detailed calculations, please see [1].

We expect our results to spur formal rate-loss analyses of other quantum repeater protocols—for instance ones that do use quantum logic for purification and error correction, and long-coherence-length quantum memories to support such protocols,—and also to provide useful abstractions to seed analyses of quantum networks of complex topologies.

References

1. S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton. J. A. Slater, C. Simon, and W. Tittel, "Rate-loss analysis of an efficient quantum repeater architecture", arXiv:1404.7183v4 [quant-ph] (2015).
2. M. Takeoka, S. Guha and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution", Nature Communications **5**, 5235 (2014).

Renormalising entanglement distillation

Stephan Waeldchen[1], Janina Gertis[1], Earl T. Campbell[2], and Jens Eisert[1]

[1] Dahlem Center for Complex Quantum Systems, Freie Universitaet Berlin, 14195 Berlin, D
[2] Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, UK

http://arxiv.org/abs/1503.04822

Entanglement distillation refers to the task of transforming a collection of weakly entangled pairs into fewer highly entangled ones. It is a core ingredient in quantum repeater protocols, needed to transmit entanglement over arbitrary distances in order to realise quantum key distribution schemes. Usually, it is assumed that the initial entangled pairs are i.i.d. distributed and uncorrelated with each other, an assumption that might not be reasonable at all in any entanglement generation process involving memory channels. Here, we introduce a framework that captures entanglement distillation in the presence of natural correlations arising from memory channels. Conceptually, we bring together ideas from condensed-matter physics - that of renormalisation and of matrix-product states and operators - with those of local entanglement manipulation, Markov chain mixing, and quantum error correction. We identify parameter regions for which we prove convergence to maximally entangled states, arising as the fixed points of a matrix-product operator renormalisation flow.

We consider a sequence of L pairs of qubits, where two parties (say Alice and Bob) each hold one qubit from each pair. These pairs are entangled, as well as correlated with each other, as a consequence of the preparation procedure involving stationary quantum memory effects. A natural preparation exhibiting such a memory involves an auxiliary quantum system C of some dimension d that embodies all the degrees of freedom of the memory. The state is then prepared in a sequential fashion, with the memory unitarily interacting with the first entangled pair, then the second, and so on [1, 2, 3]. A state generated in this way is given by a matrix-product state, if it is pure, or a *matrix-product operator* in case of noisy mixed states [4, 5], as they are considered here, with d taking the role of the *bond dimension*. The decay of memory effects in the distance between the entangled pairs naturally emerges in this construction. We introduce here how naturally correlated bi-partite MPO arising from this setting. More specifically, we work in a numerically indexed Bell basis $(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle)$, more commonly labelled as $(|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle)$. We consider a sequence of L pairs of qubits, with basis vectors $|\Phi_{\mathbf{x}}\rangle = |\phi_{x_1}\rangle |\phi_{x_2}\rangle \dots |\phi_{x_L}\rangle$, where Alice holds the first qubit of each pair and Bob holds its partner. Translationally invariant mixed states reflecting stationarity of the source are described in the MPO language as

$$\langle \Phi_{\mathbf{x}}| \rho |\Phi_{\mathbf{y}}\rangle = \mathrm{Tr}\left[M^{x_1,y_1} M^{x_2,y_2} \dots M^{x_L,y_L}\right].$$

Purely for simplicity of notation, we take periodic boundary conditions here. The dimension of the matrices $M^{x,y} \in \mathbb{C}^{d\times d}$, $x, y \in \{1, \dots, 4\}$ limits the correlations between pairs, and by increasing this bond dimension d, arbitrary quantum states can be described in this formalism. There is a gauge freedom in our choice of MPO matrices as for any invertible S, mapping $M^{x,y} \mapsto S M^{x,y} S^{-1}$ will give an alternative description of the same physical state. Generally, 16 matrices are needed for the description of each pair, reflecting the two-particle density matrix. However, without loss of generality we take $M^{x,y}$ to be Bell diagonal, which can be achieved using a suitable local group twirl over the Pauli group [6]. For this reason we use the shorthand $A = M^{1,1}$, $B = M^{2,2}$, $C = M^{3,3}$ and $D = M^{4,4}$. Without loss of generality, we consider the distillation of maximally entangled ϕ^+ pairs. The "A" matrix will be the dominant matrix, while the others we will call noise matrices.

The recurrence protocol is a $2 \to 1$ iterative protocol which uses post-selection. At every round measurement outcomes are being produced and we only proceed if certain outcomes are

obtained. Here we use a slightly improved version [7] of the recurrence scheme [6]. Cast into the MPO language, the iteration formula after two steps is

$$A_{n+2} = (A_n^2 + B_n^2)^2 + (C_n^2 + D_n^2)^2, \qquad C_{n+2} = \{A_n^2 + B_n^2, C_n^2 + D_n^2\},$$
$$B_{n+2} = \{A_n, B_n\}^2 + \{C_n, D_n\}^2, \qquad D_{n+2} = \{\{A_n, B_n\}, \{C_n, D_n\}\},$$

where curly brackets denote the anti-commutator. After two steps, the matrices are being re-gauged and rescaled. Replacing matrices by commuting scalars recovers the original i.i.d. result. We introduce the noise contribution of the coefficient matrices B_n, C_n, and D_n as

$$\epsilon_n = \max\left(\|\mathcal{B}_n\|_{1\to1}, \|\mathcal{C}_n\|_{1\to1}, \|\mathcal{D}_n\|_{1\to1}\right).$$

Due to norm sub-multiplicativity, one finds initially small ϵ_0 entails ϵ_n vanishes with n. However, ensuring A_{n+2} stays large is difficult. To do so, we shall adjust the MPO gauge after two steps, re-gauging this using a suitable gauge transformation and re-scaling, so that $\mathcal{A}_{n+2}$ is trace-preserving and hence $\|\mathcal{A}_{n+2}\|_{1\to1} = 1$. To quantify how much the gauge transformation changes the matrix norm, we rely on the *ergodicity coefficient* τ of the matrices,

$$\tau(\mathcal{M}) = \max_{\mathrm{Tr}[\sigma]=0} \frac{\|\mathcal{M}(\sigma)\|_1}{\|\sigma\|_1},$$

which allows a quantification of how rapidly a channel mixes input states into the channel's stationary state. We are interested in the ergodicity of $\mathcal{A}_n$, for which we use the shorthand $\tau_n := \tau(\mathcal{A}_n)$.

Given a translationally invariant Bell diagonal MPO with coefficient matrices A_0, B_0, C_0, and D_0, the iterative application of the recurrence protocol leads to convergence to uncorrelated pairs in the maximally entangled state ϕ_+ for

$$\epsilon_0 \leq \frac{1}{7}\frac{1-\tau_0^4}{1+\tau_0^4}.$$

In addition to our results on this postselective protocol, we also present results on a deterministic $5 \to 1$ protocol that deploys techniques from error correction codes.

We have introduced a framework of renormalising entanglement in order to achieve entanglement distillation in the presence of natural correlations. We have proven that protocols known to work for i.i.d. pairs above a threshold fidelity also give rise to feasible entanglement distillation if correlations are present. We have identified threshold fidelities and conditions on the correlation between the pairs to ensure convergence of correlated pairs described by an MPO to a number of independent maximally entangled pure states. The programme initiated here shows that correlations are not necessarily a disadvantage, and one does not have to aim at de-correlating pairs or resetting preparation procedures, steps that will take time and will in practice lead to further entanglement deterioration. We hope that this work triggers further studies on entanglement distillation and repeater protocols in the presence of realistic memory effects, as well as of further studies of renormalising matrix-product operators.

References

[1] C. Schoen et al. In: *Phys. Rev. Lett.* 95 (2005), p. 110503.
[2] M. B. Plenio and S. Virmani. In: *Phys. Rev. Lett.* 99 (2007), p. 120504.
[3] D. Perez-Garcia et al. In: *Quant. Inf. Comp.* 5&6 (2006), p. 401.
[4] F. Verstraete, J. J. Garcia-Ripoll, and J. I. Cirac. In: *Phys. Rev. Lett.* 93 (2004), p. 207204.
[5] M. Zwolak and G. Vidal. In: *Phys. Rev. Lett.* 93 (2004), p. 207205.
[6] C. H. Bennett et al. In: *Phys. Rev. A* 54 (1996), p. 3824.
[7] D. Deutsch et al. In: *Phys. Rev. Lett.* 77 (1996), p. 2818.

Unbounded entanglement can be needed to achieve the optimal success probability

Laura Maninska

CQT, Singapore

Abstract. Quantum entanglement is known to provide a strong advantage in many two-party distributed tasks. We investigate the question of how much entanglement is needed to reach optimal performance. We show that there exists a purely classical scenario for which no finite amount of entanglement suffices. To this end we introduce a simple two-party nonlocal game H, inspired by a paradox of Lucien Hardy. In our game each player has only two possible questions and can provide answers in a countable set. We exhibit a sequence of strategies which use entangled states in increasing dimension d and succeed with probability $1-O(d^{-c})$ for some $c \geq 0.13$. On the other hand, we show that any strategy using an entangled state of local dimension d has success probability at most $1-\Omega(d^{-2})$. In addition, we show that any strategy restricted to producing answers in a set of cardinality at most d has success probability at most $1-\Omega(d^{-2})$. Finally, we generalize our construction to derive similar results starting from any game G with two questions per player and finite answers sets in which quantum strategies have an advantage. (This is joint work with Thomas Vidick.)

Quantum enhancement of randomness distribution

Raul Garcia-Patron[1], William Matthews[2], and Andreas Winter[3]

[1] Quantum Information and Communication, Ecole Polytechnique de Bruxelles
CP 165, Universit Libre de Bruxelles, 1050 Bruxelles, Belgium
[2] Department of Applied Mathematics and Theoretical Physics
University of Cambridge, Cambridge CB3 0WA, U.K
[3] ICREA & Física Teòrica: Informació i Fenòmens Quàntics,
Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain

Randomness and information are different concepts. We think of information of as that which is sent as a specific message to another person or machine. On the other hand, randomness can be intuitively understood as the outcome of a noisy process. Information and randomness being different concepts, the capability to distribute them over a channel should be inequivalent resources. More precisely, the capability to distribute a bit of randomness is a weaker resource than the potential to communicate a bit of information over a channel.

From Shannon's definition of classical capacity of transmssion of information one can intuitively understand that any protocol that distributes randomness over a given channel $\mathcal{E}$ can be de-randomized and be transformed into a protocol that is capable of transmitting information at exactly the same rate, proving the equality $C(\mathcal{E}) = R(\mathcal{E})$. Similar result can be deduced from Ahslwede and Csiszar in [1] for its extension to asssited feedback communication, i.e., $C(\mathcal{E}) = R_{\leftarrow}(\mathcal{E})$. In this work we prove this equality remains true even if one considers the use of all kind of assisted classical communications, i.e., $C(\mathcal{E}) = R_{\leftrightarrow}(\mathcal{E})$, showing that in a classical world the optimal way of distributing randomness is to generate it locally and distribute it through the channel (full details of all arguments are to be found in reference [2]).

Interestingly, this is no longer true for quantum channels as the strong symmetry between both resources is broken when we consider assisted feedback scenarios. Similarly as in [3] it was shown that in the quantum case of distillation of randomness from a state, communication from A to B can result in a rate different that with communication from B to A, here we give an example of an entanglement-breaking channel where the following inequality holds $C(\mathcal{E}) = C_{\leftarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$, proving that quantum mechanics implies a strict separation between the capability to distribute randomness and the potential of communicating information (full details

of all arguments are to be found in reference [2]). Our result shows that contrary to what is predicted by classical information theory quantum mechanics allows for the activation of randomness initially locked inside the channel, which boost the amount of shared randomness generated in the process.

An alternative way of understanding our result is the following. Our result shows that a noisy channel $\mathcal{E}$ sending symbols from Alice to Bob combined with a noiseless channel $\mathcal{L}$ sending symbols from Bob to Alice can distribute more shared randomness between both partners when operated jointly than the optimal rate achievable when they operated independently, i.e., $R(\mathcal{E} \otimes \mathcal{L}) > R(\mathcal{E}) + R(\mathcal{L})$. Therefore, our result can also be seen as an activation phenomenon similar to the well-known activation of the quantum or secret capacities [4][5][6].

References

1. R. Ahlswede and Imre Csiszár, IEEE Trans. Info. Theory **39,** 1121–1132 (1993).
2. R. Garcia-Patron, W. Matthews, and A. Winter, article in preparation.
3. I. Devetak and A. Winter, IEEE Trans. Info. Theory **50,** 3183 (2004).
4. G Smith and J Yard, Science **321**, 1812 (2008).
5. Ke Li, Andreas Winter, XuBo Zou, GuangCan Guo Phys. Rev. Lett. **103**, 120501 (2009).
6. G. Smith and J. A. Smolin, Phys. Rev. Lett. 103, 120503 (2009).

Semidefinite programs for randomness extractors

Mario Berta[1], Omar Fawzi[2,3], and Volkher B. Scholz[4]

[1] Institute for Quantum Information and Matter, Caltech, USA
[2] Department of Computing and Mathematical Sciences, Caltech, USA
[3] LIP, École Normale Suprieure de Lyon, France
[4] Institute for Theoretical Physics, ETH Zurich, Switzerland

Abstract. Randomness extractors are an important building block for classical and quantum cryptography. However, for many applications it is crucial that the extractors are quantum-proof, i.e., that they work even in the presence of quantum adversaries. In general, quantum-proof extractors are poorly understood and we would like to argue that in the same way as Bell inequalities (multi prover games) and communication complexity, the setting of randomness extractors provides a operationally useful framework for studying the power and limitations of a quantum memory compared to a classical one.
We start by recalling how to phrase the extractor property as a quadratic program with linear constraints. We then construct a semidefinite programming (SDP) relaxation for this program that is tight for some extractor constructions. Moreover, we show that this SDP relaxation is even sufficient to certify quantum-proof extractors. This gives a unifying approach to understand the stability properties of extractors against quantum adversaries. Finally, we analyze the limitations of this SDP relaxation and propose a converging hierarchy of SDPs that gives increasingly tight characterizations of quantum-proof extractors.

Interferometric versus projective measurement of anyons

Michael Freedman and Claire Levaillant

No Institute Given

Abstract. We investigate the similarities and differences between projective measurement of a group of anyons by fusion and interferometric measurement of the same group of anyons with a Mach-Zehnder interferometer. Anyons are exotic particles which are used in topological quantum computation. Contrary to bosons or fermions, the wave-function is non longer symmetric or anti-symmetric under exchange of particles but rather acquires a non-trivial phase when one particle is moved around another. We show that interferometric measurement is stronger than projective measurement: any protocol involving projective measurement can be simulated by a protocol using interferometry. The proof is based on a novel technique used for reversing a physical phenomenon of decoherence happening during interferometry. While interferometry causes decoherence between the subsystem being measured and its complement, we show that decoherence can be reversed by adding more interferometric measurements. We illuminate the power of interferometry on some examples when we build quantum gates.

Qudit (Gauge) Colour Codes in All Spatial Dimensions

Fern H.E. Watson[1,2], Earl T. Campbell[3], Hussain Anwar[4], and Dan E. Browne[1]

[1] Department of Physics and Astronomy, University College London, WC1E 6BT.
[2] Department of Physics, Imperial College London, Prince Consort Road, SW7 2AZ.
[3] Department of Physics and Astronomy, University of Sheffield, S3 7RH.
[4] Department of Mathematical Sciences, Brunel University, Uxbridge, UB8 3PH.

http://arxiv.org/pdf/1503.08800.pdf

Quantum technologies are often developed in the qubit paradigm, where the basic carrier of quantum information is a two-level quantum system—a natural choice because binary is the language of classical technologies. However, in the quantum domain, qudits, d-level quantum systems, offer a state space with a richer structure than their two-level counterparts.

Colour codes [1–3] are a class of topological qubit stabilizer codes that may be defined on a topological space of any spatial dimension $\mu \geq 2$ [4]. Along with surface codes, they constitute the most successful topological codes. Qubit colour codes have several advantages over qubit surface codes, and we show these features can be transferred over into the qudit setting.

In this work, we generalise colour codes to any qudit dimension d and spatial dimensions μ. Specifically, given any lattice suitable for constructing qubit colour codes, we show how to use the same lattice to construct a qudit colour code. For qubits, a non-Clifford gate can be implemented in colour codes in 3 and higher spatial dimensions transversally, i.e. by a tensor product of local unitary gates, an inherently fault-tolerant procedure [5, 6], and we generalise this result to the qudit paradigm.

Recently, it was shown by Bravyi and König [7] that a quantum error correcting code in μ spatial dimensions can support a gate with constant depth from at most the μth level of the Clifford hierarchy. The fact that colour codes can be shown to saturate this bound with transversal gates is a very promising feature, and when combined with gauge fixing techniques [2, 8] enables universal quantum computation without the need of magic state distillation [9]. We find that 3D colour codes also provide transversal non-Cliffords in the qudit case.

The colour codes have also been generalised to gauge colour codes [10]—subsystem codes with many advantageous features—including low weight error detection measurements, universal transversal gates via gauge fixing

for $\mu > 2$, fault-tolerant conversion between codes of different spatial dimension [11], and for the $\mu = 3$ case, single shot error correction [12]—a robustness to measurement errors without the need for repeated measurements. We show that the qudit colour codes introduced here can also be generalised to gauge colour codes.

The main technique which we employ is a bipartition of the vertices in the graph that defines the code into *starred* and *unstarred* vertices. We call this the *star-bipartition*, to distinguish it from the other important colourings which define the colour codes. The commutation properties of the stabilizer and logical operators of the colour codes (and gauge colour codes) in the qubit setting can be reduced to the fact that the pairs of operators $X \otimes X$ and $Z \otimes Z$ commute. The star-bipartition we introduce replaces operators with their complex conjugate on a subset of the vertices, for example, replacing the above operators with $X \otimes X^*$ and $Z \otimes Z^*$, respectively. Crucially, this latter pair of operators commutes for qudits of any dimension. Furthermore, the star-bipartition provides a general framework for constructing transversal gates from higher levels of the Clifford hierarchy. While elements of this technique can be seen in earlier work [13, 10], this is the first time that it has been exploited systematically.

The second key technical component of our work is a generalisation of the triorthogonal matrix technique by Bravyi and Haah [14]. Bravyi and Haah prove that a so-called triorthogonal code supports a transversal non-Clifford gate in the 3rd level of the Clifford hierarchy. In this talk we show that qudit colour codes in 3 and higher spatial dimensions obey a generalised notion of triorthogonality and as a result, support transversal non-Clifford gates.

References

1. H. Bombin and M.A. Martin-Delgado, Phys. Rev. Lett. **98**, 160502 (2007)
2. H. Bombin, arXiv:1311.0879.
3. A. Kubica and M.E. Beverland, arXiv:1410.0069.
4. H. Bombin and M.A Martin-Delgado, Phys. Rev. B **75**, 075103 (2007).
5. E. Knill, R. Laflamme and W.H. Zurek, arXiv:quant-ph/9610011.
6. E. Knill, R. Laflamme and W.H. Zurek, Science **279**, 342-345 (1998).
7. S. Bravyi and R. König, Phys. Rev. Lett. **110**, 170503 (2013).
8. A. Paetznick and B.W Reichardt, Phys. Rev. Lett. **111**, 090505 (2013).
9. S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
10. H. Bombin, arXiv:1311.0879.
11. H. Bombin, arXiv:1412.5079.
12. H. Bombin, arXiv:1404.5504.
13. P. Sarvepalli, *IEEE ITW* 1–5 (2010).
14. S. Bravyi and J. Haah, Phys. Rev. A **86** 052329 (2012).

Thermalization and decoherence in open Majorana systems

Earl T. Campbell

Department of Physics & Astronomy, University of Sheffield, Sheffield, S3 7RH, United Kingdom.

http://arxiv.org/abs/1502.05626

In topologically ordered systems, information is stored non-locally within the degenerate ground space of some large many-body system. The primary benefit of topology is robustness against random adiabatic fluctuations in the system Hamiltonian. Damage from such noise is exponentially suppressed with system size. Topological systems also have an energy gap Δ between the degenerate ground space and excited states, and are said to be protected by the gap against thermal excitations. A common claim [1] is that thermal processes occur at a rate $e^{-\Delta/T}$, which is sometimes called the Arrhenius law. A often voiced assertion is that topology can exponentially eliminate noise merely by increasing system size and decreasing temperature.

Of all topological systems, Majorana zero modes have attracted the most attention. It was theorized that a so-called Kitaev wire supports Majorana zero modes at edges of a simple 1D system [5]. Beyond topological robustness, Majorana zero-modes also possess the braiding statistics of non-Abelian Ising anyons. Though insufficient for direct quantum computation, braiding Ising anyons can demonstrate nonlocality, teleportation and superdense coding [2], and are promoted to full quantum computing when supplemented with some nontopological (noisy) operations [4].

The physics of these Majorana systems is especially tractable as their Hamiltonians are quadratic in fermion creation and annihilation operators. We say such a system is Gaussian, or quasifree fermionic, in analogy with Gaussian linear optics. Gaussian states can be described purely in terms of the expectation value of quadratic observables, which are captured by a covariance matrix. Furthermore, some dissipative processes can be described within this powerful covariance matrix formalism (see e.g. [6–8]), and allow single fermions to hop between system and bath via $a_S^\dagger a_B$. Single fermion hopping violates conservation of fermion parity in the system, which is otherwise respected by unitary evolution. It is a toxic process that can cause errors without creating excitations, circumventing arguments that energy penalties suppress thermal processes

to a rate $e^{-\Delta/T}$. In particular, Majorana modes in the Kitaev wire (see Fig. **??**) have been shown to decohere due to fermion hopping at rates independently of system size or the system gap [9, 10]. This article considers all Gaussian fermionic systems, not just the Kitaev wire, and how they decohere as a function of temperature. A single fermion appearing in the system will have a partner appear in the environment, and so perhaps there is hope that a gapped bath Hamiltonian will provide an energy penalty inhibiting these processes. However, this talks presents a very general, yet simple, argument that thermalisation and decoherence is independent of temperature, assuming only that the system-bath is governed by a Gaussian Hamiltonian. We extend this argument by providing a microscopic derivation of a master equation in the weak coupling regime, and again observe temperature independent decoherence.

Coupling to a thermal bath leads to thermalisation and decoherence of stored quantum information. For a system of Gaussian fermions, the fermionic analog of linear or Gaussian optics, these dynamics can be elegantly and efficiently described by evolution of the system's covariance matrix. Taking both system and bath to be Gaussian fermionic, we observe that thermalization and decoherence occurs at a rate that is independent of the bath temperature. Furthermore, we also consider a weak coupling regime where the dynamics are Markovian. We present a microscopic derivation of Markovian master equations entirely in the language of covariance matrices, where temperature independence remains manifest. This is radically different from behaviour seen in other scenarios, such as when fermions interact with a bosonic bath. Our analysis applies to many Majorana fermion systems that have been heralded as very robust, topologically protected, qubits. In these systems, it has been claimed that thermal decoherence can be exponentially suppressed by reducing temperature, but we find Gaussian decoherence cannot be cooled away.

References

1. Nayak et al., *Reviews of Modern Physics* **80**, 1083 (2008)
2. Campbell et al., *Quant. Info. Comm.* **14**, 0981 (2014)
3. Bravyi, *Phys. Rev. A.* **73**, 042313 (2006)
4. Bravyi, *Phys. Rev. A.* **73**, 042313 (2006)
5. Kitaev, *Physics-Uspekhi.* **44**, 131 (2001)
6. Bravyi, *Quant. Inf. and Comp.* **3**, 216 (2005)
7. Prosen, *New Journal of Physics* **10**, 043026 (2008)
8. Eisert and Prosen, preprint arXiv:1012.5013 (2010)
9. Budich et al. *Phys. Rev. B* **85**, 121405 (2012)
10. Mazza et al. *Phys. Rev. B* **88**, 205142 (2013)

A quantum algorithm for computing the unit group of an arbitrary degree number field

Sean Hallgren

Pennsylvania State University

Abstract. Computing the group of units in a field of algebraic numbers is one of the central tasks of computational algebraic number theory. It is believed to be hard classically, which is of interest for cryptography. In the quantum setting, efficient algorithms were previously known for fields of constant degree. We give a quantum algorithm that is polynomial in the degree of the field and the logarithm of its discriminant. This is achieved by combining three new results. The first is a classical algorithm for computing a basis for certain ideal lattices with doubly exponentially large generators. The second shows that a Gaussian weighted superposition of lattice points, with an appropriate encoding, can be used to provide a unique representation of a real-valued lattice. The third is an extension of the hidden subgroup problem to continuous groups and a quantum algorithm for solving the HSP over $\mathbb{R}^n$.
Joint work with Kirsten Eisentraeger, Alexei Kitaev, and Fang Song.

Oracles with Costs

Shelby Kimmel[1,2], Cedric Yen-Yu Lin[2], and Han-Hsuan Lin[2]

[1] Joint Center for Quantum Information and Computer Science, University of Maryland

[2] Center for Theoretical Physics, Massachusetts Institute of Technology

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

A universal adiabatic quantum query algorithm

Mathieu Brandeho and Jérémie Roland

Université libre de Bruxelles, Quantum Information and Communication
1050 Brussels, Belgium

Abstract. In the quantum query complexity, the so-called quantum adversary bound introduced by Ambainis and later improved by Høyer *et al* [1, 6], is know to characterize the quantum query complexity for bounded error. While this result has been proved in the standard discrete-time model of quantum computation, it also holds for continuous-time (or Hamiltonian-based) quantum computation, due to a known equivalence between these two query complexity models [4].
In our work, we revisit this result by providing a direct proof in the continuous-time model. One originality of our proof is that it draws new connections between the adversary bound, a modern technique of theoretical computer science, and early theorems of quantum mechanics. Indeed, the proof of the lower bound is based on Ehrenfest's theorem [5], while the upper bound relies on the adiabatic theorem [3], as it goes by constructing a universal adiabatic quantum query algorithm.
Another originality, for the first time in the context of quantum adiabatic computation, the soundness of the algorithm relies on a version of the adiabatic theorem that does not require a spectral gap [2].

References

1. Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.
2. Joseph E. Avron and Alexander Elgart. Adiabatic Theorem without a Gap Condition. *Communications in Mathematical Physics*, 203(2):445–463, June 1999.
3. M. Born and V. Fock. Beweis des adiabatensatzes. *Zeitschrift fr Physik*, 51(3-4):165–180, 1928.
4. Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando D. Somma, and David Yonge-Mallo. Efficient discrete-time simulations of continuous-time quantum query algorithms. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 409–416. ACM, 2009.
5. P. Ehrenfest. Bemerkung über die angenäherte Gültigkeit der klassischen Mechanik innerhalb der Quantenmechanik. *Zeitschrift fur Physik*, 45:455–457, 1927.
6. Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 526–535. ACM, 2007.

On the Robustness of Bucket Brigade Quantum RAM

Srinivasan Arunachalam[1,2], Vlad Gheorghiu[2,3], Tomas Jochym-O'Connor[2,4], Michele Mosca[2,3,5,6], and Priyaa Varshinee Srinivasan[7,8]

[1] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
[2] Institute for Quantum Computing, University of Waterloo, Waterloo, Canada
[3] Department of Combinatorics & Optimization, University of Waterloo, Waterloo, Canada
[4] Department of Physics & Astronomy, University of Waterloo, Waterloo, Canada
[5] Perimeter Institute for Theoretical Physics, Waterloo, Canada
[6] Canadian Institute for Advanced Research, Toronto, Canada
[7] David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada
[8] Institute for Quantum Science and Technology, University of Calgary, Calgary, Canada

Abstract

We study the robustness of the bucket brigade quantum random access memory model introduced by Giovannetti, Lloyd, and Maccone [Phys. Rev. Lett. **100**, 160501 (2008)]. Due to a result of Regev and Schiff [ICALP '08 pp. 773, arXiv:1202.1027 [quant-ph]], we show that for a class of error models the error rate per gate in the bucket brigade quantum memory has to be of order $o(2^{-n/2})$ (where $N = 2^n$ is the size of the memory) whenever the memory is used as an oracle for the quantum searching problem. We conjecture that this is the case for any realistic error model that will be encountered in practice, and that for algorithms with super-polynomially many oracle queries the error rate must be super-polynomially small, which further motivates the need for quantum error correction. We introduce a circuit model for the quantum bucket brigade architecture and argue that quantum error correction for the circuit causes the quantum bucket brigade architecture to lose its primary advantage of a small number of "active" gates, since all components have to be actively error corrected. An interesting open question is the existence of a realistic architecture-specific error correction technique that could recover the polynomial number of physical gate activations of the routing scheme while still guaranteeing fault-tolerance.

New constructions for Quantum Money

Marios Georgiou[1] and Iordanis Kerenidis[2]

[1] CAISS-CCNY-The City University of New York
[2] CNRS-LIAFA-University Paris 7 Diderot

Abstract. We propose an information theoretically secure secret-key quantum money scheme in which the verification of a coin is classical and consists of only one round; namely, a classical query from the user to the bank and an accept/reject answer from the bank to the user. A coin can be verified polynomially (on the number of its qubits) many times before it expires. Our scheme is an improvement on Gavinsky's scheme [2], where three rounds of interaction are needed and is based on the notion of quantum retrieval games.
Moreover, we propose a publicly verifiable quantum money scheme which is computationally secure in the random oracle model, given one-time memories. This construction is derived naturally from our secret-key scheme using the fact that one-time memories are a special case of quantum retrieval games.

1 Quantum Money Definition

A quantum money scheme consists of an algorithm that is used by the bank in order to create valid coins, and a verification protocol that is run between a holder of a coin and the bank in order to verify the validity of the coin. The correctness of the scheme requires that valid coins are always accepted. The security requirement states that it is impossible for an algorithm to create more coins than what it had in the beginning. In a publicly verifiable (public-key) quantum money scheme, the verification of the coin can be done locally without interacting with the bank.

2 One-out-of-two Quantum Retrieval Games

A one-out-of-two quantum retrieval game (QRG) consists of a quantum state ρ that encodes a classical secret s and two challenges C_a, C_b. The correctness of the game requires that given ρ we can answer any of the two challenges for this s. The security requires that given ρ we cannot answer both challenges with non-negligible probability. Gavinsky has shown that the Hidden Matching [3] is such a QRG.

3 From QRGs to secret-key Quantum Money

In our scheme, a coin consists of n random QRG states. The verification protocol (a) picks at random some of them and (b) picks a random challenge for each of the picked ones. By the correctness of the QRG we can retrieve an answer for each of the challenges. These answers are sent to the bank. The bank compares the answers it receives with it's secret and accepts if all answers are correct. To prove security we argue as follows. If an algorithm $\mathcal{F}$ can create more valid coins than its input coins, then we can create another algorithm $\mathcal{A}$ that simulates $\mathcal{F}$ and, in the end, extracts answers for both challenges of a QRG. Since this is impossible, such an algorithm $\mathcal{F}$ cannot exist.

4 QRGs vs One-time Memories

It can be shown that QRGs whose challenges have only one valid answer are equivalent to one-time memories (OTM) [4]. OTMs are impossible in the plain quantum model (even with computational assumptions), however they are possible in the isolated qubits model [1]. Using OTMs instead of regular QRGs, we can create publicly verifiable quantum money in the random oracle model.

5 Publicly verifiable Quantum Money

The construction is a simple modification of the secret-key scheme. First, we replace the QRGs with OTMs. Then, we get rid of the interaction by giving the hash value of the OTM secrets as part the coin. In the random oracle model, we are guaranteed that this reveals no information about the secrets. Moreover, correctness can still be achieved by first applying the hash function to the answer we retrieve, and then comparing to the value given.

References

1. Broadbent, Anne, Gus Gutoski, and Douglas Stebila. "Quantum one-time programs." *Advances in CryptologyCRYPTO 2013* (2013): 344-360.
2. Gavinsky, Dmitry. "Quantum money with classical verification." *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on.* IEEE, 2012.
3. Gavinsky, Dmitry, et al. "Exponential separations for one-way quantum communication complexity, with applications to cryptography." Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. ACM, 2007.
4. Goldwasser, Shafi, Yael Tauman Kalai, and Guy N. Rothblum. "One-time programs." *Advances in Cryptology-CRYPTO 2008* (2008): 39-56.

Making Existentially Unforgeable Signatures Strongly Unforgeable in the Quantum Random-Oracle Model (Extended Abstract)

Edward Eaton[1] and Fang Song[1,2]

[1] Department of Combinatorics & Optimization, University of Waterloo
[2] Institute for Quantum Computing, University of Waterloo

Abstract. Strongly unforgeable signature schemes provide a more stringent security guarantee than the standard existential unforgeability. It requires that not only forging a signature on a new message is hard, it is infeasible as well to produce a new signature on a message for which the adversary has seen valid signatures before. Strongly unforgeable signatures are useful both in practice and as a building block in many cryptographic constructions.
This work investigates a generic transformation that compiles any existentially unforgeable scheme into a strongly unforgeable one, which was proposed by Teranishi et al. [4] and was proven in the classical random-oracle model. Our main contribution is showing that the transformation also works against *quantum* adversaries in the *quantum* random-oracle model. We develop proof techniques such as adaptively programming a quantum random-oracle in a new setting, which may be of independent interest. Applying the transformation to an existential-unforgeable scheme due to Cash et al. [2], which can be shown to be quantum-safe assuming certain lattice problems are hard for quantum computers, we get an efficient quantum-safe strongly unforgeable signature scheme in the quantum random-oracle model.

This work studies a generic transformation from existentially unforgeable signature schemes to strongly unforgeable ones, proposed by Teranishi et al. [4] (referred to as TOO hereafter), in the quantum setting. Among other existing transformations, TOO only needs a mild computational assumption and causes small overhead to the efficiency. Classically, TOO is proven in the random-oracle model (RO), where a hash function is treated as a truly random function and all users evaluate the hash function by querying the random function. The main difficulty towards making the TOO transformation go through in the quantum setting is that we need to consider the quantum random-oracle model (QRO) [1], where an quantum adversary can query the random-oracle in superposition. Unfortunately, many classical tricks in RO become difficult to apply

in QRO, if not entirely impossible. For starters, classically it is trivial to answer random-oracle queries on-the-fly by generating fresh random value for new queries while maintaining a table to keep consistency. It is not obvious how to handle quantum superposition queries in a similar way. Proof techniques in QRO have been developed in recent years [6,5], but many classical techniques are still missing their counterparts in QRO.

Our Contributions. We show that the TOO transformation still works against quantum adversaries in QRO under reasonable computational assumptions. The main technical tool we develop is adaptively programming a quantum random-oracle in a new setting, which we hope can lead to applications and extensions elsewhere. We then apply this technique to prove that the TOO transformation produces a quantum-safe strongly unforgeable signature scheme in QRO, assuming existence of a chameleon hash function and an existentially unforgeable signature scheme that are both quantum-safe. Finally we demonstrate that these building blocks can be instantiated based on lattice problems. Specifically, using tools from [3], we have verified that the bonsai-tree signature scheme and the chameleon hash function in [2] are both quantum-safe, assuming some lattice problem is quantum-safe[3].

Acknowledgements. The authors are grateful to Andrew Childs for helpful discussions. EE was supported by NSERC on an undergraduate research award at the Institute for Quantum Computing, University of Waterloo. FS acknowledges support from NSERC, CryptoWorks21, ORF and US ARO.

References

1. Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology–ASIACRYPT 2011*, pages 41–69. Springer, 2011.
2. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of cryptology*, 25(4):601–639, 2012.
3. Fang Song. A note on quantum security for post-quantum cryptography. In *Post-Quantum Cryptography*, pages 246–265. Springer, 2014.
4. Isamu Teranishi, Takuro Oyama, and Wakaha Ogata. General conversion for obtaining strongly existentially unforgeable signatures. In *Progress in Cryptology-INDOCRYPT 2006*, pages 191–205. Springer, 2006.
5. Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014*, pages 1–18. Springer, 2014.
6. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Proceedings of CRYPTO 2012*, 2012.

[3] Actually, we are able to show a tighter security reduction so that the assumption on the lattice problem can be weakened a little.

A Quantum Key Distribution Protocol for qu*d*its with better noise resistance

Zoé AMBLARD and François ARNAULT

XLIM Laboratory, University of Limoges

Abstract. We describe a new protocol h*d*DEB which generalize our protocol h3DEB [1] in any dimension $d \geq 3$ and we study its security against cloning attacks. It uses an homogeneous Bell inequality called hCHSH-d which belongs to the family of Bell inequalities introduced in [2].The amount of violation achieved by hCHSH-d with specific entangled states being better than for the CGLMP inequality for qu*d*its, our protocol h*d*DEB allows more tolerance to noise than N-DEB while being secure against the family of cloning attacks described in [3].

The security of Quantum Key Distribution is based on violations of local realism. As larger violations lead to a better noise resistance, the study of Bell inequalities and the choice of adequate parameters are important to strengthen Quantum Key Distribution protocols.

The entanglement-based protocol N-DEB described by Durt, Cerf, Gisin and Żukowski in [3] uses pairs of entangled qu*d*its and performs checks of the CGLMP inequality for d-dimensional systems [4] in order to detect eavesdropping. When used with a maximally entangled state and four well-chosen bases [5], this protocol for qu*d*its reaches a better noise resistance than the Ekert91 protocol for pairs of entangled qubits.

Our work improves the N-DEB protocol by increasing the amount of Bell violation, hence allowing to reach a better noise resistance. This increased amount of violation is the consequence of replacing the CGLMP inequality used in N-DEB by an inequality called hCHSH-d which belongs to the homogeneous Bell inequalities. This family of Bell inequalities has been studied in [2] and shown to form a complete set of Bell inequalities.

The use of homogeneous Bell inequalities for two qu*d*its necessitates $2d$ unitary observables. Four of them correspond to measurements that can be obtained with devices called multiport beam splitters (or ditters) in dimension d [6]. The $2(d-2)$ additional ones are products of these four observables.

We generalize the mathematical description of product observables for $d = 3$ mentioned in [1] to any d and we show that a product observable can always be implemented by a slightly modified multiport beam splitter. Once we have made clear that our protocol is fully implementable in practice, we extend our protocol h3DEB to the protocol hdDEB by replacing the inequality used in the N-DEB protocol with an homogeneous Bell inequality. This modification allow us to obtain a better amount of violation than N-DEB and reach a better noise resistance.

We also study how the addition of product measurements can impact the security of our protocol against a family of cloning attacks described in [3]. As these new measurements do not affect the form of the cloner required for this attack, we derive a security criterion for our protocol which takes the form of an upper bound over the value of the violation.

We finally provide for each $d = 3, 4, 5$ a set of parameters (basis, entangled state and homogeneous Bell inequality) which ameliorates the noise threshold of N-DEB while ensuring the security of our protocol against these cloning attacks.

d	3	4	5
N-DEB	1.436	1.448	1.455
hdDEB	1.505	1.546	1.574

Table 1. Violations obtained with N-DEB and hdDEB for $d = 3, 4, 5$

References

1. F. Arnault and Z. Amblard. A qutrit Quantum Key Distribution protocol with better noise resistance. arXiv:1404.4199 (2014).
2. F. Arnault. A complete set of multidimensional Bell inequalities. Journal of Physics A 45, 255304 (2012).
3. T. Durt, D. Kaszlikowski, J-L. Chen and L.C. Kwek. Security of Quantum Key Distribution with Entangled QuNits. Phys. Rev. A 69, 032313 (2004).
4. D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu. Bell Inequalities for Arbitrarily High-Dimensional Systems. Phys. Rev. Lett 88, 040404 (2002).
5. T. Durt, D. Kaszlikowski and M. Ẑukowski. Violations of local realism with quantum systems described by N-dimensional Hilbert spaces up to N=16. Physical Review A 64, 024101 (2001).
6. M. Ẑukowski, A. Zeilinger and M.A. Horne. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. Physical Review A 55, 2564 (1997).

Quantum control based on SU(2) decomposition of n-partite two level quantum systems

Francisco Delgado[1,2]

[1] Escuela de Ingeniera y Ciencias, Tecnológico de Monterrey
[2] Departamento de Física y Matemáticas, Tecnológico de Monterrey, Campus Estado de México. Atizapán, Estado de México, México

Abstract. This work presents, for a general n-partite two level spin system in $SU(n)$, a decomposition procedure in 2^{n-1} $SU(2)$ subsystems to establish selective control operations on a selected basis as grammar, letting manage quantum complexity of multipartite systems. Alternating the direction of local interactions, it states a universal exchange semantics on the entangled Bell gems basis.

1 Introduction

For spin systems, $SU(2)$ single system has exact and optimal control solutions in terms of energy or time [1, 2]. Recently research for anysotropic Ising model for bipartite systems in $SU(4)$ [3] has shown this model lets a $U(1)\times SU(2)^2$ block decomposition when it is written in a non-local basis, so $\mathcal{H}^2$ becomes a direct sum of two subspaces, each one generated by a pair of Bell states, while U becomes in the semi-direct product $U(1)\times SU(2)^2$. Control can then be reduced to two $SU(2)$ control problems in each sector and exact solutions can be found [4]. Controlled sectors can be selected by the direction of external driven interactions setting transformations between Bell states on demand. The brief aims of this work is to show a generalization of last procedure on general n-partite two level systems, reducing them to 2^{n-1} selective transformations on pairs of quantum states, and then show how a natural basis for this reduction procedure for an even number of parts, $n = 2d$, is the Bell gems basis.

2 Brief development

Problem stated here is established for a general Hamiltonian for n coupled two level systems on $U(2^n)$ conforming a closed system:

$$\tilde{H} = \sum_{\{i_k\}} h_{\{i_k\}} \bigotimes_{k=1}^{n} \sigma_{i_k} \tag{1}$$

where $\{i_k\} = \{i_1, i_2, ..., i_n\}$, $i_k = 0, 1, 2, 3$ and $h_{\{i_k\}}$, a set of time dependent real functions in general. Additionally, $k = 1, 2, ..., n$ and σ_i for $i = 0, 1, 2, 3$ are respectively the unitary matrix and traditional Pauli matrices expressed for the computational basis $|0\rangle, |1\rangle \in \mathcal{H}^2$ of each part.

If $\{E_j \ | j = 1, ..., 2^n\}$ are their eigenvalues and $\{|b_j\rangle \in \mathcal{H}^{2^n} | j = 1, ..., 2^n\}$ their eigenvectors, then by considering a set of 2^n orthogonal states: $\{|\alpha_i\rangle\}$ and 2^{n-1} pairs $\{j(i), k(i)\}, i = 1, 2, ..., 2^{n-1}$ with $k(i) = j(i) + 1$ (note that energies E_j are not necessarily ordered) fulfilling:

$$\left|\alpha_{j(i)}\right\rangle = A_i^* \left|b_{2i-1}\right\rangle - B_i \left|b_{2i}\right\rangle, \left|\alpha_{k(i)}\right\rangle = B_i^* \left|b_{2i-1}\right\rangle + A_i \left|b_{2i}\right\rangle \tag{2}$$

with: $|A_i|^2 + |B_i|^2 = 1$. It is possible reduce H to the block form:

$$H = \left(\begin{array}{c|c|c|c} \mathbf{S_{H}}_1 & \mathbf{0} & ... & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{S_{H}}_2 & ... & \mathbf{0} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & ... & \mathbf{S_{H}}_{2^{n-1}} \end{array}\right) \tag{3}$$

with $\mathbf{0}$, the 2×2 zero matrix. With $\mathbf{S_{H}}_i = a_i \mathbf{I_i} + \mathbf{b_i X_i} + \mathbf{c_i Y_i} + \mathbf{d_i Z_i} \in \mathbf{SU(2)}$. Because this structure is preserved under matrix products, then it is inherited by the evolution matrix U. This decomposition establishes exact control when blocks are reduced to diagonal forms $\mathbf{I_i}, \mathbf{Z_i}$(quasi-Evolution Loops) or to anti-diagonal forms $\mathbf{X_i}, \mathbf{Y_i}$ (Exchange Operations) [4] in terms of well known control schemes in $SU(2)$. Additionally, this work shows that Bell gems basis [5, 6] is, under certain restrictions, the general basis $\{|\alpha_i\rangle\}$ to state this decomposition:

$$\left|\Psi_{\mathcal{I}_4^d}\right\rangle = \frac{1}{\sqrt{2^d}} \sum_{\{\epsilon_j\},\{\delta_k\}} (\tilde{\sigma}_{i_1} \otimes ... \otimes \tilde{\sigma}_{i_d})_{\epsilon_1 ... \epsilon_d, \delta_1 ... \delta_d} \left|\epsilon_1 ... \epsilon_d\right\rangle \otimes \left|\delta_1 ... \delta_d\right\rangle \tag{4}$$

References

1. D'Alessandro and Dahleh, M., IEEE Transactions on Automatic Control **46** (6) 866 (2001).
2. Boscain, U. and Mason, P., J. Math. Phys. **47**, 062101 (2006).
3. F. Delgado, *Algebraic and group structure for bipartite three dimensional anisotropic Ising model on a non-local basis.* arXiv:1410.5148 [quant-ph]
4. F. Delgado, *Generation of non-local evolution loops and exchange operations for quantum control in three dimensional anisotropic Ising model.* arXiv:1410.5515 [quant-ph]
5. Jaeger, G. Physics Letters A **329** (6), 425-429 (2004).
6. Sych, D. and Leuchs, G. New Journal of Physics **11**, 013006 (2009).

Area laws and efficient descriptions of quantum many-body states

Yimin Ge[1] and Jens Eisert[2]

[1] Max-Planck-Institut für Quantenoptik
D-85748 Garching, Germany
[2] Dahlem Center for Complex Quantum Systems
Freie Universität Berlin
D-14195 Berlin, Germany

It is commonly believed that area laws for entanglement entropies imply that a quantum many-body state can be faithfully represented by efficient tensor network states – a conjecture frequently stated in the context of numerical simulations and analytical considerations. We show that this is in general not the case, except in one dimension. We prove that the set of quantum many-body states that satisfy an area law for all Renyi entropies contains a subspace of exponential dimension. Establishing a novel link between quantum many-body theory and the theory of communication complexity, we then show that there are states satisfying area laws for all Renyi entropies but cannot be approximated by states with a classical description of small Kolmogorov complexity, including polynomial projected entangled pair states (PEPS) or states of multi-scale entanglement renormalisation (MERA). Not even a quantum computer with post-selection can efficiently prepare all quantum states fulfilling an area law, and we show that not all area law states can be eigenstates of local Hamiltonians. We also prove translationally invariant and isotropic instances of these results, and show a variation with decaying correlations using quantum error-correcting codes.

Efficient Implementation of Quantum Walk Based Search Algorithms

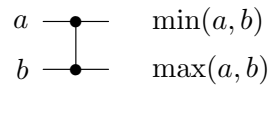
András Gilyén[1,2,3]

[1] Department of Quantum Optics and Quantum Information, SZFI, WIGNER RCP, Budapest
[2] Institute of Physics, Budapest University of Technology and Economics, Budapest
[3] Institute of Mathematics, Eötvös Loránd University, Budapest

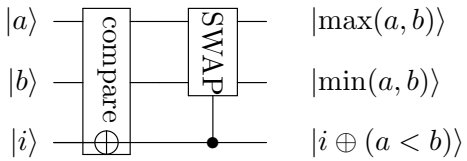
Abstract. This work investigates how to implement quantum walk based search algorithms which fit in the general framework introduced by Mario Szegedy[Sz]. Various techniques and subroutines are introduced to implement the necessary unitary operations used to construct the walk algorithm. The techniques include the usage of reversible sorting networks and a sort of "quantum derandomisation method" for generating coherent states corresponding to a sophisticated probability distribution. As a demonstration we show that using these new techniques one gets a faster, parallel implementation of Andris Ambainis's [Amb] optimal quantum query algorithm for the element distinctness problem.

1 Reversible Sorting Network

A quite versatile subroutine is the usage of reversible sorting networks. A reversible or quantum sorting network is basically a sorting network where an additional flag (qu)bit is flipped whenever a comparator swaps its two arguments. To construct a reversible sorting network one can take a classical sorting network and replace all the comparators with their reversible/quantum version as depicted below.



Classical comparator



To demonstrate the power of this tool we mention that using a reversible sorting network it is straightforward to implement a quantum RAM [GLM] gate efficiently.

2 Implementation of the Element Distinctness Algorithm

The element distinctness problem is the following: Given a unitary operator U_f corresponding to the unknown function $f : \{1, \ldots, N = 2^n\} \to \{1, \ldots, M = 2^m\}$ find out whether there is a pair $i \neq j$ such that $f(i) = f(j)$. Ambainis's [Amb] optimal query algorithm can solve the problem using $N^{2/3}$ queries to U_f with high probability utilising a quantum walk on the Johnson Graph.

To implement the element distinctness algorithm it is sufficient to implement three unitary operations corresponding to some sort of walk steps on the Johnson Graph as described by Szegedy [Sz] and Magniez et al. [MNRS].

2.1 Op.1: Generation of the initial probability distribution

The first step is the preparation of a pure state corresponding to a uniform probability distribution over all the nodes of the Johnson Graph i.e. over all the size $N^{2/3}$ subsets of $\{1,\ldots,N\}$. One also needs a proper data structure to be able to represent all the $\binom{N}{N^{2/3}}$ subsets in a way they can accessed easily by the following two operators.

We store the numbers $k_i, i \in \{1,\ldots,N^{2/3}\}$ of a subset in increasing order $(i<j \Rightarrow k_i<k_j)$ in a qubit array $\bigotimes_{i=1}^{N^{2/3}} |k_i\rangle$. The preparation of a state describing this structure is nontrivial. We use a classical randomised algorithm which requires a few times more coin tosses than $\log\binom{N}{N^{2/3}}$, and partially transform this random series to the desired data structure. (We prepare the coin toss states by the usage of many parallel Hadamard gates.) The main trick is that we arrange the rest of the qubits in such a way that whole state gets very close to a product state, so we can forget the rest: (we call this trick "quantum derandomisation")
$|\text{uniform distribution over } \binom{N}{N^{2/3}}\rangle\,|\text{unused qubits}\rangle$

As a final step we query U_f to achieve a new data array $|S\rangle = \bigotimes_{i=1}^{N^{2/3}} |k_i, f(k_i)\rangle$.

2.2 Op.2: Check whether there are two non-distinct elements in a subset

This operation is straightforward using a reversible sorting network. Suppose we have a set of numbers $k_i, i \in \{1,\ldots,N^{2/3}\}$ together with the function values $f(k_i)$. Then we simply sort our data array $|S\rangle = \bigotimes_{i=1}^{N^{2/3}} |k_i, f(k_i)\rangle$ consisting the subset of numbers and the corresponding function values according to the function values. After sorting it is enough to check whether there are any neighbors having the same f value.

2.3 Op.3: Update/Step to neighbor nodes

This operation performs a "diffusive" step to all neighbor nodes in the Johnson Graph representing subsets which differ in exactly one number. I.e. it does the following action: $|S\rangle\,|0\rangle \to \frac{\sum_{S \triangle S_j=2} |S\rangle|S_j\rangle}{N^{2/3}(N-N^{2/3})}$. This operation can be implemented using ideas similar to the above two operations.

3 Conclusion

Careful analysis [MSc] shows that the above described steps can be well parallelised and thus we obtain an overall circuit depth of $\mathcal{O}(\log(N)\log\log(N))$ for one step operator of the Element Distinctness Algorithm. In contrast Ambainis's original an more involved implementation [Amb] could resolve one step with circuit depth $\mathcal{O}(\log^4(N))$.

Also the developed techniques may be useful for other quantum algorithmic tasks.

References

Amb. A. Ambainis: Quantum walk algorithm for element distinctness, Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, pages 22-31 (2004)

GLM. V. Giovannetti, S. Lloyd, L. Maccone: Quantum random access memory, Phys. Rev. Lett. 100, 160501 (2008)

MNRS. F. Magniez, A. Nayak, J. Roland, M. Sántha: Search via quantum walk, Proc. 39th STOC, ACM Press 575-584 (2007)

Sz. M. Szegedy: Quantum Speed-Up of Markov Chain Based Algorithms, Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, pages 32-41 (2004)

MSc. A. Gilyén: Quantum walk based search methods and algorithmic applications, MSc Thesis, Eötvös Loránd University, Budapest (2014)

Dealing with loss in a linear optical quantum computer

Mercedes Gimeno-Segovia[1], Pete Shadbolt[1], Dan Browne[2], and Terry Rudolph[1]

[1] Department of Physics, Imperial College London, London SW7 2AZ, United Kingdom
[2] Department of Physics and Astronomy, University College London, London WC1E 6BT, United Kingdom

Abstract

Single photons, manipulated using integrated linear optics, constitute a promising platform for universal quantum computation. A series of increasingly efficient proposals have shown linear-optical quantum computing to be formally scalable. However, existing schemes typically require extensive adaptive switching, which is experimentally challenging and noisy, thousands of photon sources per renormalized qubit, and/or large quantum memories for repeat-until-success strategies. Our work overcomes all these problems. We present a scheme to construct a cluster state universal for quantum computation, which uses no adaptive switching, no large memories, and which is at least an order of magnitude more resource-efficient than previous passive schemes. Unlike previous proposals, it is constructed entirely from loss-detecting gates and offers a robustness to photon loss. Even without the use of an active loss-tolerant encoding, our scheme naturally tolerates a total loss rate $\sim 1.6\%$ in the photons detected in the gates. This scheme uses only 3-GHZ states as a resource, together with a passive linear-optical network. We fully describe and model the iterative process of cluster generation, including photon loss and gate failure. We also demonstrate how error correcting codes can be embedded in this architecture to achieve the fidelities necessary for fault tolerant quantum computation. This demonstrates that building a linear optical quantum computer need be less challenging than previously thought.

A linear condition for a wide range of exact quantum algorithms*

S. A. Grillo and F. L. Marquezino

Federal University of Rio de Janeiro, Brazil
{sgrillo,franklin}@cos.ufrj.br

Abstract. In this work, we present a system of linear equations which solution guarantees the existence of an exact quantum algorithm for a given function and fixed number of steps. This result is obtained using a novel parametrization of the quantum query model.

The construction of quantum algorithms that outperform their classical counterparts is a challenging problem in quantum computing. In particular, the toolbox for designing exact quantum algorithms is still limited [1–3]. Thus, a possible strategy is to reformulate the Quantum Query Model (QQM) in order to have better insights.

We prove that any algorithm in the QQM is equivalent to a set of vectors that satisfy a set of properties, which we call *block set properties*, and we call *block set* any set of vectors satisfying such properties. For each QQM algorithm there is a block set algorithm and vice versa. Finally, we define the output of a block set in such way that its Gram matrix of final states is the same of its corresponding QQM algorithm. Thus, our formulation is another parametrization for QQM algorithms before the measurement step. Each pair of elements in the block set determines a matrix, the sum of all those matrices is the Gram matrix of output states. If we consider a block set whose elements are pairwise orthogonal, we obtain our linear conditions. We introduce some notation first.

Let $S_x := \{i : x_i = 1\}$, where x_i is the i-th bit in x. The Dirac measure, denoted as $\delta_z(A)$, equals 1 if $z \in A$ and 0 otherwise. There are:

$$P_k = \left\{(x,y) : (-1)^{\sum_{i=0}^{t} \delta_{k_i}(S_x)} = 1 \text{ and } (-1)^{\sum_{i=0}^{t} \delta_{k_i}(S_y)} = 1\right\}, \quad (1)$$

$$Q_k = \left\{(x,y) : (-1)^{\sum_{i=0}^{t} \delta_{k_i}(S_x)} = -1 \text{ and } (-1)^{\sum_{i=0}^{t} \delta_{k_i}(S_y)} = -1\right\}, \quad (2)$$

for $k, h \in \mathbb{Z}_{n+1}^{t+1}$. Now we may define the square matrices $\bar{P}_{k,h}$ and $\bar{Q}_{k,h}$, with row x and column y being indexed by elements of $\{0,1\}^n$ and with

* The authors acknowledge financial support from CNPq and CAPES.

entries taking values in $\{0,1\}$, as follows: $\bar{P}_{k,h}[x,y]=1$ iff $(x,y)\in P_k\cap P_h$ and, similarly, $\bar{Q}_{k,h}[x,y]=1$ iff $(x,y)\in Q_k\cap Q_h$.

Finally, let $X,Y\subset\{0,1\}^n$ be two disjoint sets, and let $(x,y)\in X\times Y$. We define the system of equations $\widehat{E}\,(t,n,X,Y)$ with unknowns $\{w_{kk}\}$, to be:

$$\sum_{k\in\mathbb{Z}_{n+1}^{t+1}}\left(\bar{P}_{k,k}[x,y]+\bar{Q}_{k,k}[x,y]\right)\cdot w_{kk}=\frac{1}{2}, \tag{3}$$

$$\sum_{k\in\mathbb{Z}_{n+1}^{t+1}} w_{kk}=1. \tag{4}$$

Theorem 1. *Let $f:\{0,1\}^n\to\{0,1\}$ be a function where $(x\in X)\wedge(y\in Y)$ implies that $f(x)\neq f(y)$. If $\widehat{E}\,(t,n,X,Y)$ has solution over the non-negative real numbers, then there is a quantum query algorithm that calculates f exactly in $t+1$ queries.*

This result is different to tools as semi-definite programming [4], because it allows the analysis and design of quantum algorithms rather than black-box numerical solutions. Each Equation 3 represents an entry in the Gram matrix and we can state that each variable w_{kk} receives a weight that is summed in its corresponding region of the Gram Matrix. For example, if we analyse just the row 0^n, we can define

$$F=\left\{\bigoplus_i x_{j_i} : x_0=0, j\in J\subset\mathbb{Z}_{n+1}^{t+1}\right\}, \tag{5}$$

where $\oplus$ denotes binary sum. If we associate each formula to a weight $w_{jj}>0$, taking $w_{jj}=1/|J|$, we solve system $\widehat{E}\,(t,n,X,Y)$ for $X=\{0^n\}$ and a set Y, where $y\in Y$ if and only if y satisfies exactly $|J|/2$ formulas. This implies a family of exact quantum algorithms that recognizes a null vector from a wide range of possible patterns, using $t+1$ queries.

References

1. A. Ambainis (2013), *Superlinear advantage for exact quantum algorithms*, In Proc. of the 45th ACM STOC.
2. A. Ambainis, A. Iraids and J. Smotrovs (2013), *Exact quantum query complexity of EXACT and THRESHOLD*, arXiv:1302.1235.
3. A. Montanaro, R. Jozsa and G. Mitchison (2013), *On Exact Quantum Query Complexity*, Algorithmica.
4. H. Barnum, M. Saks and M. Szegedy (2003), *Quantum decision trees and semidefinite programming*, In Proc. of the 18th IEEE Conf. on Computational Complexity.

Bidirectional quantum controlled teleportation by using EPR states and entanglement swapping

Shima Hassanpour [1] and Monireh Houshmand [2]

[1]Corresponding author, Ms Student, Department of Electrical Engineering, Imam Reza International University, Iran
[2]Assistant Professor, Department of Electrical Engineering, Imam Reza International University, Iran
shimahassanpour@yahoo.com, m_houshmand61@yahoo.com

Abstract. In this paper, a novel protocol for bidirectional controlled quantum teleportation (BCQT) is proposed. Based on entanglement swapping of initiate Bell state, two users can teleport an unknown single-qubit state to each other under the permission of the supervisor. This proposed protocol would be utilized to a system in which a controller controls the communication in one direction only. Indeed, just one of the users needs the permission of the controller to reconstruct the unknown quantum state. In comparison to the existing BCQT protocols which their quantum channels are cluster and brown state, the proposed protocol is more practical within today's technology, since it merely uses Bell states as the quantum resource.

BACKGROUND

Quantum mechanics represents some special capabilities for the transmission of quantum information [1]. Based on the principles of quantum mechanics, there are many forms of quantum communication [2]. Quantum teleportation (QT) is a type of quantum communication that an unknown quantum state is teleported from one place to the other place via entanglement and with the help of classical information. Many quantum teleportation protocols have been proposed since Bennett et al., [3] first proposed a QT protocol in 1993.

Controlled quantum teleportation (CQT), first presented by Karlsson et al., [4] in 1998. Over the past few years, much attention has been considered on this interesting topic. Consequently, several CQT protocols by applying various types of entangled state have been introduced.

In 2013, Zha et al., [5] proposed the first Bidirectional controlled quantum teleportation (BCQT) by employing five-qubit entangled state. After that, based on different types of entangled states as a quantum channel, several BCQT protocols have been suggested. In all of these BCQT protocols, without the permission of Charlie as a controller the other two users cannot reconstruct an unknown quantum state.

Current results

In this protocol, Alice and Bob as a two legitimate users want to teleport a single qubit state to each other under the permission of the controller. In this scheme, just one of the users requires the controller's classical information to get the unknown quantum state. Suppose Alice and Bob have a single qubit state, which are described as Eq. (1).

$$|\emptyset\rangle_A = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad |\emptyset\rangle_B = \beta_0|0\rangle + \beta_1|1\rangle, \tag{1}$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and $|\beta_0|^2 + |\beta_1|^2 = 1$. This protocol consists of the following steps:

Step1. Assume that the quantum channel linking Alice, Bob and Charlie is composed of three EPR entangled state, which has the form of Eq. (2).

$$\begin{aligned}|\varphi\rangle_{a_1b_1c_1a_2c_2b_2} &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \tfrac{1}{2\sqrt{2}}|000000\rangle + |000011\rangle + |001100\rangle + |001111\rangle \\ &\quad + |110000\rangle + |110011\rangle + |111100\rangle + |111111\rangle)_{a_1b_1c_1a_2c_2b_2},\end{aligned} \tag{2}$$

where the qubits a_1a_2, b_1b_2, c_1c_2 belong to Alice, Bob and Charlie respectively. The state of the whole system can be expressed as Eq. (3).

$$|\Psi\rangle_{a_1b_1c_1a_2c_2b_2AB} = |G\rangle_{a_1b_1c_1a_2c_2b_2} \otimes |\emptyset\rangle_A \otimes |\emptyset\rangle_B. \tag{3}$$

Step2. In this step, Alice and Bob make a CNOT operation with qubits A and B as control qubits and qubits a_1 and b_2 as target respectively. The state will be the form of Eq. (4).

$$\begin{aligned}|\Psi'\rangle_{a_1b_1c_1a_2c_2b_2AB} = \tfrac{1}{2\sqrt{2}}[&(|000000\rangle + |000011\rangle + |001100\rangle + |001111\rangle \\ &+ |110000\rangle + |110011\rangle + |111100\rangle + |111111\rangle)_{a_1b_1c_1a_2c_2b_2})\ \alpha_0\beta_0|00\rangle_{AB} \\ &+ (|000001\rangle + |000010\rangle + |001101\rangle + |001110\rangle \\ &+ |110001\rangle + |110010\rangle + |111101\rangle + |111110\rangle)_{a_1b_1c_1a_2c_2b_2})\ \alpha_0\beta_1|01\rangle_{AB} \\ &+ (|100000\rangle + |100011\rangle + |101100\rangle + |101111\rangle\end{aligned}$$

$$+|010000\rangle + |010011\rangle + |011100\rangle + |011111\rangle)_{a_1b_1c_1a_2c_2b_2})\ \alpha_1\beta_0|10\rangle_{AB}$$
$$+(|100001\rangle + |100010\rangle + |101101\rangle + |101110\rangle$$
$$+|010001\rangle + |010010\rangle + |011101\rangle + |011110\rangle)_{a_1b_1c_1a_2c_2b_2})\ \alpha_1\beta_1|11\rangle_{AB}. \quad (4)$$

Step3. Alice and Bob perform a single qubit measurement in the Z-basis on qubits a_1 and b_2 and the X-basis measurement on qubits A and B respectively. The remaining particles may collapse into one of the 16 possible state with the same probability.

Step4. After Alice (Bob) tells the result to Bob (Alice) and Charlie, if Charlie wants to co-operate with the other two users, he applies Hadamard operation on his two qubits. As an example, if Alice's and Bob's measurement results in the first step is $|0\rangle_{a_1}|+\rangle_A$, and $|0\rangle_{b_2}|+\rangle_B$, the state of the remaining particles collapse into the state as Eq. (5) shows.

$$|\Omega\rangle_{b_1c_1a_2c_2} = \frac{1}{4\sqrt{2}}[\alpha_0\beta_0(|0000\rangle + |0001\rangle + |0100\rangle + |0101\rangle + |0010\rangle + |0011\rangle - |0110\rangle - |0111\rangle)_{b_1c_1a_2c_2}$$
$$+\alpha_0\beta_1(|0000\rangle - |0001\rangle + |0100\rangle - |0101\rangle + |0010\rangle - |0011\rangle - |0110\rangle + |0111\rangle)_{b_1c_1a_2c_2}$$
$$+\alpha_1\beta_0(|1000\rangle + |1001\rangle + |1100\rangle + |1101\rangle + |1010\rangle + |10111\rangle - |1110\rangle - |1111\rangle)_{b_1c_1a_2c_2}$$
$$+\alpha_1\beta_1(|1000\rangle - |1001\rangle + |1100\rangle - |1101\rangle + |1010\rangle - |1011\rangle - |1110\rangle + |1111\rangle)_{b_1c_1a_2c_2}]. \quad (5)$$

Then Charlie performs Bell measurement and announces his result to the users. The state is as follows:

$$|\Omega\rangle_{b_1c_1a_2c_2} = \frac{1}{4}[|\emptyset^+\rangle_{c_1c_2}(\alpha_0|0\rangle + \alpha_1|1\rangle)_{b_1}(\beta_0|0\rangle + \beta_1|1\rangle)_{a_2} + |\emptyset^-\rangle_{c_1c_2}(\alpha_0|0\rangle + \alpha_1|1\rangle)_{b_1}(\beta_0|1\rangle + \beta_1|0\rangle)_{a_2}$$
$$+|\Psi^+\rangle_{c_1c_2}(\alpha_0|0\rangle + \alpha_1|1\rangle)_{b_1}(\beta_0|0\rangle - \beta_1|1\rangle)_{a_2} + |\Psi^-\rangle_{c_1c_2}(\alpha_0|0\rangle + \alpha_1|1\rangle)_{b_1}(\beta_0|1\rangle - \beta_1|0\rangle)_{a_2}]. \quad (6)$$

Now, each legitimate user can reconstruct the unknown single-qubit state by applying suitable unitary operation as we can see in Table I.

TABLE I. RELATION BETWEEN THE MEASUREMENT RESULTS AND APPROPRIATE UNITARY OPERATION

Charlie's measurement result	$\|\emptyset^+\rangle$	$\|\emptyset^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
Bob's operation	I_{b_1}	$\sigma^{x}_{b_1}$	$\sigma^{z}_{b_1}$	$\sigma^{iy}_{b_1}$
Alice's operation	I_{a_2}	I_{a_2}	I_{a_2}	I_{a_2}

Unlike other schemes which their quantum channels are cluster and brown state, this scheme utilizes entanglement swapping technique [6] for sharing three-EPR pair. Therefore, the proposed protocol is experimentally more efficient compared with related works in two aspects. On the one hand, the quantum channel is easier to be prepared [7]; on the other hand, the entanglement must be held between two qubits, while preserving entanglement between more than two qubits is more complicated.

In Table II, T.D and O.D refer to types of Charlie's control which denote two and one-direction respectively. Also, B.M and S.P.M indicates the Bell and the single photon measurement respectively.

TABLE II. THE COMPARISON BETWEEN PROPOSED BCQT PROTOCOL WITH EXISTING ONES

Ref.	[20]	[21]	[22]	[23]	[24]	[25]	Proposed protocol
Type of channel	$Cluster_5$	$Cluster_6$	Six-qubit	$Brown_5$	Seven-qubit	Six-qubit	EPR_6
Type of control	T.D	T.D	T.D	T.D	T.D	T.D	O.D
Measurement method	S.P.M	S.P.M	B.M	B.M	B.M	B.M	B.M

References

1 M. A. Nielsen, I. L. Chuang, Cambridge University Press, Cambridge, 2002.

2 C. H. Bennett, G. Brassard, Proceedings of the International Conference on Computers, Systems and Signal Processing Bangalore press. (India), 1984, p. 175.

3 C. H. Bennet, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wooters, Phys. Rev. Lett, 70 (1993) 1895.

4 A. Karlsson, M. Bourennane, Phys. Rev. A, 58 (1998) 4394.

5 X. W. Zha, Z. C. Zou, J. X. Qi, H.Y. Song, Int J Theor Phys. 52 (2013) 1740.

6 S. Hassanpour, M. Houshmand, Quantum Inf. Process, DOI 10.1007/s11128-014-0866-z (2014).

7 M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.

Bounds on quantum non-locality via partial transposition

Karol Horodecki[1,2] and Gláucia Murta[2,3]

[1] Institute of Informatics, University of Gdańsk, Gdańsk, Poland
[2] National Quantum Information Centre in Gdańsk, Sopot, Poland
[3] Dep. de Física, Universidade Federal de Minas Gerais, Belo Horizonte, MG, Brazil

Abstract. We explore the link between two concepts: the level of violation of a Bell inequality by a quantum state and discrimination between two states by means of local operations and classical communication (LOCC). For any bipartite Bell inequality, we show that its value on a given quantum state cannot exceed the classical bound by more than the maximal quantum value shrunk by a factor related to distinguishability of this state from the separable set by means of restricted class of operations. The bounds are strong enough to limit the use of certain states containing private key in the device-independent scenario. We then consider the general scenarios where the parties are allowed to perform a local pre-processing of many copies of the state before the Bell test (asymptotic and hidden-non-locality scenarios). We define the rate of non-locality and, for PPT states, we bound this quantity by the relative entropy of entanglement of the partially transposed state.

Our first result is a bound on the maximal violation of a Bell inequality $\mathcal{S}$ by a single copy of a bipartite state ρ_{AB}, which we denote $Q_S(\rho_{AB})$. We show that it exceeds the classical value, $C(\mathcal{S})$, by the maximum quantum value $Q(\mathcal{S})$ for the inequality, shrunk by a factor related to distinguishability between the state and separable states (SEP) by means of a restricted class of operations. More precisely:

$$Q_{\mathcal{S}}(\rho_{AB}) \leq C(\mathcal{S}) + Q(\mathcal{S}) \times \inf_{\sigma \in SEP} ||\rho_{AB}^{\Gamma} - \sigma||. \tag{1}$$

Regarding the *asymptotic* and *hidden non-locality* scenarios, following [1] we base on the relative entropy to measure the non-locality of a box and we define the *rate of non-locality* for a bipartite state, $R(\rho_{AB})$, which takes into account all boxes one can obtain from many copies of the state ρ_{AB}, after processing it by LOCC. Also for the hidden non-locality scenario [2], in which the parties can perform a 'filtering' operation prior to the Bell test, we define a *rate of hidden non-locality*, $R_H(\rho_{AB})$, which takes into account the probability of success of the filter. Our main result consists

of upper-bounds on the non-locality of these scenarios via entanglement measures and partial transposition. For any bipartite PPT state ρ_{AB}:

$$\max\{R(\rho_{AB}), R_H(\rho_{AB})\} \leq \min\{E_r(\rho_{AB}), E_r(\rho_{AB}^{\Gamma})\}, \tag{2}$$

where E_r is the relative entropy of entanglement, $E_r \equiv \inf_{\sigma \in SEP} S(\rho||\sigma)$. To the best of our knowledge, this is the first quantitative approach for the asymptotic and hidden non-locality scenarios.

We apply the derived bounds to private [3, 4] and approximate private bits. For a certain private bit γ of dimension $4d^2$, we obtain that the violation of the CHSH inequality is bounded by: $Q_{CHSH}(\gamma) \leq 2 + \frac{\sqrt{2}+1}{2\sqrt{2}d}$. This shows that, in spite of the fact that all private states are distillable [5] and, more importantly, non-local [6], the non-locality gain can be severely limited for some of them.

We then consider a family of approximate private PPT states ρ_d, also of dimension $4d^2$ [7, 8], and obtain the bound: $Q_{\mathcal{S}}(\rho_d) \leq C(\mathcal{S}) + Q(\mathcal{S})\frac{1}{\sqrt{d}}$. Then, if the Bell inequality $\mathcal{S}$ has number of inputs or outputs growing significantly slower than $\sqrt{d}$, one can observe only negligible violation [9]. We also show that even with access to many copies of the initial state, the yield of non-locality for the states ρ_d is negligible. From the bound (2), due to asymptotic continuity of the relative entropy of entanglement, one obtains that, for states ρ_ϵ for which ρ_ϵ^{Γ} is ϵ-close to some separable state: $\max\{R(\rho_\epsilon), R_H(\rho_\epsilon)\} \leq 4\epsilon \log d + 2h(\epsilon)$, where $h(.)$ is the binary Shannon entropy. Therefore, for the family of states ρ_d, both R and R_H vanishes when dimension of the state increases. This is a striking result, as at the same time, the states ρ_d contain 1 bit of secure key (in limit of large d), and are shown to be useful for Quantum Key Distribution.

References

1. W. van Dam, R. Gill, and P. Grunwald, IEEE Trans. Inf. Theory **51**, 2812 (2005).
2. S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
3. K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
4. K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).
5. P. Horodecki and R. Augusiak, Phys. Rev. A **74**, 010302 (2006).
6. R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acin, Phys. Rev. Lett. **104**, 230401 (2010).
7. K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008b).
8. S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, Nature Comm. **6**, 6908 (2014).
9. M. Junge and C. Palazuelos, Comm. Math. Phys. **306**, 695 (2011).

Trotterization in universal quantum simulators under faulty control

George C. Knee and William J. Munro

NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan

Abstract. Universal quantum simulation may provide insights into those many-body systems that cannot be described classically, and that cannot be efficiently simulated with current technology. The Trotter formula, which decomposes a desired unitary time evolution of the simulator into a stroboscopic sequence of repeated elementary evolutions, is a key algorithmic component which makes quantum simulation of dynamics tractable. The Trotter number n sets the timescale on which a computer running this algorithm is switched from one elementary evolution to another. In the ideal case, the precision of the simulation can be arbitrarily controlled by increasing n. We study a more realistic scenario where each gate is applied imperfectly. The resultant tradeoff in errors leads to an ultimate limit on the precision of the simulation. We calculate the optimum Trotter number n^* that achieves this limit, which is the minimum statistical distance from the actual simulation to the ideal one.

1 Two kinds of error

Lloyd's algorithm [1] is a general but approximate way to simulate a local Hamiltonian $H = \sum_{j=1}^{k} H_j$. The true evolution is approximated through a truncation of the Trotter [2] formula:

$$U = \exp[iHt] = \left(\prod_{j=1}^{k} \exp[iH_j t/n] \right)^n + \dots \tag{1}$$

It is clear that for any finite value of n (the 'Trotter number'), the higher order terms in the above equation will be non-zero. Their neglect then necessarily leads to an discrepancy sometimes called the 'digital error'. In principle this can be reduced arbitrarily by increasing n. In a realistic quantum simulator, however, a second kind of error (introduced by faulty operations $\mathcal{E}$ concatenated $\circ$ with the target operations $\mathcal{V}$) competes with the first and the capacity to arbitrarily control the error disappears.

2 Results

To quantify the precision of a quantum simulator, we ignore the problems of state preparation and data extraction and concentrate on the fidelity of the dynamics itself. The quantum channel norm $||\cdot||_\diamond$ is the maximum quantum trace norm over all possible input states, and as such determines the probability of distinguishing the actual quantum channel

$$\mathcal{E}^{\text{faultyTrotter}}(\rho) = \bigcirc_{i=1}^{n} \bigcirc_{j=1}^{k} \mathcal{E}_{ij} \circ \mathcal{V}_j(\rho) \tag{2}$$

from the ideal one $\mathcal{U}$. For this problem we find

$$D := \left|\left|\mathcal{U} - \mathcal{E}^{\text{faultyTrotter}}\right|\right|_\diamond \leq \frac{\mathscr{C}}{n} + \mathscr{D}n. \tag{3}$$

As we show in [3], $\mathscr{C}$ is fixed by the pair $\{H, t\}$, while $\mathscr{D}$ depends on the gate noise. In the tradeoff between digital errors and gate errors, the optimum Trotter number is

$$n^* = \sqrt{\frac{\mathscr{C}}{\mathscr{D}}} \tag{4}$$

and this gives the lowest (best) channel distance

$$D(n^*) = 2\sqrt{\mathscr{C}\mathscr{D}}. \tag{5}$$

This square root dependence implies that reaching the sorts of precision we are accustomed to with modern classical computers (the current standard 'single precision' is about 10^{-7} [4]) will require a factor of at least 10^6 more Trotter steps and therefore a 10^{12} improvement in the error per Trotter step $\mathscr{D}$ over the current state of the art [5, 6]. This may be achieved in the future with the help of error correction [7].

References

1. S. Lloyd, Science **273**, 1073 (1996).
2. H. F. Trotter, Proc. Amer. Math. Soc. **10**, 545 (1959).
3. G. C. Knee and W. J. Munro, (2015), 1502.04536v1.
4. IEEE Std 754-2008 , 1 (2008).
5. Y. Salathé *et al.*, (2015), 1502.06778v1.
6. R. Barends *et al.*, (2015), 1501.07703v1.
7. R. Raussendorf, Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **370**, 4541 (2012).

Grover's search with faults on some marked elements

Dmitry Kravchenko, Nikolajs Nahimovs, Alexander Rivosh*

Faculty of Computing, University of Latvia

Abstract. Grovers algorithm is a quantum query algorithm solving the unstructured search problem of size N using $O(\sqrt{N})$ queries. It provides a significant speed-up over any classical algorithm [2].
The running time of the algorithm, however, is very sensitive to errors in queries. It is known that if query may fail (report all marked elements as unmarked) the algorithm needs $\Omega(N)$ queries to find a marked element [3]. [1] have proved the same result for the model where each marked element has its own probability to be reported as unmarked.
We study the behavior of Grovers algorithm in the model where the search space contains both faulty and non-faulty marked elements. We show that in this setting it is indeed possible to find one of non-faulty marked items in $O(\sqrt{N})$ queries.
We also analyze the limiting behavior of the algorithm for a large number of steps and show the existence and the structure of limiting state ρ_{lim}.

References

1. A.Ambainis, A.Backurs, N.Nahimovs, A.Rivosh. Grover's algorithm with errors. *Proceedings of MEMICS 2012*, LNCS 7721:180-189, 2013.
2. L. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th ACM STOC*, 212-219, 1996.
3. O. Regev, L. Schiff. Impossibility of a Quantum Speed-up with a Faulty Oracle *Proceedings of ICALP'2008*, LNCS 5125:773-781, 2008.

* This research was supported by EU FP7 projects QALGO (Dmitry Kravchenko, Nikolajs Nahimovs) and MQC (Alexander Rivosh).

A Generalized Quantum Inspired Evolutionary Algorithm for Signature-based Intrusion Detection Systems

Monisha Loganathan

No Institute Given

EPR Steering and Quantum Steering Ellipsoids in non-Markovian Spin Chains

Ruari McCloskey[1], Tony J. G. Apollaro[1,2], Salvatore Lorenzo[2], and Mauro Paternostro[1]

[1] Centre for Theoretical Atomic, Molecular, and Optical Physics, School of Mathematics and Physics, Queen's University Belfast,BT7,1NN, United Kingdom

[2] Dipartimento di Fisica e Chimica, Università degli Studi di Palermo, Via Archirafi 36, I-90123 Palermo, Italy

Abstract. In this work we examine for the first time the dynamical evolution of the Quantum Steering Ellipsoid and a genuine measure of Einstein-Podolski-Rosen steering in a non-Markovian environment. Alongside some entanglement and non-Markovianity measures we investigate how the volume of the Quantum Steering Ellipsoid changes dynamically, and how it compares to other measures of non-local correlations.

1 Introduction

Recently, a lot of work has been done on Quantum Steering Ellipsoids (QSEs) [1,**?**]. These QSEs are a useful way of visualising two-qubit systems (ρ_{AB}) which are correlated as in Fig.1. This method for depicting two qubits has a real emphasis on the idea of correlations really being seen through measurement. The surface of the QSE is obtained by making projective measurements on one qubit, and using the results of the measurement to examine correlations with the other qubit. Using this interpretation, it is obvious to use the volume of the QSE as a measure of non-local information, indeed, bounds on the size of the QSE have already been formulated for separable states [1]. Our treatment largely focusses on the volume of the QSE and its dynamical evolution alongside the concurrence to see the similarities and differences between the two measures of correlations. We also present some results generally on the volume of the QSEs, looking at a distribution of random two-qubit input states and seeing how it varies with the Linear Entropy, $(1 - \mathrm{Tr}\left[\rho_{AB}^2\right])$.

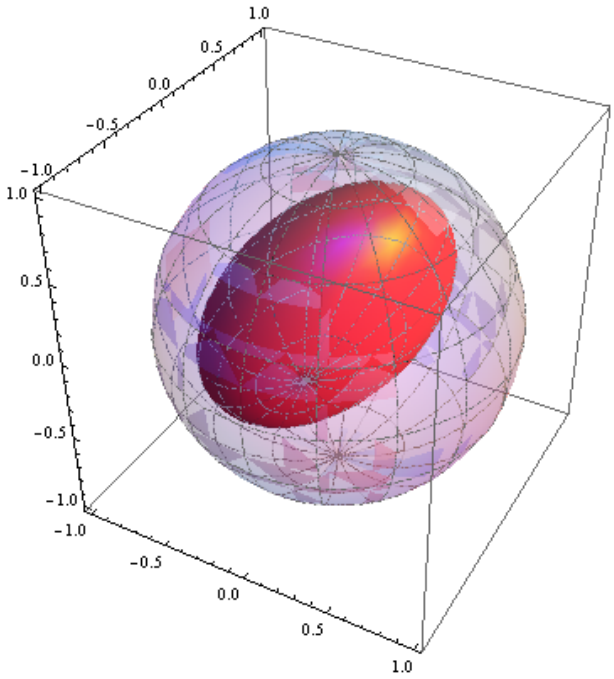


Fig. 1. The Quantum Steering Ellipsoid, a possible representation of an entangled 2-qubit state. The center of the QSE is the block vector of the reduced state of Bob's qubit. Alice can "steer" Bob's state to anywhere inside the QSE (the surface being obtained with projective measurements, and the inside with POVMs). (Animated Online)

2 Non-Markovian Spin Chains

In this work we do the first examination of the QSEs which are connected to a non-Markovian environment. To make our model more explicit, we use a non-Markovian model with two initially entangled qubits each connected locally to their own baths of spin chains shown here in Fig. 2. These are then examined analytically with very symmetric baths and numerically using smaller, unsymmetric baths, using the tools previously presented by two of us and others [3] we look at the differences between the volume of the QSE and the concurrence. Recently, some analysis was done on the

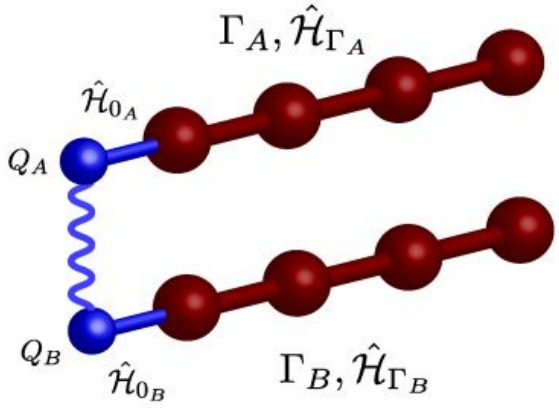


Fig. 2. Sketch of the model. Each of a pair of entangled qubits, Q_A and Q_B, is locally coupled to a spin chain, Γ_A and Γ_B via interaction Hamiltonians $\mathcal{H}_{0_A}$ and $\mathcal{H}_{0_B}$.

QSE where one of the parties is connected to a local, decohering channel. [4] Our work differs in that we have two non-Markovian baths and so the dynamics of the QSE are very rich. We look at the relationship between non-Markovianity and revivals in QSE volume. Interestingly, we find that Entanglement Sudden Death that we observe in these systems is not correspondingly represented in the QSE volume. The volume can decrease to almost zero and we do see quite a close correspondence between the QSE volume and the concurrence, but we do not see the same sudden death. We speculate that this is due to the presence of classical correlations which can explain some steering (not to be confused with EPR steering) so that even when the concurrence suddenly dies we can have some classical correlations between our qubits to explain the non-zero volume of the QSE.

References

1. S. Jevtic, M. Pusey, D. Jennings and T. Rudolph, arxiv 1303.4724 (2013)
2. A. Milne, S. Jevtic, D. Jennings, H. Wiseman, and T. Rudolph, arxiv 1403.0418 (2014)
3. T.J.G. Apollaro, A. Cuccoli, C. Di Franco, M. Paternostro, F. Plastina, and P. Verucchi, arxiv 1001.5440 (2010)
4. X. Hu and H. Fan, Phys. Rev. A **91**, 022301, (2015)

Computing many-party quantum correlations — analytical results

Leiba Rodman[1], Ilya M. Spitkovsky[1,2], Arleta Szkoła[3], and Stephan Weis[4]

[1] Department of Mathematics
College of William and Mary
P. O. Box 8795
Williamsburg, VA 23187-8795
[2] Division of Science and Mathematics
New York University Abu Dhabi
Saadiyat Island, P.O. Box 129188
Abu Dhabi, UAE
[3] Max Planck Institute for
Mathematics in the Sciences
Inselstrasse 22
04103 Leipzig, Germany
[4] Independent researcher

Abstract. We study the continuity of a genuine three-party correlation quantity of three qubits. This many-party correlation quantity, called *irreducible correlation* by Linden et al. [1], is based on the maximum-entropy principle. Remarkably, it is a discontinuous map for three qubits and a continuous map for classical bits. We use an approach of convex geometry and operator theory to investigate this continuity issue.

1 Maximum-entropy definition of many-party correlations

The work by Linden et al. [1] and Zhou [2] distinguishes correlations by particle numbers based on the maximum-entropy principle. For example, the *irreducible three-party correlation* $I^{(3)}(\rho)$ in the state ρ of a three-qubit system ABC is the information which can not be observed in any subsystem of less than three qubits.

More precisely, let M_d, $d \in \mathbb{N}$, denote the algebra of $d \times d$-matrices with complex entries, $\mathcal{M}_d$ the space of density matrices in M_d and

$$\rho^{(2)} : \mathcal{M}_8 \to \mathcal{M}_2 \times \mathcal{M}_2 \times \mathcal{M}_2, \quad \rho \mapsto (\rho_{BC}, \rho_{AC}, \rho_{AB})$$

the map from the global state $\rho = \rho_{ABC}$ to its two-party marginals ρ_{BC}, ρ_{AC} and ρ_{AB}. Every property of the state ρ which can be observed in a

two-party subsystem is contained in the triple of marginals $\rho^{(2)}(\rho)$ which is, according to Jaynes, represented in the most unbiased way by the maximum-entropy state $\rho^*[\rho^{(2)}(\rho)]$. Thereby the convex set of two-party marginals is denoted by

$$\mathcal{C} := \rho^{(2)}(\mathcal{M}_8)$$

and Jaynes' statistical inference map ρ^* chooses a state σ with maximal *von Neumann entropy* $S(\sigma) := -\operatorname{tr}\sigma\log(\sigma)$, that is

$$\rho^* : \mathcal{C} \to \mathcal{M}_8, \quad x \mapsto \operatorname{argmax}\{S(\sigma) \mid \sigma \in \mathcal{M}_8, \rho^{(2)}(\sigma) = x\}.$$

The non-negative *irreducible three-party correlation*

$$I^{(3)}(\rho) := S(\rho^*[\rho^{(2)}(\rho)]) - S(\rho)$$

quantifies deviation of ρ from the maximal entropy. It quantifies information not contained in $\rho^{(2)}(\rho)$ and hence genuine three-party correlations in ρ. These are present if and only if $I^{(3)}(\rho) > 0$.

2 The continuity issue

2.1 A discontinuity seen by pure state reconstruction

A result in [1] shows that for every pure state $\psi \in \mathcal{M}_8$ the pre-image $(\rho^{(2)})^{-1}[\rho^{(2)}(\psi)]$ is a singleton. So $I^{(3)}(\psi) = 0$, that is a pure three-qubit state has no irreducible three-party correlation. There is only one possible exception which is when ψ is local unitary equivalent to a pure state of the form $\alpha|000\rangle + \beta|111\rangle$. For example $I^{(3)}$ is discontinuous at the GHZ-state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ which has one bit of irreducible correlation.

2.2 Analytic approach: Convex geometry and operator theory

Based on earlier work [3] about the continuity of the inference ρ^* we have proved [4] that the irreducible three-party correlation $I^{(3)}$ is discontinuous at every point of the convex set $\mathcal{C}$ of two-party marginals which is a limit of extremal points of $\mathcal{C}$ but not an extremal point itself.

We have started [4] a systematic continuity analysis of the inference ρ^* in the setting of quantum inference which refers to two observables. This is based on numerical range techniques in operator theory.

References

1. Linden, N., Popescu, S., Wootters, W. (2002) Phys. Rev. Lett. 89(20) 207901
2. Zhou, D. (2008) Phys Rev Letters 101(18) 180505
3. Weis, S. (2014) Commun Math Phys 330(3) 1263–1292
4. Rodman, L., Spitkovsky, I. M., Szkoła, A., Weis, S. (2015) `arXiv:1502.02018`

Moments of Coinless Quantum Walks on Lattices

Raqueline Azevedo Medeiros Santos[1], Renato Portugal[1,2], and Stefan Boettcher[3]

[1] Laboratório Nacional de Computação Científica, Petrópolis, RJ 25651-075, Brazil
[2] Universidade Católica de Petrópolis, Petrópolis, RJ, 25685-070, Brazil
[3] Department of Physics, Emory University, Atlanta, GA 30322, USA

The coinless or staggered quantum walk model is defined by an evolution operator that is the product of two reflections, U_0 and U_1, acting on the site basis. These reflections can be obtained through a process of lattice tessellation as described by Falk [1]. Example of tessellations for the one-dimensional lattice is depicted in Fig. 1. Different tessellations

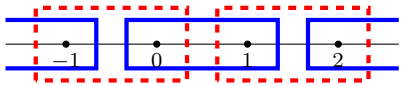


Fig. 1. Example of tessellations for the one-dimensional lattice. U_0 is associated to the blue tessellation (solid line) and U_1 is associated to the red tessellation (dashed line).

can be used to the generic d-dimensional lattice but some of them generate operators which describe trivial walks. Quantum search algorithms on two-dimensional lattices using the coinless model were analyzed in Refs. [2, 3, 1, 4]. Ref. [5] analyzed the dynamics of one-dimensional coinless walks and its relation with the coined model. The coinless model has not been so extensively analyzed as the coined model. Specially important in this context are the moments of the probability distribution. The mean square displacement, for example, gives us information about how far from the initial position a walker can be found. If quantum walks spread faster than random walks, there is hope for improving random-walk-based algorithms by using quantum walks.

We analyze the moments of the coinless model on lattices. Due to the translational invariance, it is possible to find a Fourier transform that generates a $2d \times 2d$ reduced evolution operator, which contains all information about the dynamics. After calculating the eigenvalues of this reduced operator, we obtain an analytical expression of the nth moment in terms of the nth derivative of the eigenvalues and give explicit solutions for the one- and two-dimensional lattices. For the one-dimensional lattice we use the most generic coinless quantum walk with a 2-site tessellation

taking a localized initial condition. For the two-dimensional lattice we use a 4-site tessellation taking the simplest basis vectors with non-localized initial conditions. In both cases we analyze the mean square displacement and obtain what are the best choice for the largest spread and compare with the results of the coined model. For more details, see [6].

For example, consider the one-dimensional lattice. The evolution operator in this case is a product of two reflections around the spaces generated by the vectors $\left|u_x^0\right\rangle = \cos\frac{\alpha}{2}\left|2x\right\rangle + e^{i\phi_1}\sin\frac{\alpha}{2}\left|2x+1\right\rangle$ and $\left|u_x^1\right\rangle = \cos\frac{\beta}{2}\left|2x+1\right\rangle + e^{i\phi_2}\sin\frac{\beta}{2}\left|2x+2\right\rangle$. The variance σ^2 will depend only on parameters α and β and the values of those parameters that produce the maximum σ^2 are depicted in Fig 2.

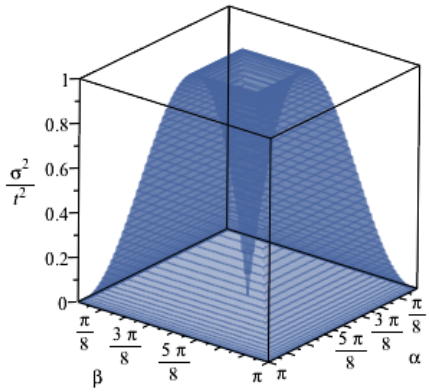


Fig. 2. Rescaled variance of the coinless quantum walk on the one-dimensional lattice with initial condition at the origin.

References

1. M. Falk. Quantum search on the spatial grid, 2013. arXiv:quant-ph/1303.4127.
2. A. Patel, K. S. Raghunathan, and P. Rungta. Quantum random walks do not need a coin toss. *Phys. Rev. A*, 71:032347, Mar 2005.
3. A. Patel, K. S. Raghunathan, and Md. A. Rahaman. Search on a hypercubic lattice using a quantum random walk. ii. $d = 2$. *Phys. Rev. A*, 82:032331, Sep 2010.
4. A. Ambainis, R. Portugal, and N. Nahimov. Spatial search on grids with minimum memory. arXiv:quant-ph/1312.0172.
5. R. Portugal, S. Boettcher, and S. Falkner. One-dimensional coinless quantum walks, 2014. arXiv:quant-ph/1408.5166v2.
6. R.A.M. Santos, R. Portugal, and S. Boettcher. Moments of coinless quantum walks on lattices, 2015. arXiv:quant-ph/1502.06293.

Degradable Channels From Products of Pure States

Vikesh Siddhu and Robert B. Griffiths

Physics Department, Carnegie-Mellon University

Abstract. A class of quantum channels is constructed using isometries that map a basis of pure states in the channel input $\mathcal{H}_a$ to a product of pure states on the tensor product $\mathcal{H}_b \otimes \mathcal{H}_c$ of the direct and complementary channel outputs. Degradable $a \to b$ channels are produced if there is a second isometry that maps $\mathcal{H}_b$ to a tensor product $\mathcal{H}_b \otimes \mathcal{H}_d$ of the channel output and an auxiliary system d. The Gram matrices of the different bases are related by Hadamard products making it easy to construct examples. The collection of degradable channels constructed in this way contains all twisted-diagonal and Hadamard channels, and some channels which are both degradable and conjugate degradable.

1 Summary

Degradable and conjugate degradable quantum channels (see [1, 2] for references) have the pleasant property that their quantum capacities are easily calculated. A large class of degradable channels can be constructed using isometries that map particular pure states to products of pure states. Some of these are also conjugate degradable, but the method does not yield conjugate degradable channels which are *not* degradable.

Let $\mathcal{H}_a$, $\mathcal{H}_b$, $\mathcal{H}_c$, $\mathcal{H}_d$ be four Hilbert spaces of equal finite dimension, where $\mathcal{H}_a$ corresponds to the entrance and $\mathcal{H}_b$ to the exit of the degradable channel, while $\mathcal{H}_c$ is the exit of the complementary channel and $\mathcal{H}_d$ an auxiliary system. Let J and K be isometries

$$J : \mathcal{H}_a \to \mathcal{H}_b \otimes \mathcal{H}_c, \quad K : \mathcal{H}_b \to \mathcal{H}_c \otimes \mathcal{H}_d. \tag{1}$$

The superoperator for the $a \to b$ channel is given by

$$\mathcal{N}_{b\,a}(\rho) = \mathrm{Tr}_c(J\rho J^\dagger), \tag{2}$$

and the other channels are defined using J or K in an analogous fashion.

Next let $\{|\alpha_j\rangle\}$, $\{|\beta_j\rangle\}$, $\{|\gamma_j\rangle\}$ and $\{|\delta_j\rangle\}$ be bases of $\mathcal{H}_a$, $\mathcal{H}_b$, $\mathcal{H}_c$, $\mathcal{H}_d$ consisting of normalized states *which in general are not mutually orthogonal*, and define J and K so that

$$J|\alpha_j\rangle = |\beta_j\rangle \otimes |\gamma_j\rangle, \quad K|\beta_j\rangle = |\gamma_j\rangle \otimes |\delta_j\rangle. \tag{3}$$

For J and K to be isometries it is necessary and sufficient that the Gram matrices satisfy

$$A_{jk} = \langle\alpha_j|\alpha_k\rangle = \langle\beta_j|\beta_k\rangle\langle\gamma_j|\gamma_k\rangle = B_{jk}C_{jk}, \text{ or } A = B * C,$$
$$B = C * D, \text{ with } D_{jk} = \langle\delta_j|\delta_k\rangle, \tag{4}$$

where $*$ denotes a Hadamard product of matrices. By following the trajectories of the dyads $|\alpha_j\rangle\langle\alpha_k|$ directly from a to c, or from a to b and thence to c, one can show that

$$\mathcal{N}_{c\,a} = \mathcal{N}_{c\,b} \circ \mathcal{N}_{b\,a}, \tag{5}$$

which is to say $\mathcal{N}_{c\,b}$ is the degrading map for the degradable channel $\mathcal{N}_{b\,a}$.

The Gram matrices A, B, C, and D have 1's on the diagonal since the basis states are normalized, and are positive definite because the basis states are linearly independent. Furthermore, the Hadamard product of two positive definite matrices is positive definite (e.g., p. 458 of [3]), and a positive definite matrix is always the Gram matrix for some basis. Consequently, a simple way of constructing a degradable channel is to start with two positive definite matrices C and D with all diagonal elements equal to 1, and then form the Hadamard products

$$B = C * D, \quad A = C * C * D. \tag{6}$$

Any twisted-diagonal channel [4] can be constructed in this way, and any Hadamard channel [5] by using a subspace (which might be the entire space) of the channel entrance $\mathcal{H}_a$. When the $|\alpha_j\rangle$ and the $|\beta_j\rangle$ are orthonormal bases, channels constructed in this way are conjugate degradable as well as degradable, but in all other cases they are only degradable. Our hope is that this fairly simple and "geometrical" approach will yield additional insights into why degradable channels are special, and the more general problem of additivity of quantum channel capacities.

References

1. Toby Cubitt, Mary-Beth Ruskai, and Graeme Smith. The structure of degradable quantum channels. *J. Math. Phys.*, 49:102104, 2008. arXiv:0802.1360v2.
2. Kamil Brádler. The existence of conjugate degradable channels that are not degradable. arXiv:1407.3942 v2, 2014.
3. Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1985.
4. Michael M. Wolf and David Pérez-García. Quantum capacities of channels with small environment. *Phys. Rev. A*, 75:012303, 2007.
5. Kamil Brádler, Patrick Hayden, Dave Touchette, and Mark M. Wilde. Trade-off capacities of the quantum hadamard channels. *Phys. Rev. A*, 81:062312, 2010. arXiv:1001.1732v2.

Classical Simulation of Quantum Walks on Clusters of Computers

David S. Souza, Franklin L. Marquezino, and Alexandre A. B. Lima

Federal University of Rio de Janeiro, Brazil
{davidsds, franklin, assis}@cos.ufrj.br

Abstract. We propose a classical simulator for quantum walks using Apache Hadoop in order to achieve high performance on distributed-memory clusters of computers. Our approach allows the simulation of quantum walks on situations where the required memory is typically very large, such as multi-particle quantum walks or quantum walks on fractals.

1 Introduction

Quantum walks are very important for the development of quantum algorithms. Although any low cost desktop computer would be able to simulate a quantum walk in principle, they are usually limited to a relatively small number of steps due to RAM limitations or lack of processing power. These restrictions limit numerical experiments that demand a large number of steps and very large Hilbert spaces. When multiple walkers interact, for instance, the problem is even worse because the calculations demand much higher computational costs and memory consumption.

There are many quantum walk simulators, such as QWalk [4] and HiperWalk [5], and other more generic simulators that can also be used to simulate quantum walks, such as QuIDDPro [6] and QuTIP [7]. Although other simulators as QuTiP and HiPerWalk support multiprocessing and perform the simulation in parallel, they are not specifically designed for distributed-memory environments.

The basic operations required to perform a quantum walk simulation are matrix multiplication and Kronecker product [3]. In order to mitigate the problems caused by memory consumption and to accelerate the execution of the simulation, we use Apache Hadoop [1] to make these calculations in parallel, thus reducing the amount of time required to perform the quantum walk simulation and allowing its execution with more steps.

The Apache Hadoop is a framework that allows the parallel processing of large data sets across clusters of computers using a simple programming model. For an algorithm to run on Hadoop, it must be implemented

using the Map/Reduce [2] model. In this model, the users specify a *map* function that processes key/value pairs to generate a new set of intermediate key/value pairs, and a *reduce* function that merges all intermediate values associated with the same intermediate key [2].

2 Implementation

In order to perform a quantum walk simulation we implemented two algorithms to run on Hadoop: matrix multiplication and Kronecker product. Both algorithms take as input two files, each one with a matrix. They run the necessary calculations in parallel and provide as output a file containing the result.

3 Contributions

Our approach is focused on simulations of quantum walks that require much more RAM memory than would be available on a conventional desktop computer. Examples of such simulations include quantum walks on fractals or with multiple walkers.

With matrix multiplications and Kronecker products running on Hadoop, we intend to allow the simulation of quantum walks in very large Hilbert spaces, *i.e.*, in scenarios that would cause a conventional computer to exceed its available RAM.

Acknowledgements. The authors acknowledge financial support from CNPq and CAPES.

References

1. Apache Hadoop, The Apache Hadoop Project. Website, 2015, http://hadoop.apache.org/
2. Dean, J. and Ghemawat, S., "MapReduce: simplified data processing on large clusters." Communications of the ACM 51.1 (2008): 107-113.
3. Portugal, R., Quantum walks and search algorithms. Springer, 2013.
4. Marquezino, F. L. and Portugal, R., "The QWalk simulator of quantum walks." Computer Physics Communications 179.5 (2008): 359-369.
5. HiPerWalk, High-Performance Quantum Walk Simulator. Users Manual, 2014, http://qubit.lncc.br/qwalk/hiperwalk.pdf
6. Viamontes, G.F., Markov, I. L. and Hayes, J.P., Quantum circuit simulation. Springer, 2009.
7. Johansson, J. R., Nation, P.D. and Nori, F., "QuTiP: An open-source Python framework for the dynamics of open quantum systems." Computer Physics Communications 183.8 (2012): 1760-1772.

Quantum Adiabatic Evaluation of Trees

Luís Tarrataca[1]

QCG/LNCC
Rio de Janeiro, Brazil

Tree evaluation is a crucial task in many computational problems which requires $O(N)$ time in order to analyse N elements. Although continuous- and discrete-time quantum algorithms exist to perform such an evaluation in $O(\sqrt{N})$ time, no quantum adiabatic procedure is known to exist. Quantum adiabatic algorithms rely on a slow system evolution, where a known initial state is evolved towards the ground state of a Hamiltonian encoding the answer to an optimization problem, alongside an energy minimisation function to perform a computation. Current approaches to quantum NAND tree evaluation rely, respectively, on a combination of plane wave transmission on a continuous walk and phase estimation on a weighted discrete walk to determine the value of a tree [2, 1]. Thus, it is natural to question how to tackle evaluation of NAND trees in an adiabatic context. Accordingly, a series of issues can be immediately considered. Namely, is it possible to devise adiabatic methods based on the existing formulations for tree evaluation? What are the main advantages and disadvantages associated with each procedure? What are the potential running times of potential methods?

The continuous-time approach relies on a Hamiltonian H representing the adjacency matrix of an extended version of the original graph. The authors showed that for energy values close to zero, *i.e.* $E \to 0$ then the amplitudes recurse down the tree in a manner that is equivalent to the NAND gate. Because trees are bipartite graphs their spectrum is symmetric around zero. As a result, applying H^2 instead of H will result in a remapped spectrum whose ground state has energy zero. This means that by preparing the adiabatic system in a state with energy close to zero and evolving towards the ground state of H^2 we are able to obtain information regarding the value of a tree. More specifically, by measuring the subspace corresponding to the root node and a node that was added connected to the root, respectively $r = 0$, it is possible to determine whether the tree evaluates to true or false. Furthermore, since H^2 starts behaving in accordance with the NAND gate when $E \in]0, \frac{1}{256N}[$, there is no need to perform full adiabatic evolution.

The real issue is how the gap between the two lowest energy levels of the interpolation Hamiltonian behaves. This is importante because the minimum gap will dictate overall performance. Unfortunately, performing simple simulations is enough to demonstrate that there is no clear general expression for the gap condition. Not surprisingly, lengthier bit sequences, and the associated increase in the number of dimensions, result in more complex expressions. This contrasts with the local adiabatic quantum search algorithm [3] where the gap expression could be easily determined. As a result, the most that can be performed is a set of numerical simulations that try to give an overview of the gap. However, given the exponential growth, in time and space, that is associated with Hilbert spaces of dimension 2^n, where n is the number of bits, we are only able to evaluate search spaces up to and including 16 bits. For these cases, the numerical plots exhibit relatively small variation with each increase in problem space size and there exists a close resemblance between the data points and the exponential function with a negative power. This behaviour hints at the possibility of performing some-type of fitting. However, as is the case with any type of fitting procedure there may be multiple hypothesis which may not necessarily correspond to the original function. One such possibility is the aforementioned exponential function. More specifically, given gap $g_k(s)$ it is possible to contemplate a fit based on function $a + b^{-s}$ where a and b are constants and s is the variable controlling the time evolution of the adiabatic interpolation. The average gap condition based on such a fitting has the form $0.0117078a + 103.268^{-s}$. By performing local adiabatic evolution it is possible to derive a $O\left(\frac{N^2}{\log N}\right)$ complexity. This result is a function of b, which for the instances analysed appears to be showing as a worse-case scenario a quadratic growth. Consequently, the final complexity of the adiabatic evolution is $O\left(\frac{N^4}{\log N^2}\right)$, which represents an overall performance penalty of $N^3/(2 \log N)$ when compared against the classical $O(N)$ time.

References

1. A. Ambainis, A.M. Childs, and B.W. Reichardt. Any and-or formula of size n can be evaluated in time $n^{\frac{1}{2}+o(1)}$ on a quantum computer. In *Foundations of Computer Science, 2007. FOCS '07. 48th Annual IEEE Symposium on*, pages 363 –372, oct. 2007.
2. Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum algorithm for the hamiltonian nand tree. *Theory of Computing*, 4(1):169–190, 2008.
3. Jérémie Roland and Nicolas J. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev. A*, 65:042308, Mar 2002.

Secrecy in prepare-and-measure CHSH games with a qubit bound

Erik Woodhead[1] and Stefano Pironio[2]

[1] ICFO – Institut de Ciències Fotòniques, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain
[2] Laboratoire d'Information Quantique, CP 225, Université libre de Bruxelles, Av. F. D. Roosevelt 50, 1050 Bruxelles, Belgium

Semi-device-independent [1] quantum key distribution (QKD) protocols are protocols whose correct functioning can be established based on the assumption of a dimension bound on at least one of the devices. In terms of the degree of trust placed in the implementation, this places semi-device-independent protocols midway between fully trusted and fully device-independent (DI) QKD. Unlike DIQKD protocols, whose correct functioning is established based on the detection of nonlocal statistics and which require the preparation of entangled states as a resource, semi-DIQKD can be implemented in a prepare-and-measure configuration, where one party (Alice) prepares the necessary quantum states and transmits them to a second party (Bob), who then measures them.

In traditional QKD, there is a well known correspondence between prepare-and-measure and entanglement-based protocols, in that a security proof of a given entanglement-based QKD protocol also implies the security of its prepare-and-measure analogue. In the device-independent setting the correspondence is less clear. In particular, the prepare-and-measure analogue of a DIQKD protocol cannot be fully device independent and the states prepared by the source will generally not satisfy a condition of basis independence. Some minimal assumptions about the devices must thus be introduced; the approach taken in semi-DIQKD is to assume a bound on the dimension of the emitted source states.

In this work, we consider a prepare-and-measure analogue of the DIQKD protocol studied in [2], whose security is based on the violation of the CHSH inequality, $S \leq 2$, where the CHSH correlator S is defined by

$$S = \sum_{abxy} (-1)^{a+b+xy} P(ab \mid xy)\,, \tag{1}$$

$x, y \in \{0, 1\}$ are Alice's and Bob's possible inputs, $a, b \in \{0, 1\}$ are the possible outputs, and $P(ab \mid xy)$ is the joint probability that Alice and Bob obtain results a and b given that they chose the inputs x and y. In

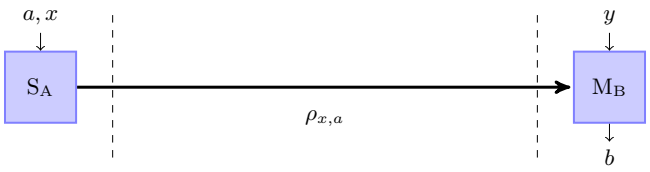


Figure 1. The semi-device-independent scenario with qubit source. Alice's source ($\mathrm{S_A}$) can emit one of four different qubit states $\rho_{x,a}$ depending on a choice of input $(x, a) \in \{0,1\}^2$. Bob's measurement device ($\mathrm{M_B}$) performs one of two measurements depending on a choice of input $y \in \{0,1\}$, yielding an outcome $b \in \{0,1\}$.

the semi-DI version, illustrated in Figure 1, Alice's output a becomes an additional input and the measurement device is replaced with a source which emits one of four quantum states, $\rho_{x,a}$, depending on the input $(x, a) \in \{0,1\}^2$. In this setting, Alice and Bob can estimate a prepare-and-measure version of the CHSH correlator, which we express here as

$$S = \tfrac{1}{2} \sum_{abxy} (-1)^{a+b+xy} P(b \mid axy)\,. \tag{2}$$

Assuming that the source states $\rho_{x,a}$ share their support on a common two-dimensional Hilbert space, that Alice chooses the input $a \in \{0,1\}$ uniformly and randomly, and allowing for an adversary (Eve) who may attack the states unitarily and individually and identically, our main result is a lower bound on the randomness of the input a from Eve's perspective, conditioned on a choice of input x (for instance, $x = 0$), which depends only on S. Specifically, we show that

$$H_{\min}(A \mid \mathrm{E}, x = 0) \geq 1 - \log_2\bigl(1 + \sqrt{2 - S^2/4}\bigr)\,, \tag{3}$$

where A is Alice's choice of input (treated as a random variable) and E denotes Eve's quantum side information.

Our main result (3) has the same functional dependence on the correlator S as an analogous bound derived for the entanglement-based scenario, which first appeared in the context of device-independent randomness generation and later in a number of DIQKD security proofs.

References

1. Pawłowski, M., Brunner, N.: Semi-device-independent security of one-way quantum key distribution. Phys. Rev. A **84** (Jul 2011) 010302(R)
2. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett **98** (Jun 2007) 230501

On the Breakdown of Quantum Search with Spatially Distributed Marked Vertices

Thomas G. Wong

Faculty of Computing, University of Latvia, Raiņa bulv. 19, Rīga, LV-1586, Latvia

Abstract. Grover's algorithm finds one of k "marked" items in an *unstructured* "database" of size N in time $O(\sqrt{N/k})$, and the algorithm's parameter(s) and runtime are unchanged no matter which of the k items are marked. For *structured* search by continuous-time quantum walk, however, we show that rearranging the marked elements can cause the parameter(s) or runtime to vary such that, without prior knowledge of the spatial distribution of the marked elements, a potentially sub-exponential number of configurations would need to be tried, meaning it would be better to not run the search algorithm at all.

A full paper with references is available at arXiv:1501.07071 [quant-ph].

A randomly walking quantum particle searches on a graph by starting in a uniform superposition over the N vertices and evolving by Schrödinger's equation with Hamiltonian

$$H = -\gamma A - \sum_w |w\rangle\langle w|,$$

where γ is the jumping rate, A is the adjacency matrix of the graph, and $\sum_w |w\rangle\langle w|$ marks the k vertices to search for. Then Grover's algorithm is simply search on the (unstructured) complete graph. When γ takes its critical value of $\gamma_c = 1/N$, the system evolves to the marked vertices in time $(\pi/2)\sqrt{N/k}$, as shown in Fig. 1. When γ is away from its critical value, however, the initial state is approximately an eigenstate of H, so the system fails to evolve for large N, also shown in Fig. 1. Thus to use the algorithm, one must know: (1) the parameter(s) to use (*i.e.*, γ_c in this formulation) and (2) the runtime at which to stop and measure the system. On the complete graph, these two quantities are unchanged no matter which k vertices are marked.

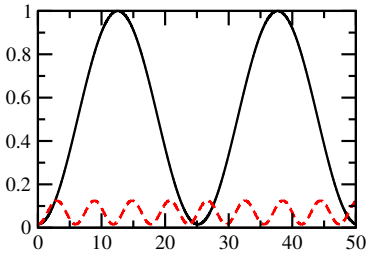


Fig. 1. Success probability vs time for search on the complete graph of $N = 1024$ vertices with $k = 16$ marked vertices. The solid black and red dashed curves are $\gamma = \gamma_c = 1/N$ and $\gamma = 2\gamma_c = 2/N$, respectively.

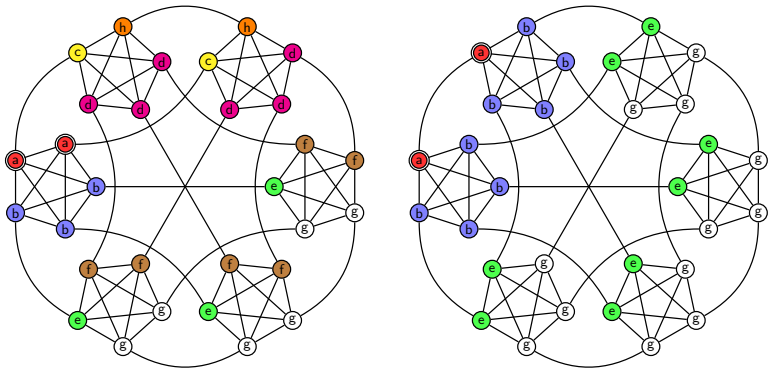


Fig. 2. Two ways to distribute two marked vertices, indicated by double circles, on the simplex of complete graphs.

On non-complete graphs, however, we show that the spatial arrangement of the marked vertices can change these two quantities. That is, one arrangement of k marked vertices can require a particular γ_c and runtime, while another arrangement can require different values. Thus without knowledge of the spatial distribution of the k marked vertices, one may not know which γ_c and runtime to use. This raises issues not addressed by previous work on spatial search by quantum walk, which typically only give runtime *scalings*.

In particular, we analytically derive γ_c's and runtimes for search on the "simplex of complete graphs," examples of which are shown in Fig. 2. We analyze all four possible configurations of two marked vertices, and four additional configurations with large numbers of marked vertices. Our results suggest that moving marked vertices from one complete graph to another affects γ_c (and perhaps the runtime), while moving them within a complete graph makes no difference.

In some cases, the marked vertices have a sub-exponential number of ways to be distributed among the complete graphs. Since our results suggest that there are different γ_c's for each of these arrangements, trying each possibility is clearly prohibitive. Thus it would be better to classically guess for a marked vertex. This leaves many open questions to determine whether the number of γ_c's is truly sub-exponential, and if quantum walks can speed up search of spatial regions without knowing the distribution of the marked vertices.