August 30, 2016 (Tuesday)

09:00 - 10: 00 **[Invited Talk]** *The largest possible gaps between quantum and classical Algorithms*……1
Andris Ambainis (University of Latvia)

10:30 - 11: 00 **[Long Talk]** *Higher-Effciency Quantum Algorithms for Simulation of Chemistry*……2
Ryan Babbush (Google), Dominic W. Berry (Macquarie University), Ian D. Kivlichan (Harvard University), Annie Y. Wei (Harvard University), Dean Southwood (Macquarie University), Peter J. Love (Tufts University), and Alań Aspuru-Guzik (Harvard University)

11:00 - 11:30 **[Long Talk]** *Perfect commuting-operator strategies for linear system games*.....5
Richard Cleve (University of Waterloo), Li Liu (University of Waterloo), and William Slofstra (University of Waterloo)

11:30 - 12:00 **[Long Talk]** *A Four-Round LOCC Protocol Outperforms All Two-Round Protocols in Reducing the Entanglement Cost for A Distributed Quantum Information Processing*……..7
Eyuri Wakakuwa (University of Electro-Communications), Akihito Soeda(University of Tokyo), and Mio Murao (University of Tokyo)

14:00 - 16:00 **[Parallel Session A]**

14:00 - 14:20 *Universal Quantum Emulator*……9
Iman Marvian (MIT) and Seth Lloyd (MIT)

14:20 - 14:40 *Characterizing Supremacy in Near Term Quantum Devices*……..……..…11
Sergio Boixo (Google), Sergei Isakov(Google), Vadim Smelyanskiy (Google), Ryan Babbush (Google), Ding Nan (Google), Zhang Jiang (NASA), John Martinis (Google), and Hartmut Neven (Google)

14:40 - 15:00 *Factoring with Qutrits: Application of Improved Circuit Synthesis on Two Ternary Architectures*……..14
Alex Bocharov (Microsoft), Shawn X. Cui (UCSB), Martin Roetteler (Microsoft), and Krysta M.Svore (Microsoft)

15:00 - 15:20 *Space-Efficient Error-Reduction for Unitary Quantum Computations*……..17
Bill Fefferman (University of Maryland), Hirotada Kobayashi (National Institute of Informatics), Cedric Yen-Yu Lin (University of Maryland), Tomoyuki Morimae (Gunma University), and Harumichi Nishimura (Nagoya University)

15:20 - 15:40 *Hamiltonian quantum computer in one dimension*…..……..……...……19
Tzu-Chieh Wei (State Uiversity of New York at Stony Brook) and John C. Liang (Rumson-Fair Haven Regional High School)

15:40 - 16:00 *Nonlocal correlations: Fair and Unfair Strategies in Bayesian Game*…..……21
Arup Roy (Indian Statistical Institute), Amit Mukherjee (Indian Statistical Institute), Tamal Guha (Indian Statistical Institute), Sibasish Ghosh (Institute of Mathematical Sciences),

Some Sankar Bhattacharya (Indian Statistical Institute), and Manik Banik (Institute of Mathematical Sciences)

14:00 – 16:00 **[Parallel Session B]**

14:00 - 14:20 *Bell Correlations in Many-Body Systems*……23
Jean-Daniel Bancal (University of Basel), Roman Schmied (University of Basel), Baptiste Allard (University of Basel), Matteo Fadel (University of Basel), Valerio Scarani (National University of Singapore), Philipp Treutlein (University of Basel), and Nicolas Sangouard (University of Basel)

14:20 - 14:40 *Reliable and robust entanglement witness*……25
Xiao Yuan (Tsinghua University, Beijing), Quanxin Mei (Tsinghua University, Beijing), Shan Zhou (Tsinghua University, Beijing), and Xiongfeng Ma (Tsinghua University, Beijing)

14:40 - 15:00 *Separability of Bosonic States*……27
Nengkun Yu (University of Technology Sydney / University of Waterloo / University of Guelph)

15:00 - 15:20 *A geometric approach to entanglement quantification with polynomial measures*……29
Bartosz Regula (University of Nottingham) and Gerardo Adesso (University of Nottingham)

15:20 - 15:40 *An Improved Semidefinite Programming Upper Bound on Distillable Entanglement and Nonadditivity of Rains' Bound*……31
Xin Wang (University of Technology Sydney) and Runyao Duan (University of Technology Sydney / Chinese Academy of Sciences)

15:40 - 16:00 *Extendability, complete extendability and a measure of entanglement for Gaussian states*……33
B. V. Rajarama Bhat (Indian Statistical Institute), K. R. Parthasarathy (Indian Statistical Institute), and Ritabrata Sengupta (Indian Statistical Institute)

16:30-18:30 **[Poster session]**

Posters

PT1 *A lower bound on expected communication cost of quantum state redistribution*……35
Anurag Anshu (National University of Singapore)

PT2 *An approximated single photon state generation from coherent states entangled with qubits by measuring qubits*……59
Fumiaki Matsuoka (Hokkaido University) and Akihisa Tomita (Hokkaido University)

PT3 *Asymptotic Convertibility of Entanglement: A General Approach to Entanglement Concentration and Dilution*……61
Yong Jiao (University of Electro-Communications), Eyuri Wakakuwa (University of Electro-Communications), and Tomohiro Ogawa (University of Electro-Communications)

PT4 *Attenuated quantum channel with probabilistic transmissivity*……63
Kenshiro Kita (Aichi Prefectural University), Shinji Koyama (Aichi Prefectural University),

Minami Tanaka (Aichi Prefectural University), and Tsuyoshi Sasaki Usuda (Aichi Prefectural University)
PT5 *Bridging the theory and experiment for device-independent quantum information*……..….65
Pei-Sheng Lin (National Cheng Kung University), Denis Rosset (National Cheng Kung University), and Yeong-Cherng Liang (National Cheng Kung University)
PT6 *Device-independent witnesses for entanglement depth: a case study*……..….67
Jui-Chen Hung (National Cheng Kung University) and Yeong-Cherng Liang (National Cheng Kung University)
PT7 *Estimation on the execution time of a quantum computer from the analysis on quantum assembly code*……69
Yongsoo Hwang (Electronics and Telecommunications Research Institute) and Byung-Soo Cho (Electronics and Telecommunications Research Institute)
PT8 *Generating tripartite nonlocality from bipartite resources*……...71
Zhaofeng Su (University of Technology Sydney) and Yuan Feng (University of Technology Sydney)
PT9 *Graph-Associated Entanglement Cost of Multipartite State in Exact and Finite-Block-Length Approximate Construction*……..…73
Hayata Yamasaki (University of Tokyo), Akihito Soeda (University of Tokyo), and Mio Murao (University of Tokyo)
PT10 *Homological codes and abelian anyons*……..……..……...75
Péter Vrana (Budapest University of Technology and Economics) and Máté Farkas (Budapest University of Technology and Economics / University of Gdańsk)
PT11 *On Thermalisation of Two-Level Quantam Systems*……..……77
Sagnik Chakraborty (The Institute of Mathematical Sciences), Prathik Cherian J (The Institute of Mathematical Sciences), and Sibasish Ghosh (The Institute of Mathematical Sciences)
PT12 *Optimization of Quantum Circuits with Multiple Outputs*……..……..80
Masato Onoda (Ritsumeikan University), Kouhei Kushida (Ritsumeikan University), and Shigeru Yamashita (Ritsumeikan University)
PT13 *Parallelization of Braiding Operations for Topological Quantum Computation*……...82
Kotaro Hoshi (Ritsumeikan University) and Shigeru Yamashita (Ritsumeikan University)
PT14 *Performance of Coupled Systems as Quantum Thermodynamic Machines*…..……84
George Thoma (The Institute of Mathematical Sciences), Manik Banik (The Institute of Mathematical Sciences), and Sibasish Ghosh (The Institute of Mathematical Sciences)
PT15 *Quantum Algorithm for Linear Equations with a Circulant Matrix*……..……...87
Souichi Takahira (Aichi Prefectural University), Asuka Ohashi (Ritsumeikan University), Tomohiro Sogabe (Nagoya University), and Tsuyoshi Sasaki Usuda (Aichi Prefectural University)

PT16 *Quantum Circuit Design of Integer Division Optimizing Ancillary Qubits and T-count*……..89
Himanshu Thapliyal (University of Kentucky), T. S. S. Varun (University of Kentucky), and Edgard Munoz-Coreas (University of Kentucky)
PT17 *Quantum Computation with Flying Electron Spin Qubits in Surface Acoustic Wave Systems* ……..……....91
David Arvidsson-Shukur (University of Cambridge / Hitachi Cambridge Laboratory), Jacek Mosakowski (University of Cambridge / Hitachi Cambridge Laboratory), Mrittunjoy Guha-Majumdar (University of Cambridge / Hitachi Cambridge Laboratory), Ward Haddadin (University of Cambridge), and Crispin Barnes (University of Cambridge)
PT18 *Quantum input-output algorithms for quantum systems with limited controllability*……..…..94
Ryosuke Sakai (University of Tokyo), Akihito Soeda (University of Tokyo), and Mio Murao (University of Tokyo)
PT19 *Quantum Media Conversion Between SAW Driven Flying Electron-Spin Qubits and Flying Photon-Polarization Qubits*…….……96
H. V. Lepage (University of Cambridge) and C. H. W. Barnes (University of Cambridge)
PT20 *Quantum Multiclass Support Vector Machine with Quantum One Against All Approach for Big Data Classification*……...98
Arit Kumar Bishwas (Amity University), Ashish Mani (Amity University), and Vasile Palade (Coventry University)
PT21 *Reducing Loops for Topological Cluster State Quantum Computation*……100
Kentaro Haneda (Ritsumeikan University), Shigeru Yamashita (Ritsumeikan University), Simon Devitt (Riken), and Kae Nemoto (National Institute of Informatics)
PT22 *Reduction of computation complexity of classical optimal decoding by adiabatic quantum computation*…….……..102
Yuta Nishino (Aichi Prefectural University), Souichi Takahira (Aichi Prefectural University), Akihito Kadoya (Aichi Prefectural University), Asuka Ohashi (Ritsumeikan University), and Tsuyoshi Sasaki Usuda (Aichi Prefectural University)
PT23 *Reduction of Quantum Cost by Changing the Functionality*……..……104
Nurul Ain Binti Adnan (Ritsumeikan University), Kouhei Kushida (Ritsumeikan University), and Shigeru Yamashita (Ritsumeikan University)
PT24 *Regularized Boltzmann entropy determines possibility of macroscopic adiabatic transformation*……..……..……106
Hiroyasu Tajima (RIKEN) and Eyuri Wakakuwa (University of Electro-Communications)
PT25 *States evolution of a quantum-feedback-enhanced single photon source*……....108
C. Y. Chang (Georgia Institute of Technology / Georgia Tech Lorraine), D. S. Citrin (Georgia Institute of Technology / Georgia Tech Lorraine), L. Lanco (LPN/CNRS), and P. Senellart (LPN/CNRS)
PT26 *Steering fraction and its application to the superactivation of Einstein-Podolsky-Rosen*

steering……110
Chung-Yun Hsieh (Tsing Hua University, Hsinchu), Yeong-Cherng Liang (National Cheng Kung University), and Ray-Kuang Lee (Tsing Hua University, Hsinchu / National Center for Theoretical Science)
PT27 *Visualizing the sets of 3-local and 3-quantum correlations*……112
Rui-Yang You (National Cheng Kung University), Denis Rosset (National Cheng Kung University / University of Geneva), and Yeong-Cherng Liang (National Cheng Kung University)

The largest possible gaps between quantum and classical algorithms

Andris Ambainis

University of Latvia

Abstract. We investigate the biggest possible gaps between quantum and classical algorithms in the query model of computation (which encompasses most of the known quantum algorithms). We consider two settings: computing partial functions and computing total functions.

For partial functions, we exhibit a property-testing problem called Forrelation, where one needs to decide whether one Boolean function is highly correlated with the Fourier transform of a second function. We show that this problem can be solved using 1 quantum query but any randomized algorithm needs $\Omega(\sqrt{N}/logN)$ queries (improving an $\Omega(N^{1/4})$ lower bound of Aaronson). We also show that this separation is close to being optimal: any 1-query quantum algorithm can be simulated by a randomized algorithm that makes $\Omega(\sqrt{N})$ queries and any t-query quantum algorithm whatsoever can be simulated by an $\Omega(N^{1-1/2t})$-query randomized algorithm. We conjecture that a natural generalization of Forrelation achieves the optimal t versus $\Omega(N^{1-1/2t})$ separation for all t.

For total functions, much smaller gaps between different models of computation are achievable (due to the fact that the algorithm must output a decisive answer on every input). Before our work, the biggest known gap for total functions was the quadratic gap achieved by Grover's search algorithm. We improve on this, showing a function that can be computed by a quantum algorithm making m queries but requires $\Omega(m^4/log^c m)$ queries for deterministic algorithms. We also substantialy improve the biggest known advantage for exact quantum algorithms (algorithms that always output the correct answer), to a nearly-quadratic (m queries for an exact quantum algorithms vs. $\Omega(m^2/log^c m)$ queries for classical algorithms) and solve two longstanding open questions about relations between classical models of computation: - we show a function that can be computed by a randomized algorithm with m queries but requires $\Omega(m^2/log^c m)$ queries deterministically, improving over a result by Snir from 1986; - we show the first example of a function for which randomized algorithms that are allowed to make a mistake with a small probability are better than zero-error randomized algorithms.

Joint work with Scott Aaronson (STOC'2015, arxiv:1411.5729) and Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha and Juris Smotrovs (STOC'2016, arxiv:1506.04719).

Higher-Efficiency Quantum Algorithms for Simulation of Chemistry

Ryan Babbush[1] * Dominic W. Berry[2] † Ian D. Kivlichan[3] Annie Y. Wei[3]
Dean Southwood[2] Peter J. Love[4] Alán Aspuru-Guzik[3]

[1] *Quantum A. I. Lab, Google, Venice CA 90291, USA*
[2] *Department of Physics and Astronomy, Macquarie University, Sydney, NSW 2109, Australia*
[3] *Department of Chemistry and Chemical Biology, Harvard University, Cambridge, MA 02138, USA*
[4] *Department of Physics and Astronomy, Tufts University, Medford, MA 02155, USA*

Abstract. We introduce novel algorithms for the quantum simulation of molecular systems which are asymptotically more efficient than those based on the Lie-Trotter-Suzuki decomposition. Our results build upon recently developed techniques for simulating Hamiltonian evolution using a Taylor series. The key difficulty in applying algorithms for general sparse Hamiltonian simulation to quantum chemistry is that a query, corresponding to computation of an entry of the Hamiltonian, is difficult to compute. This means that the gate complexity would be much higher than quantified by the query complexity. We solve this problem with a novel quantum algorithm for on-the-fly computation of integrals that is exponentially faster than classical sampling. We apply this technique in two different representations. First, we use the second quantized molecular Hamiltonian, which can be decomposed into local Hamiltonians. Second, we use the Configuration Interaction representation of the molecular Hamiltonian, which we decompose into 1-sparse matrices using a novel decomposition that leads to improved scaling. Our second approach yields gate complexity scaling as $\eta^2 N^3$, where N is the number of spin orbitals and η is the number of electrons. This is a dramatic improvement over the best previous approach which formally scaled as N^8.

Keywords: Hamiltonian Simulation, Quantum Algorithms, Quantum Chemistry, Lie-Trotter-Suzuki

As small, fault-tolerant quantum computers come increasingly close to viability there has been substantial renewed interest in quantum simulating chemistry [1–3] due to low qubit requirements and industrial importance [4–15]. Using arbitrarily high-order Lie-Trotter-Suzuki formulas, the tightest known bound on the gate count of any quantum simulation of chemistry is $\widetilde{\mathcal{O}}(N^8 t/\epsilon^{o(1)})$ [16, 17], where ϵ is the precision and N is the number of spin-orbitals. However, using significantly more practical Lie-Trotter decompositions, the best known gate complexity is $\widetilde{\mathcal{O}}(N^9\sqrt{t^3/\epsilon})$ [7]. With typical numbers of orbitals, such scaling becomes prohibitively costly [6].

The scaling using Lie-Trotter-Suzuki formulas originates because the scaling of that approach is not optimal in the sparseness d of the Hamiltonian. Lie-Trotter-Suzuki formulas have scaling at least as d^2, whereas more advanced approaches to the sparse Hamiltonian simulation problem yield scaling that is close to linear in d [18–21]. Note that these are the scalings if a decomposition of the Hamiltonian into a sum is known, as is the case for quantum chemistry. The difficulty with the more advanced approaches is that they quantify the complexity in terms of an oracle, corresponding to calculation of matrix entries of the Hamiltonian. For quantum chemistry, the matrix entries of the Hamiltonian must be calculated by evaluation of a integral, which is computationally intensive. As a result, those approaches would yield substantially higher cost in terms of gate counts.

We build upon the simulation technique introduced in [20] which is based on implementing a truncated Taylor series. In order to evaluate the integral, we discretize it on a grid. Then our quantum algorithm is able to evaulate this integral with only logarithmic cost in the number of grid points. This speedup is possible, because the integral is only used for the weighting of terms in the Hamiltonian evolution, and the algorithm does not need to output an explicit value of the integral. Our algorithms also need to use a database of the orbitals, with complexity $\widetilde{\mathcal{O}}(N)$.

We first use the second quantized molecular Hamiltonian, where the N spin-orbital system is encoded on N qubits, which yields complexity $\widetilde{\mathcal{O}}(N^5 t)$. Our best result uses the Configuration Interaction representation of the Hamiltonian, where the sparseness is $d = \mathcal{O}(\eta^2 N^2)$, together with a novel decomposition of the Hamiltonian into only $\mathcal{O}(d)$ 1-sparse Hamiltonians (whereas general decomposition techniques require at least d^2). This enables us to obtain complexity scaling as $\widetilde{\mathcal{O}}(\eta^2 N^3 t)$, which is a significant improvement in N. Moreover, the scaling is logarithmic in ϵ. It has been shown that for real molecules, the scaling of the original Trotterized quantum chemistry algorithm can be significantly improved [6–10]. Similarly, for real molecules, the complexity of our algorithm is likely to be further improved; this is a question for future work.

In summary, we have provided practical quantum algorithms to solve an industrially important problem (quantum chemistry) with the lowest asymptotic complexity in the literature. Our improved scalings should allow for the quantum simulation of molecular systems much larger than would be possible using Trotter-based methods.

Method

Our technique builds upon the simulation procedure described in [20], which we first summarize. Given a Hamiltonian that is a weighted sum of unitaries, the

*babbush@google.com
†dominic.berry@mq.edu.au

truncated Taylor series of the propagator can also be expressed as a weighted sum of unitary operators. To implement this sum, an ancilla register is prepared in a superposition state with amplitudes proportional to the square roots of the coefficients of terms in the Taylor series sum. This task is performed using an operator referred to as B. Next, an operator is applied to the system which coherently executes a single term in the Taylor series sum that is selected according to the ancilla register. This task is performed using an operator referred to as select(H). By applying $B^\dagger$select(H) B, one probabilistically simulates evolution under the propagator. The algorithm is made deterministic using oblivious amplitude amplification [19]. This procedure is implemented on many time segments to obtain the complete evolution.

In second quantization one can expand the molecular electronic structure Hamiltonian as a sum of unitaries via

$$H = \sum_{ij} h_{ij} a_i^\dagger a_j + \frac{1}{2} \sum_{ijk\ell} h_{ijk\ell} a_i^\dagger a_j^\dagger a_k a_\ell = \sum_{\gamma=1}^{\Gamma} W_\gamma H_\gamma, \quad (1)$$

where the operators $a_i^\dagger$ and a_j obey the fermionic anticommutation relations and the scalar coefficients W_γ are given as spatial integrals with no closed-form analytical solution. The state is represented on the quantum computer using N qubits to indicate the occupation of each of the orbitals. Using the Jordan-Wigner transformation [22, 23], the fermionic operators can be written as sums of unitary operators H_γ, which are just tensor products of Pauli operators. The number of these operators is $\Gamma = \mathcal{O}(N^4)$.

One might construct the operator B by precomputing the W_γ and using a database to prepare the ancilla superposition state. However, accessing this data would have time complexity of at least $\Omega(\Gamma)$. The number of segments is also $\Omega(\Gamma)$, so that approach would yield complexity no better than N^8, not improving over Lie-Trotter formulas. Instead, we exploit the fact that the W_γ are defined by integrals. We approximate these integrals as finite Riemann sums so that

$$W_\gamma = \int_{\mathcal{Z}} w_\gamma(\vec{z})\, d\vec{z} \approx \frac{\mathcal{V}}{\mu} \sum_{\rho=1}^{\mu} w_\gamma(\vec{z}_\rho), \quad (2)$$

where $\vec{z}_\rho$ is a point in the integration domain at grid point ρ. Equation (2) represents a discretization of the integrals defining the W_γ using μ grid points where the domain of the integral, denoted as $\mathcal{Z}$, has been truncated to have total volume $\mathcal{V}$. This truncation is possible because the functions $w_\gamma(\vec{z})$ can be chosen to decay exponentially for molecules studied in chemistry. Our algorithm is effectively able to compute this integral with complexity logarithmic in the number of grid points.

If we were to use the decomposition of the Hamiltonian directly with this integral, then the complexity would not be improved because of the difficulty of preparing a state with amplitudes $\sqrt{w_\gamma(\vec{z}_\rho)}$. Instead we further decompose each $w_\gamma(\vec{z}_\rho)$ into a sum of terms which differ only by a sign. The decomposition is of the form

$$w_\gamma(\vec{z}) \approx \zeta \sum_{m=1}^{M} w_{\gamma,m}(\vec{z}), \qquad w_{\gamma,m}(\vec{z}) \in \{-1, +1\}. \quad (3)$$

Using this decomposition, we can express the Hamiltonian as a sum of unitaries weighted by identical amplitudes which differ only by an easily computed sign,

$$H = \frac{\zeta \mathcal{V}}{\mu} \sum_{\gamma=1}^{\Gamma} \sum_{m=1}^{M} \sum_{\rho=1}^{\mu} w_{\gamma,m}(\vec{z}_\rho) H_\gamma. \quad (4)$$

The number of terms in the sum has been greatly increased, but the complexity is only logarithmic in the number of terms in the sum. This representation enables us to implement B by making a single query to the integrand. For quantum chemistry the cost of sampling the integrand is $\widetilde{\mathcal{O}}(N)$, which is needed to access a database of orbitals, which are chosen in advance classically. The number of time segments required for the simulation is $\widetilde{\mathcal{O}}(N^4 t)$, resulting in an overall complexity for the simulation of $\widetilde{\mathcal{O}}(N^5 t)$.

Our second algorithm uses the Configuration Interaction representation of the Hamiltonian (known as the CI matrix). The CI matrix uses a compressed basis, where the numbers of the occupied orbitals are stored, rather than the using qubits for all the orbitals. This reduces the number of qubits needed to store the state to $\mathcal{O}(\eta \log N)$, where η is the number of electrons. Though the CI matrix cannot be expressed as a sum of polynomially many local Hamiltonians, a paper by Toloui and Love [24] demonstrated that the CI matrix can be decomposed as a sum of $\mathcal{O}(N^4)$ 1-sparse Hermitian operators.

If we were to just use the decomposition technique of Toloui and Love we would obtain the same scaling as in our first algorithm. Instead we introduce a decomposition into $\mathcal{O}(\eta^2 N^2)$ 1-sparse Hermitian operators. This technique is based on taking the i'th occupied orbital in the list, and exciting it by p, and the j'th occupied orbital and exciting it by q. Since i and j are at most η, and p and q can each take $\mathcal{O}(N)$ different values, the total number of alternatives is $\mathcal{O}(\eta^2 N^2)$.

Given i, j, p and q, one can connect a list of occupied orbitals α to a list of occupied orbitals β. The subtlety is that we also need to be able to obtain α from β, and the simple scheme would be ambiguous. To resolve the ambiguity, we first choose whether i and j are taken as indexing the occupied orbitals in α or β according the separation of the occupied orbitals, in such a way as to minimize the ambiguity. Then we use two additional bits b_1, b_2 to resolve the remaining ambiguity.

Using techniques introduced in [19], we further decompose the 1-sparse operators into unitary operators which are also self-inverse. In this representation, the Hamiltonian itself, rather than the coefficients of terms, is an integral over a Hermitian matrix-valued function. Accordingly, we can use the same strategy for computing integrals on-the-fly in order to compute matrix elements of the Hamiltonian. Due to the improved decomposition, the complexity is improved to $\widetilde{\mathcal{O}}(\eta^2 N^3 t)$.

References

[1] Seth Lloyd. Universal Quantum Simulators. *Science*, 273(5):1073–1078, August 1996.

[2] Alán Aspuru-Guzik, Anthony D Dutoi, Peter J Love, and Martin Head-Gordon. Simulated Quantum Computation of Molecular Energies. *Science*, 309(5741):1704, 2005.

[3] James D Whitfield, Jacob Biamonte, and Alán Aspuru-Guzik. Simulation of electronic structure Hamiltonians using quantum computers. *Mol. Phys.*, 109(5):735–750, 2011.

[4] Libor Veis and Jirí Pittner. Adiabatic state preparation study of methylene. *The Journal of Chemical Physics*, 140(214111):1–21, 2014.

[5] James Daniel Whitfield. Unified views of quantum simulation algorithms for chemistry. *e-print arXiv: 1502.03771*, 2015.

[6] David Wecker, Bela Bauer, Bryan K. Clark, Matthew B. Hastings, and Matthias Troyer. Gate-count estimates for performing quantum chemistry on small quantum computers. *Physical Review A*, 90:022305, 2014.

[7] Matthew B. Hastings, Dave Wecker, Bela Bauer, and Matthias Troyer. Improving Quantum Algorithms for Quantum Chemistry. *Quantum Information & Computation*, 15(1-2):1–21, 2015.

[8] David Poulin, M. B. Hastings, Dave Wecker, Nathan Wiebe, Andrew C. Doherty, and Matthias Troyer. The Trotter Step Size Required for Accurate Quantum Simulation of Quantum Chemistry. *Quantum Information & Computation*, 15(5-6):361–384, 2015.

[9] Jarrod R. McClean, Ryan Babbush, Peter J. Love, and Alán Aspuru-Guzik. Exploiting locality in quantum computation for quantum chemistry. *The Journal of Physical Chemistry Letters*, 5(24):4368–4380, 2014.

[10] Ryan Babbush, Jarrod McClean, Dave Wecker, Alán Aspuru-Guzik, and Nathan Wiebe. Chemical basis of Trotter-Suzuki errors in quantum chemistry simulation. *Physical Review A*, 91(2):022311, February 2015.

[11] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5(4213):1–7, 2014.

[12] D. Wecker, M. B. Hastings, and M. Troyer. Towards Practical Quantum Variational Algorithms. *e-print arXiv: 1507.08969*, 2015.

[13] Colin J. Trout and Kenneth R. Brown. Magic state distillation and gate compilation in quantum algorithms for quantum chemistry. *International Journal of Quantum Chemistry*, 115(19):1296–1304, 2015.

[14] Dave Wecker, Matthew B. Hastings, Nathan Wiebe, Bryan K. Clark, Chetan Nayak, and Matthias Troyer. Solving strongly correlated electron models on a quantum computer. *e-print arXiv: 1506.05135*, June 2015.

[15] Leonie Mueck. Quantum reform. *Nature Chemistry*, 7(5):361–363, 2015.

[16] Dominic W. Berry, Graeme Ahokas, Richard Cleve, and Barry C. Sanders. Efficient Quantum Algorithms for Simulating Sparse Hamiltonians. *Communications in Mathematical Physics*, 270(2):359–371, December 2006.

[17] Nathan Wiebe, Dominic W Berry, Peter Hoyer, and Barry C Sanders. Simulating quantum dynamics on a quantum computer. *Journal of Physics A: Mathematical and Theoretical*, 44:445308, November 2011.

[18] Dominic W. Berry and Andrew M. Childs. Black-box hamiltonian simulation and unitary implementation. *Quantum Information & Computation*, 12(1-2):29–62, January 2012.

[19] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Exponential improvement in precision for simulating sparse hamiltonians. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 283–292, New York, NY, USA, 2014. ACM.

[20] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. *Physical Review Letters*, 114(9):090502, 2015.

[21] Dominic W. Berry, Andrew M. Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. *e-print arXiv: 1501.01715*, 2015.

[22] P. Jordan and E. Wigner. über das paulische äquivalenzverbot. *Zeitschrift für Phys.*, 47(9-10):631–651, 1928.

[23] R. D. Somma, G. Ortiz, J.E. Gubernatis, E. Knill, and R. Laflamme. Simulating physical phenomena by quantum networks. *Physical Review A*, 65(4):17, 2002.

[24] Borzu Toloui and Peter J. Love. Quantum Algorithms for Quantum Chemistry based on the sparsity of the CI-matrix. *e-print arXiv: 1312.2579*, 2013.

Perfect commuting-operator strategies for linear system games

Richard Cleve[1 2] Li Liu[1 2] William Slofstra[1]

[1] *Institute for Quantum Computing, University of Waterloo, Canada*
[2] *School of Computer Science, University of Waterloo, Canada*

Mermin [8] implicitly considers a non-local game that is sometimes called the *magic square game* (see also [11, 9, 1, 4]). This game is based around a system of linear equations over $\mathbb{Z}_2$ with nine variables and six equations. Generalizing the magic square game, Cleve and Mittal [3] investigate a class of games based on binary linear systems of the form $Mx = b$, where $M \in \mathbb{Z}_2^{m\times n}$ and $b \in \mathbb{Z}_2^m$. The non-local game associated with a binary linear system is:

Definition 1 *Let $Mx = b$ be a binary linear system, so $M \in \mathbb{Z}_2^{m\times n}$ and $b \in \mathbb{Z}_2^m$. In the associated linear system game, Alice receives as input $s \in \{1, \ldots, m\}$, and Bob receives $t \in \{1, \ldots, n\}$, where $M_{s,t} = 1$. Alice outputs an assignment to the variables in equation s, and Bob outputs a bit. Alice and Bob win if Alice's assignment satisfies equation s and Alice's assignment to variable x_t is the same as Bob's output bit.*

A *classical strategy* is one where Alice and Bob do not share entanglement. It can be shown that $Mx = b$ has a perfect classical strategy (i.e., a strategy with success probability 1) if and only if the system of equations has a solution. An entangled quantum strategy is a strategy in which Alice and Bob share an entangled quantum state $|\psi\rangle$. In the tensor-product model, $|\psi\rangle$ is a bipartite state in a tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$, and Alice and Bob's measurements of this state are modeled as observables on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively.

It is shown in [3] that a binary linear system game has a perfect entangled strategy in the tensor-product model if and only if the linear system has a finite-dimensional operator solution in the following sense. We first express our linear systems in a multiplicative notation, so a vector $x \in \{\pm 1\}^n$ satisfies equation ℓ if and only if

$$x_{k_1} x_{k_2} \ldots x_{k_r} = (-1)^{b_\ell},$$

where $V_\ell = \{k_1, k_2, \ldots, k_r\} = \{1 \le k \le n : M_{\ell,k} = 1\}$ is the set of indices of variables in equation ℓ. Next, we extend the binary variables (the x_i's) to binary observables as:

Definition 2 (Operator solution) *An* operator solution *to a binary linear system $Mx = b$ is a sequence of bounded self-adjoint operators $A_1, \ldots, A_n$ on a Hilbert space $\mathcal{H}$ such that:*

(a) $A_i^2 = \mathbb{1}$ (that is, A_i is a binary observable) for all $1 \le i \le n$.

(b) If x_i and x_j appear in the same equation (i.e., $i, j \in V_\ell$ for some $1 \le \ell \le m$) then A_i and A_j commute (we call this local compatibility*).*

(c) For each equation of the form $x_{k_1} x_{k_2} \ldots x_{k_r} = (-1)^{b_l}$, the observables satisfy

$$A_{k_1} A_{k_2} \cdots A_{k_r} = (-1)^{b_\ell} \mathbb{1}$$

(we call this constraint satisfaction*).*

A finite dimensional operator solution *to a binary linear system $Mx = b$ is an operator solution in which the Hilbert space $\mathcal{H}$ is finite dimensional.*

The term "local compatibility" comes from quantum mechanics, where two observables commute if and only if they are compatible in the sense that they represent quantities which can be measured (or known) simultaneously. It is noteworthy that the result of [3] applies even when the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are allowed to be infinite dimensional; in this case, the operator solutions will still be finite dimensional.

In this paper we are interested in the *commuting operator model* for entanglement, in which $|\psi\rangle$ belongs to a joint Hilbert space $\mathcal{H}$, and Alice and Bob's measurements are modeled as observables on $\mathcal{H}$ with the property that Alice's observables commute with Bob's observables. This model—which clearly subsumes the tensor-product model—is used in algebraic quantum field theory. For any non-local game, a finite-dimensional strategy in the commuting-operator model can be converted into a strategy in the tensor product model, but the precise relationship between the tensor-product model and the commuting-operator model is unknown in general. We refer to [13, 12, 7, 5] for more discussion.

The main result of our paper is that a binary linear system game has a perfect entangled strategy in the commuting operator model if and only if the linear system has a (possibly-infinite-dimensional) operator solution. Our result relies on a useful characterization of the relations in Definition 2 using finitely-presented groups, which we call the *solution group*.

Definition 3 (Solution group) *The* solution group *of a binary linear system $Mx = b$ is the group Γ generated by $g_1, \ldots, g_n$ and J satisfying the following relations (where e is the group identity, and $[a, b] = aba^{-1}b^{-1}$ is the group commutator):*

(a) $g_i^2 = e$ *for all* $1 \leq i \leq n$, *and* $J^2 = e$ *(generators are involutions).*

(b) $[g_i, J] = e$ *for all* $1 \leq i \leq n$ *(*J *commutes with each generator).*

(c) *If* x_i *and* x_j *appear in the same equation (i.e.,* $i, j \in V_\ell$ *for some* ℓ*) then* $[g_i, g_j] = e$ *(local compatibility).*

(d) $g_1^{M_{\ell 1}} g_2^{M_{\ell 2}} \cdots g_n^{M_{\ell n}} = J^{b_\ell}$ *for all* $1 \leq \ell \leq m$ *(constraint satisfaction).*

The new variable J acts as the scalar -1 in an operator solution. In fact, an operator solution is a representation of the solution group with $J = -\mathbb{1}$.

Now we are ready to give the full statement of our main theorem.

Theorem 4 *Let* $Mx = b$ *be a binary linear system. The following statements are equivalent:*

1. *There is a perfect commuting-operator strategy for the non-local game associated to* $Mx = b$.
2. *There is an operator solution for* $Mx = b$ *(possibly on an infinite-dimensional Hilbert space).*
3. *The solution group for* $Mx = b$ *has the property that* $J \neq e$.

As is typical with results of this type (compare for instance [10, Proposition 5.11]), the main difficulty in the proof arises in showing that an operator solution can be turned into a perfect strategy. In particular, an operator solution does not come with an entangled state. By considering the solution group Γ, we construct a tracial state on the group algebra of Γ to use as our entangled state. In addition, the solution group captures some interesting properties of the linear system games, which we discuss shortly.

We do not know of any computational procedure which can determine if a binary linear system has a perfect entangled strategy. Arkhipov showed that, in the special case where each variable appears in exactly two constraints, there is a polynomial-time algorithm to determine if a perfect entangled strategy exists [2] (in this case, a game has a perfect commuting-operator strategy if and only if it has a perfect tensor-product strategy). For the general case, we can attempt to use the characterization of perfect strategies in [3] by searching for operator solutions over $\mathbb{C}^d$, $d \in \mathbb{N}$. It is decidable to determine if there is an operator solution over $\mathbb{C}^d$ for fixed d, and thus this naive procedure is guaranteed to find a perfect strategy if one exists. However, if a perfect strategy does not exist, then the naive procedure does not halt. We note that, for arbitrarily large d, Ji gives examples of binary linear systems which have finite-dimensional operator solutions, but for which the solutions require dimension at least d [6].

In contrast, there is no apparent way to search through operator solutions over infinite-dimensional Hilbert spaces. What we can do instead is try to show that $J = e$ in the group Γ by searching through products of the defining relations. Using our characterization, we see that this procedure will halt if and only if the linear system game does not have a perfect strategy in the commuting-operator model. Thus this problem would be decidable if the tensor-product model and commuting-operator model were equivalent. Determining whether or not these two models are equivalent is a well-known open problem due to Tsirelson [13].

A final comment is that our results easily generalize to linear systems over $\mathbb{Z}_p$.

References

[1] P. K. Aravind, *Quantum mysteries revisited again*, American Journal of Physics **72** (2004), 1303–1307.

[2] A. Arkhipov, *Extending and characterizing quantum magic games*, arXiv:1209.3819 (2012).

[3] R. Cleve and R. Mittal, *Characterization of binary constraint system games*, Proceedings of the 41st International Colloquium on Automata, Languages, and Programming (ICALP), 2012, pp. 320–331.

[4] R. Cleve, P. Høyer, B. Toner, and J. Watrous., *Consequences and limits of nonlocal strategies*, Proceedings of the 19th IEEE Conference on Computational Complexity (CCC), 2004, pp. 236–249.

[5] T. Fritz, *Tsirelson's problem and Kirchberg's conjecture*, Reviews in Mathematical Physics **24** (2012), no. 5, 1250012.

[6] Z. Ji, *Binary constraint system games and locally commutative reductions*, arXiv:1310.3794 (2013).

[7] Marius Junge, Miguel Navascues, Carlos Palazuelos, D Perez-Garcia, Volkher B Scholz, and Reinhard F Werner, *Connes' embedding problem and Tsirelson's problem*, Journal of Mathematical Physics **52** (2011), no. 1, 012102.

[8] N. D. Mermin, *Simple unified form for the major no-hidden-variables theorems*, Physical Review Letters **65** (1990), no. 27, 3373–3376.

[9] ———, *Hidden variables and the two theorems of John Bell*, Reviews of Modern Physics **65** (1993), no. 3, 803–815.

[10] V. I. Paulsen, S. Severini, D. Stahlke, I. G. Todorov, and A. Winter, *Estimating quantum chromatic numbers*, 2014, Manuscript available at arXiv1407.6918.

[11] A. Peres, *Incompatible results of quantum measurements*, Physics Letters A **151** (1990), no. 3,4, 107–108.

[12] Volkher B. Scholz and Reinhard F. Werner, *Tsirelson's problem*, arXiv preprint arXiv:0812.4305 (2008).

[13] B. S. Tsirelson, *Some results and problems on quantum Bell-type inequalities*, Hadronic Journal Supplement **8** (1993), 329–345.

A Four-Round LOCC Protocol Outperforms All Two-Round Protocols in Reducing the Entanglement Cost for A Distributed Quantum Information Processing

Eyuri Wakakuwa[1] * Akihito Soeda[2] Mio Murao[2 3]

[1] *Graduate School of Information Systems, The University of Electro-Communications, Japan*
[2] *Department of Physics, Graduate School of Science, The University of Tokyo, Japan*
[3] *Institute for Nano Quantum Information Electronics, The University of Tokyo, Japan*

Abstract. We prove that there is a trade-off relation between the entanglement cost and the number of rounds of communication, for two distant parties to accomplish a bidirectional quantum information task by local operations and classical communication (LOCC). We consider an implementation of a class of two-qubit controlled-unitary gate by LOCC assisted by shared entanglement, in an information theoretical scenario of asymptotically many input pairs and vanishingly small error. We prove the trade-off relation by showing that one ebit of entanglement per pair is necessary to be consumed for implementing the unitary by any two-round protocol, whereas the entanglement cost by a four-round protocol is strictly smaller than one ebit per pair.

Keywords: LOCC protocols, number of rounds, entanglement

1 Introduction

When two distant parties collaborate to perform a distributed quantum information processing, it is necessary to communicate some information with each other. If the communication is restricted to be transmission of classical bits, it may also be necessary to make use of some entanglement shared in advance, depending on the task. Entanglement and classical communication are thus regarded as resources for distributed quantum information processing, and minimizing the cost of those resources has been one of the central issues in quantum information theory.

A relatively unexplored question about distributed quantum information processing is how the performance of a protocol to accomplish a task depends on the number of rounds of communication in the protocol [1]. It has been known that the performance of a protocol with more than one round of communication is strictly better than that of any protocol with only one round of communication, for several tasks such as entanglement distillation [2], quantum key distribution [3], state discrimination [4–6] and hypothesis testing [7–9]. However, few example of tasks is known for which an r'-round protocol outperforms any r-round protocol and $2 \leq r < r'$, with the exception of the result of [5]. Moreover, to our knowledge, it is not known whether there exists a trade-off relation between the entanglement cost and the number of rounds of a protocol for a "genuinely bidirectional" task, which cannot be accomplished by any protocol with only one round of communication.

In this contribution, we investigate implementation of a bipartite unitary gate by LOCC (local operations and classical communication) assisted by shared entanglement, in an information theoretical scenario introduced in [10]. We prove that, for a class of two-qubit controlled-unitary gates, a four-round protocol outperforms all two-round protocols in reducing the entanglement cost. Thus we provide a first example of genuinely bidirectional tasks for which there is a trade-off relation between the entanglement cost and the number of rounds of communication. It is different from the trade-off relation between the entanglement cost and the *classical communication cost*, which exists, e.g., for remote state preparation [11–14].

Notations. $|\Phi_d\rangle$, $|\Phi_{K_n}\rangle$ and $|\Phi_{L_n}\rangle$ represent the maximally entangled state with the Schmidt rank d, K_n and L_n, respectively. π_d is the maximally mixed state of rank d. The fidelity and the trace distance between two quantum states ρ and σ are defined as $F(\rho,\sigma) := (\mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}])^2$ and $\|\rho-\sigma\|_1 := \mathrm{Tr}[\sqrt{(\rho-\sigma)^2}]$, respectively. We abbreviate $F(\rho,|\psi\rangle\langle\psi|)$ as $F(\rho,|\psi\rangle)$. For a quantum operation $\mathcal{E}$, we abbreviate $\mathcal{E}(|\psi\rangle\langle\psi|)$ as $\mathcal{E}(|\psi\rangle)$.

2 Definitions

In this section, we describe a task that we analyze in this contribution, and present a definition of a trade-off relation between the entanglement cost and the number of rounds.

Suppose Alice and Bob are given a sequence of bipartite quantum states $|\psi_{i_1}\rangle^{AB}\cdots|\psi_{i_n}\rangle^{AB}$, generated by an i.i.d. quantum information source of an ensemble $\{p_i,\psi_i\}_i$. We assume that the source is completely mixed, i.e., $\sum_i p_i|\psi_i\rangle\langle\psi_i|^{AB} = \pi_d^A\otimes\pi_d^B$. Alice and Bob perform the same bipartite unitary U^{AB} on each of $|\psi_{i_1}\rangle^{AB},\cdots,|\psi_{i_n}\rangle^{AB}$ by LOCC using a resource state $\Phi_{K_n}^{A_0B_0}$, where K_n is a natural number, in such a way that the average error vanishes in the limit of $n\to\infty$. Following the formulation of the Schumacher compression [15], we assume that Alice and Bob do not know $\{p_i,\psi_i\}_i$, but know that the average state is completely mixed.

Equivalently, we consider a task in which Alice and Bob apply $(U^{AB})^{\otimes n}$ on $(|\Phi_d\rangle^{AR_A}|\Phi_d\rangle^{BR_B})^{\otimes n}$ by LOCC using a resource state $\Phi_{K_n}^{A_0B_0}$. Here, R_A and R_B are imaginary reference systems that are inaccessible to Alice and

*wakakuwa@quest.is.uec.ac.jp

Bob. Rigorous definitions are given below.

Definition 1 *(Definition 1 in [10]) Let U be a bipartite unitary acting on two d-dimensional quantum systems A and B. Let Alice and Bob have quantum registers $\{A_0, A_1\}$ and $\{B_0, B_1\}$, respectively, and let $\mathcal{M}_n$ be a quantum operation from $A^n A_0 \otimes B^n B_0$ to $A^n A_1 \otimes B^n B_1$. $\mathcal{M}_n$ is called an (r, n, ϵ)-protocol for implementing U if $\mathcal{M}_n$ is an r-round LOCC that satisfies*

$$F(\rho(\mathcal{M}_n), |\Psi_U\rangle^{\otimes n} |\Phi_{L_n}\rangle^{A_1 B_1}) \geq 1 - \epsilon,$$

where $|\Psi_U\rangle := U^{AB} |\Phi_d\rangle^{AR_A} |\Phi_d\rangle^{BR_B}$ and

$$\rho(\mathcal{M}_n) := \mathcal{M}_n(|\Phi_d^{AR_A}\rangle^{\otimes n} |\Phi_d^{BR_B}\rangle^{\otimes n} |\Phi_{K_n}\rangle^{A_0 B_0}).$$

The entanglement cost of $\mathcal{M}_n$ is defined by $\log K_n - \log L_n$.

Definition 2 *A rate E is said to be achievable by an r-round protocol for implementing U if, for any $\epsilon > 0$, there exists n_ϵ such that for any $n \geq n_\epsilon$, we find an (r, n, ϵ)-protocol for implementing U with the entanglement cost nE. For a technical reason, we additionally require that*

$$\lim_{\epsilon \to 0} \epsilon \cdot n_\epsilon^4 = 0.$$

The entanglement cost of U by r-round protocols is defined as

$$E_r(U) := \inf\{E \mid E \text{ is achievable by an } r\text{-round protocol for implementing } U\}.$$

The main focus of this contribution is whether there is a trade-off relation between the entanglement cost and the number of rounds for implementing a bipartite unitary. In considering "trade-off relation", we compare the entanglement cost of a unitary by r-round protocols and that by r'-round protocol ($r < r'$). If the latter is strictly smaller than the former, we could say that there exists a trade-off relation between the entanglement cost and the number of rounds. A rigorous definition is as follows:

Definition 3 *There exists a trade-off relation between the entanglement cost and the number of rounds for implementing U if there exists $r, r' \in \mathbb{N}$ such that*

$$r < r', \ E_r(U) > E_{r'}(U).$$

3 Result and Proof

We consider a class of two-qubit controlled-phase gate, which takes the form of

$$U_\theta^{AB} = |0\rangle\langle 0|^A \otimes I^B + |1\rangle\langle 1|^A \otimes (e^{i\theta\sigma_z})^B$$

where

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ 0 < \theta \leq \frac{\pi}{2}.$$

The main result of this contribution is as follows:

Theorem 4 *There exists a trade-off relation between the entanglement cost and the number of rounds for implementing U_θ for any $\theta \in (0, \theta_{\max}]$, where $\theta_{\max} \in (0, \pi/2]$ is a constant.*

We prove Theorem 4 by showing that the following relations hold for any $\theta \in (0, \theta_{\max}]$:

$$E_2(U_\theta) \geq 1, \quad E_4(U_\theta) < 1.$$

The first inequality is proved in [10] (see the converse part of Theorem 25 therein). A proof of the second inequality is presented in the technical version of this manuscript, in which we also derive a stronger relation that $\lim_{\theta \to 0} E_4(U_\theta) = 0$.

4 Conclusion

We considered implementation of a class of two-qubit controlled-unitary gate by local operations and classical communication (LOCC), assisted by shared entanglement. We proved that a four-round protocol outperforms all two-round LOCC protocols in reducing the entanglement cost. Our result provides a first example of genuinely bidirectional distributed quantum tasks, for which there exists a trade-off relation between the entanglement cost and the number of rounds of communication.

Acknowledgements

This work is supported by the Project for Developing Innovation Systems of MEXT, Japan and JSPS KAKENHI (Grant No. 23540463, No. 23240001, No. 26330006, and No. 15H01677). We also gratefully acknowledge to the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas MEXT KAKENHI (Grant No. 24106009)) for encouraging the research presented in this contribution.

References

[1] E. Chitambar et al. *Comm. Math. Phys.*, Vol. 328, pp. 303–326, 2014.

[2] C. H. Bennett et al. *Phys. Rev. A*, Vol. 54, p. 3824, 1996.

[3] D. Gottesman et al. *IEEE Trans. Inf. Theory*, Vol. 49, p. 457, 2003.

[4] S. M. Cohen. *Phys. Rev. A*, Vol. 75, p. 052313, 2007.

[5] Y. Xin et al. *Phys. Rev. A*, Vol. 77, p. 012315, 2008.

[6] M. Owari et al. *New J. of Phys.*, Vol. 10, p. 013006, 2008.

[7] M. Owari et al. *IEEE Trans. Inf. Theory*, Vol. 61, pp. 6995–7011, 2010.

[8] M. Owari et al. *Phys. Rev. A*, Vol. 90, p. 032327, 2014.

[9] M. Owari et al. e-print arXiv:1409.3897v3.

[10] E. Wakakuwa et al. e-print arXiv:1505.04352v2.

[11] C. H. Bennett et al. *IEEE Trans. Inf. Theory*, Vol. 51, p. 56, 2005.

[12] A. Abeyesinghe et al. *Phys. Rev. A*, Vol. 68, p. 062319, 2003.

[13] C. H. Bennett et al. *Phys. Rev. Lett.*, Vol. 87, p. 077902, 2001.

[14] I. Devetak et al. *Phys. Rev. Lett.*, Vol. 87, p. 197901, 2001.

[15] B. Schumacher. Quantum coding. *Phys. Rev. A*, Vol. 51, p. 2738, 1995.

Universal Quantum Emulator

Iman Marvian[1] * Seth Lloyd[1 2] †

[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139*
[2] *Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139*

Abstract. We propose a quantum algorithm that emulates the action of an unknown unitary transformation on a given input state, using multiple copies of some unknown sample input states of the unitary and their corresponding output states. The algorithm does not assume any prior information about the unitary to be emulated, or the sample input states. Remarkably, the runtime of the algorithm is logarithmic in D, the dimension of the Hilbert space, and increases polynomially with d, the dimension of the subspace spanned by the sample input states. Furthermore, the sample complexity of the algorithm, i.e. the total number of copies of the sample input-output pairs needed to run the algorithm, is independent of D, and polynomial in d.

Keywords: Quantum algorithm, Quantum simulation, Tomography

In this paper we introduce a quantum algorithm that emulates the action of an unknown unitary transformation on new given input states. The algorithm couples the new input state to multiple copies of some unknown *sample input-output pairs*, that is copies of some input states of the unitary as well as copies of the corresponding output states. We do not assume any prior information about the unitary to be emulated, or the given sample input states. The algorithm emulates the action of the unitary on any given state in the subspace spanned by the previously given input states, which could be much smaller than the system Hilbert space. Indeed, we are interested in the cases where d, the dimension of this subspace is constant or, at most, polylogarithmic in D, the dimension of the system Hilbert space.

Obviously, having multiple copies of sample input-output pairs we can perform measurements on them, and using state tomography find an approximate classical description of these states in a standard basis. This, in turn, yields the classical description of the unknown unitary transformation, which then can be used to simulate its action on the new given states. This approach, however, is highly inefficient and impractical: First of all, state tomography in a large Hilbert space is a hard task and requires lots of copies of the sample states. Second, even if we find the classical description of the unitary transformation, in general, this unitary cannot be implemented efficiently.

More precisely, the approaches based on tomography run in time $\Omega(D)$ and need $\Omega(D)$ copies of state, where D is the dimension of the system Hilbert space. In contrast, the runtime of the algorithm proposed in this work is $\mathcal{O}(\log D)$ and polynomial in d, and its *sample complexity*, i.e. the total number of copies of the sample input-output pairs that are needed to run the algorithm, is independent of D and polynomial in d. Therefore, our algorithm is not only exponentially faster than the approaches based on tomography, its sample complexity is also dramatically lower.

*marvian@mit.edu
†slloyd@mit.edu

1 Preliminaries

Here we present the algorithm for the special case of pure sample states. In the paper we explain how the algorithm can be generalized to the case of mixed states as well.

Let $S_{\text{in}} = \{|\phi_k^{\text{in}}\rangle\langle\phi_k^{\text{in}}| : k = 1, \cdots, K\}$ be a set of sample input states of the unitary U and $S_{\text{out}} = \{|\phi_k^{\text{out}}\rangle\langle\phi_k^{\text{out}}| = U|\phi_k^{\text{in}}\rangle\langle\phi_k^{\text{in}}|U^\dagger : k = 1, \cdots, K\}$ be the corresponding outputs. Let $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ be the subspaces spanned by $\{|\phi_k^{\text{in}}\rangle : k = 1, \cdots, K\}$ and $\{|\phi_k^{\text{out}}\rangle : k = 1, \cdots, K\}$ respectively, and d be the dimension of these subspaces. We assume the set of input samples S_{in} contains sufficient number of different states to uniquely determine the action of U on the subspace $\mathcal{H}_{\text{in}}$ (up to a global phase). It can be easily shown that having the classical description of the input and output states in S_{in} and S_{out} we can uniquely determine the action of U on any input state $|\psi\rangle \in \mathcal{H}_{\text{in}}$ (up to a global phase), if and only if the matrix algebra generated by S_{in}, that is the set of polynomials in the elements of S_{in}, is the full matrix algebra on $\mathcal{H}_{\text{in}}$, i.e. contains all operators with supports contained in $\mathcal{H}_{\text{in}}$. Therefore, in the following we naturally assume this assumption is satisfied. Furthermore, we assume K the number of different sample input states in S_{in} is poly(d).

To implement the algorithm, we need multiple copies of each sample state in S_{in} and S_{out}. Interestingly, at the end of the algorithm most of these states remain almost unaffected. Indeed, the main use of the given copies of sample states is to simulate *controlled-reflections* about these states.

Let $R^{\text{in}}(k) = e^{i\pi|\phi_k^{\text{in}}\rangle\langle\phi_k^{\text{in}}|}$ and $R^{\text{out}}(k) = e^{i\pi|\phi_k^{\text{out}}\rangle\langle\phi_k^{\text{out}}|}$ be the reflections about the input and output states $|\phi_k^{\text{in}}\rangle$ and $|\phi_k^{\text{out}}\rangle$, respectively. In the proposed algorithm we need to implement the controlled-reflections $R_a^{\text{in}}(k)$ and $R_a^{\text{out}}(k)$, defined as

$$R_a(k) = |0\rangle\langle 0|_a \otimes I + |1\rangle\langle 1|_a \otimes e^{i\pi|\phi_k\rangle\langle\phi_k|} \ , \qquad (1)$$

where a is the label for the control qubit, and I is the identity operator on the main system. Note that we have suppressed the superscripts *in* and *out* in both sides.

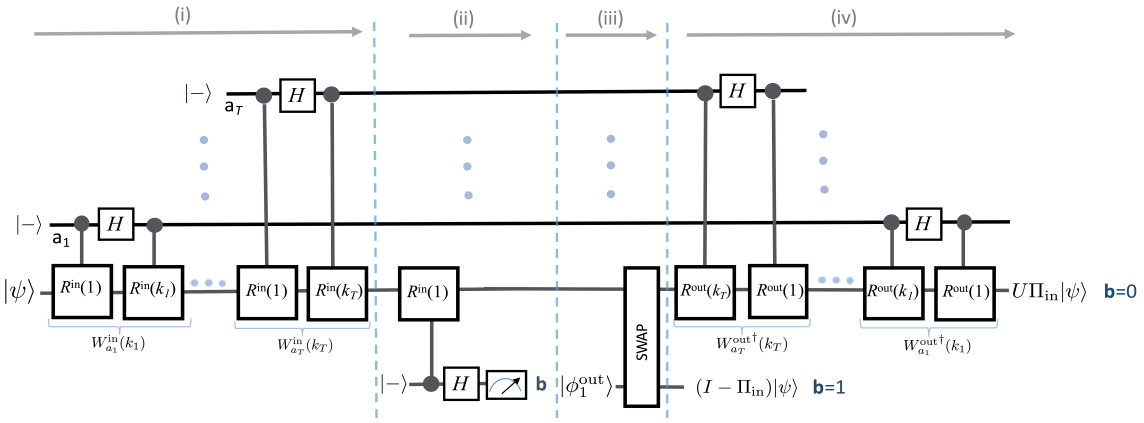


Figure 1: The quantum circuit for emulating unitary transformation U for the special case of pure input-output sample pairs. Here $k_1, \cdots, k_T$ are $T = \text{poly}(d)$ integers chosen uniformly at random from integers $1, \cdots, K$. We use the given copies of sample states in S_{in} and S_{out} to simulate the controlled-reflections $R_a^{\text{in}}(k)$ and $R_a^{\text{out}}(k)$, respectively. A modified version of this circuit can be implemented using only $\mathcal{O}(\log T)$ ancillary qubits (instead of T qubits).

Using the given copies of the sample states, we can efficiently simulate these controlled-reflections via the *density matrix exponentiation* technique of Ref.[1]. It turns out that using n copies of state σ one can simulate the unitary $e^{-it\sigma}$, or its controlled version $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{-it\sigma}$, for any real t, with error $\epsilon = \mathcal{O}(t^2/n)$, and in time $\mathcal{O}(n \times \log(D))$, where D is the dimension of the Hilbert space. In the simplest case where the system is a qubit ($D = 2$), this technique is basically simulating the Heisenberg interaction between the system and each given copy of state σ.

Therefore, in the following, where we present the algorithm, we assume all the controlled-reflections $\{R_a(k) : 1 \leq k \leq K\}$ can be efficiently implemented.

To simplify the presentation, we use the notation $W_a(k) \equiv R_a(k) H_a R_a(1)$, where again we have suppressed *in* and *out* superscripts in both sides. Here H_a denotes the Hadamard gate H acting on qubit a, where $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The algorithm also uses a SWAP gate defined by $\text{SWAP}|\nu\rangle|\mu\rangle = |\mu\rangle|\nu\rangle$, for any pair of states $|\mu\rangle$ and $|\nu\rangle$.

2 The algorithm (Special case)

In this section we present the algorithm for the universal quantum emulator, in the special case where all the sample input-output pairs are pure states. In the paper we present several generalizations of this algorithm, including to the case where the given samples contain mixed states. Also, we present a modified version of this circuit which realizes this algorithm with exponentially less ancillary qubits.

Fig.(1) exhibits the quantum circuit that emulates the action of an unknown unitary transformation U on any given state $|\psi\rangle$ in the input subspace $\mathcal{H}_{\text{in}}$. For a general input state, which is not restricted to this subspace, this circuit first projects the state to this subspace, and if successful, then applies the unitary U to it.

In this algorithm $(k_1, \cdots, k_T)$ are T integers chosen uniformly at random from integers $1, \cdots, K$, where T is a constant that determines the precision of emulation, and we choose it to be polynomial in d, and independent of D. Furthermore, state $|\phi_1^{\text{in}}\rangle$ (and $|\phi_1^{\text{out}}\rangle$) is one of the sample input states (and its corresponding output) which is chosen randomly at the beginning of the algorithm, and is fixed during the algorithm. In steps (i) and (iv) of the algorithm we implement, respectively, the unitaries $W_{a_i}^{\text{in}}(k_i)$ and $W_{a_i}^{\text{out}\,\dagger}(k_i)$ on the system and qubit a_i, for $i = 1, \cdots, T$. As we explained before, all the conditional reflections $R_a^{\text{in}}(k)$ and $R_a^{\text{out}}(k)$ can be efficiently simulated using the given copies of states $|\phi_k^{\text{in}}\rangle$ and $|\phi_k^{\text{out}}\rangle$.

In step (ii) of the algorithm we perform a qubit measurement in the computational basis $\{|0\rangle, |1\rangle\}$. Then, after the measurement with probability $1 - \langle\psi|\Pi_{\text{in}}|\psi\rangle$ we get outcome $b = 1$, in which case we project the system to a state close to $(I - \Pi_{\text{in}})|\psi\rangle/\sqrt{1 - \langle\psi|\Pi_{\text{in}}|\psi\rangle}$, where Π_{in} is the projector to the subspace $\mathcal{H}_{\text{in}}$. On the other hand, with probability $\langle\psi|\Pi_{\text{in}}|\psi\rangle$ we get the outcome $b = 0$, in which case the final state of circuit is close to $U\Pi_{\text{in}}|\psi\rangle/\sqrt{\langle\psi|\Pi_{\text{in}}|\psi\rangle}$. In this case the algorithm consumes a copy of state $|\phi_1^{\text{out}}\rangle$, and returns a copy of state $|\phi_1^{\text{in}}\rangle$.

Note that, although the algorithm uses random integers $(k_1, \cdots, k_T)$, for sufficiently large T it *always* transforms the input state $|\psi\rangle \in \mathcal{H}_{\text{in}}$ to a state with high fidelity with the desired output state $U|\psi\rangle$.

References

[1] S. Lloyd, M. Mohseni, and P. Rebentrost. Quantum principal component analysis In *Nature Physics*, 10:631–633, 2014.

Characterizing Supremacy in Near Term Quantum Devices

Sergio Boixo[1] * Sergei Isakov[1] Vadim Smelyanskiy[1] † Ryan Babbush[1] ‡
Ding Nan[1] Zhang Jiang[2] John Martinis[1] Hartmut Neven[1]

[1] *Google, Venice, CA 90291, USA*
[2] *Quantum A. I. Lab, NASA Ames Research Center, Moffett Field, CA 94035, USA*

Abstract. A critical question for the field of quantum computing in the near future is whether quantum devices without error correction can perform a well-defined computational task beyond the capabilities of state-of-the-art classical computers, achieving so-called quantum supremacy. We study the computational task of sampling from the output distribution of random quantum circuits. We introduce the cross entropy difference as a useful benchmark of random quantum circuits which approximates the circuit fidelity. We show that the cross entropy can be efficiently measured when circuit simulations are available. Beyond the classically tractable regime, the cross entropy can be extrapolated and compared with theoretical estimates to define a practical quantum supremacy demonstration. We conclude that quantum supremacy can be achieved in the near-term with approximately fifty qubits.

Keywords: quantum supremacy, quantum chaos, device characterization, quantum complexity theory

This work proposes a minimal resource demonstration of quantum supremacy based on the implementation of random quantum circuits. Random quantum circuits are known examples of quantum chaotic evolutions [1, 2, 5–8]. A signature of chaos is that small changes in model specification or numerical errors lead to large divergences in system trajectories. In quantum chaotic dynamics this sensitivity manifests itself as a loss of fidelity $|\langle\psi_t|\psi_t^\epsilon\rangle|^2$ of a quantum state $|\psi_t\rangle$ which decreases exponentially in the evolution time t and in the magnitude of a small perturbation ϵ to the Hamiltonian that evolves $|\psi_t\rangle$.

With realistic superconducting hardware constraints [3], gates act in parallel on distinct sets of $n = \log N$ qubits restricted to a planar lattice. In a random quantum circuit, gates are sampled from a universal set. The cycle number t plays the role of time in the chaotic dynamics of the quantum state $|\psi_t\rangle$. The real and imaginary parts of the amplitudes $\langle x_j|\psi_t\rangle$ in any local basis $\{x_j\}_{j=1}^N$ are approximately uniformly distributed in a $2N$ dimensional sphere subject to normalization. This implies that their distribution is an unbiased Gaussian with variance $\propto 1/N$, up to finite moments. The distribution of probabilities $|\langle x_j|\psi_t\rangle|^2$ approaches the form Ne^{-pN}, known as the Porter-Thomas distribution [11].

Consider a sample $S = \{x_1, \ldots, x_m\}$ of bit-strings x_j obtained from m global measurements of every qubit in the computational basis $\{|x_j\rangle\}$ (or any other basis obtained from local operations). The joint probability of the set of outcomes S is $\Pr_U(S) = \prod_{x_j\in S} p_U(x_j)$ where $p_U(x) \equiv |\langle x|\psi\rangle|^2$. For a typical sample S, the central limit theorem implies that

$$\begin{aligned}\log \Pr_U(S) &= \sum_{x_j\in S} \log p_U(x_j) \\ &= -m\,\mathrm{H}(p_U) + O(m^{1/2})\,, \end{aligned} \tag{1}$$

where $\mathrm{H}(p_U) \equiv -\sum_{j=1}^N p_U(x_j)\log p_U(x_j)$ is the entropy of the output of U. Because $p_U(x)$ are *i.i.d.* distributed according to the Porter-Thomas distribution,

$$\begin{aligned}\mathrm{H}(p_U) &= -\int_0^\infty pN^2e^{-Np}\log p\,dp \\ &= \log N - 1 + \gamma\,, \end{aligned} \tag{2}$$

where $\gamma \approx 0.577$ is the Euler constant.

Let $A_{\mathrm{pcl}}(U)$ be a classical algorithm with computational time cost *polynomial* in n that takes a specification of the random circuit U as input and outputs a bit-string x with probability distribution $p_{\mathrm{pcl}}(x|U)$. Consider a typical sample $S_{\mathrm{pcl}} = \{x_1^{\mathrm{pcl}}, \ldots, x_m^{\mathrm{pcl}}\}$ obtained from $A_{\mathrm{pcl}}(U)$. We now focus on the probability $\Pr_U(S_{\mathrm{pcl}}) = \prod_{x_j^{\mathrm{pcl}}\in S_{\mathrm{pcl}}} p_U(x_j^{\mathrm{pcl}})$ that this sample S_{pcl} is observed from the output $|\psi\rangle$ of the circuit U. The central limit theorem implies that

$$\log \Pr_U(S_{\mathrm{pcl}}) = -m\,\mathrm{H}(p_{\mathrm{pcl}}, p_U) + O(m^{1/2})\,, \tag{3}$$

where

$$\mathrm{H}(p_{\mathrm{pcl}}, p_U) \equiv -\sum_{j=1}^N p_{\mathrm{pcl}}(x_j|U)\log p_U(x_j) \tag{4}$$

is the cross entropy between $p_{\mathrm{pcl}}(x|U)$ and $p_U(x)$. If the cross entropy $\mathrm{H}(p_{\mathrm{pcl}}, p_U)$ is larger than the entropy $\mathrm{H}(p_U)$ then $p_{\mathrm{pcl}}(x|U)$ is sampling bit-strings that have lower probability of being observed by the circuit U.

We are interested in the average performance of the classical algorithm. Therefore, we average the cross entropy over an ensemble $\{U\}$ of random circuits

$$\mathbb{E}_U\left[\mathrm{H}(p_{\mathrm{pcl}}, p_U)\right] = \mathbb{E}_U\left[\sum_{j=1}^N p_{\mathrm{pcl}}(x_j|U)\frac{1}{\log p_U(x_j)}\right]. \tag{5}$$

Based on aforementioned insights from quantum chaos, we assume that the output of a classical algorithm with polynomial cost is almost statistically uncorrelated with

*boixo@google.com
†smelyan@google.com
‡babbush@google.com

$p_U(x)$. Thus, averaging over the ensemble $\{U\}$ can be done independently for the output of the polynomial classical algorithm $p_{\rm pcl}(x|U)$ and $\log p_U(x)$. The distribution of universal random quantum circuits converges to the uniform (Haar) measure with increasing depth [7, 8]. For fixed x_j, the distribution of values $\{p_U(x_j)\}$ when unitaries are sampled from the Haar measure also has the Porter-Thomas form. Therefore, if we use sufficiently deep random quantum circuits, we find that

$$-\mathbb{E}_U\left[\log p_U(x_j)\right] \approx -\int_0^\infty N e^{-Np} \log p \, dp = \log N + \gamma \, . \tag{6}$$

Then using $\sum_{j=1}^N p_{\rm pcl}(x_j|U) = 1$ we get

$$\mathbb{E}_U\left[\mathrm{H}(p_{\rm pcl}, p_U)\right] = \log N + \gamma \, . \tag{7}$$

From Eqs. (2) and (7) we obtain

$$\mathbb{E}_U\left[\log \Pr_U(S) - \log \Pr_U(S_{\rm pcl})\right] \simeq m \, . \tag{8}$$

Equation (8) reveals that a typical sample S from a random circuit U represents a signature of that circuit. Note that the l.h.s. is the expectation value of the log of $\Pi_{x\in S}|\langle x|\psi\rangle|^2 / \Pi_{x\in S_{\rm pcl}}|\langle x|\psi\rangle|^2$. The numerator is dominated by measurement outcomes x that have high measurement probabilities $|\langle x|\psi\rangle|^2 > 1/N$. Conversely, the values of x in the denominator are chosen essentially at random. Therefore, they are dominated by the support of the Porter-Thomas distribution with $p < 1/N$.

The result in Eq. (7) also corresponds to the cross entropy $\mathrm{H}_0 = \log N + \gamma$ of an algorithm which picks bit-strings uniformly at random, $p_0(x) = 1/N$. This leads to a proposal for a test of quantum supremacy. We will measure the quality of an algorithm A as the difference between its cross entropy and the cross entropy of a uniform classical sampler. The algorithm A can be an experimental quantum implementation or a classical algorithm. We call this the cross entropy difference:

$$\Delta\mathrm{H}(p_A) \equiv \mathrm{H}_0 - \mathrm{H}(p_A, p_U) = \sum_j \left(\frac{1}{N} - p_A(x_j|U)\right) \log \frac{1}{p_U(x_j)} \, . \tag{9}$$

The cross entropy difference measures how well algorithm $A(U)$ can predict the output of a (typical) quantum random circuit U. This quantity is unity for the ideal random circuit and zero for the uniform distribution.

Because an experimental implementation of a quantum circuit is a realization of a quantum algorithm, we refer to the experimental implementation as $A_{\rm exp}(U)$ and associate with it the probability distribution $p_{\rm exp}(x_j|U) = \langle x_j|\,\rho_{\mathcal{K}}\,|x_j\rangle$ and samples $S_{\rm exp}$. The experimental cross entropy difference is $\alpha \equiv \mathbb{E}_U[\Delta\mathrm{H}(p_{\rm exp})]$. Quantum supremacy is achieved, in practice, when

$$1 \geq \alpha > C \, , \tag{10}$$

where a lower bound for C is given by the performance of the best known classical algorithm A^* executed on an existing classical computer,

$$C = \mathbb{E}_U[\Delta\mathrm{H}(p^*)] \, . \tag{11}$$

Here p^* is the output distribution of A^*.

The space and time complexity of simulating a random circuit by using tensor contractions is exponential in the treewidth of the quantum circuit, which is proportional to $\min(d, n)$ in a 1D lattice, and $\min(d\sqrt{n}, n)$ in a 2D lattice [10]. For large depth d, algorithms are limited by the memory required to store the wavefunction in random-access memory, which in single precision is $2^n \times 2 \times 4$ bytes. For $n = 48$ qubits this requires at least 2.25 Petabytes, which is approximately the limit of what can be done on the largest supercomputers of today[1]. For circuits of small depth or less than approximately 48 qubits, direct simulation is viable so $C = 1$ and quantum supremacy is impossible. Beyond this regime, the most viable approximation scheme (of which we are aware) is an estimation of the Feynman path integral corresponding to the unitary transformation U. In this regime, the lower bound for C decreases exponentially with the number of gates $g \gg n$.

We now address the question of how the cross entropy difference α can be estimated from an experimental sample of bit-strings $S_{\rm exp}$ obtained by measuring the output of $A_{\rm exp}(U)$ after m realizations of the circuit. For a typical sample $S_{\rm exp}$ (see Eq. (2)), the central limit theorem applied to Eq. (9) implies that

$$\alpha \simeq \mathrm{H}_0 - \frac{1}{m}\sum_{j=1}^m \log \frac{1}{p_U(x_j^{\rm exp})} \, . \tag{12}$$

The statistical error in this equation, from the central limit theorem, goes like $\kappa/\sqrt{m}$, with $\kappa \simeq 1$. The estimation would proceed as:

1. Select a random circuit U by sampling from an available universal set of one and two qubit gates, subject to experimental layout constraints.

2. Take a sufficiently large sample $S_{\rm exp} = \{x_1^{\rm exp}, \ldots, x_m^{\rm exp}\}$ of bit-strings x in the computational basis ($m \sim 10^3 - 10^6$).

3. Compute the quantities $\log 1/p_U(x_j^{\rm exp})$ with the aid of a sufficiently powerful classical computer.

4. Estimate α using Eq. (12).

A close correspondence between experiment, numerics and theory provides a reliable foundation from which to extrapolate α to larger circuits where the quantities $p_U(x_j)$ can no longer be obtained numerically. At this point, $C \simeq 0$, and supremacy can be achieved. The value of α can be extrapolated from circuits that can be simulated because they have either less qubits (direct simulation), mostly Clifford gates (stabilizer simulations) [4] or smaller depth (tensor contraction simulations) [10].

[1] Trinity, the sixth fastest supercomputer in TOP500 has about two Petabytes of primary memory, which is one of the largest.

We now present a theoretical error model for α that can be compared with experiment. The output ρ of the experimental realization of a random circuit U is

$$\rho = \tilde{\alpha} U |\psi_0\rangle\langle\psi_0| U^\dagger + (1-\tilde{\alpha})\sigma_U \ , \qquad (13)$$

where $\langle\psi_0| U^\dagger \sigma_U U |\psi_0\rangle = 0$ and $\tilde{\alpha}$ is the circuit fidelity. Under this ansatz, by the same arguments leading to Eq. (7), we obtain that the circuit fidelity $\tilde{\alpha}$ is approximately equal to the cross entropy difference, i.e. $\alpha \approx \tilde{\alpha}$. The absence of correlations is supported by numerical simulations of typical random circuits. Estimating the circuit fidelity by directly measuring the cross entropy (see Eq. (12)) is a fundamentally new way to characterize complex quantum circuits.

The standard approach for studying circuit fidelities is a digital error model where each gate is followed by an error channel [3, 9]. Within this model, the circuit fidelity can be estimated as [3]

$$\alpha \approx \exp(-r_1 g_1 - r_2 g_2 - r_{\text{init}} n - r_{\text{mes}} n) \ , \qquad (14)$$

where $r_1, r_2 \ll 1$ are the Pauli error rates for one and two qubit gates, $r_{\text{init}}, r_{\text{mes}} \ll 1$ are the initialization and measurement error rates, and $g_1, g_2 \gg 1$ are the numbers of one and two qubits gates respectively.

Figure 1 compares the cross entropy difference, Eq. (9), obtained from our numerical simulations, with the estimated fidelity, Eq. (14). We observe a good fit between these two quantities. The validation of the digital error model for complex quantum circuits is a long standing problem. Our proposal represents a novel way of characterizing devices and validating error models for multi-qubit circuits. While our method requires exponential classical computation, it can be performed with a relatively small number of experiments and can be performed for up to 48 qubits.

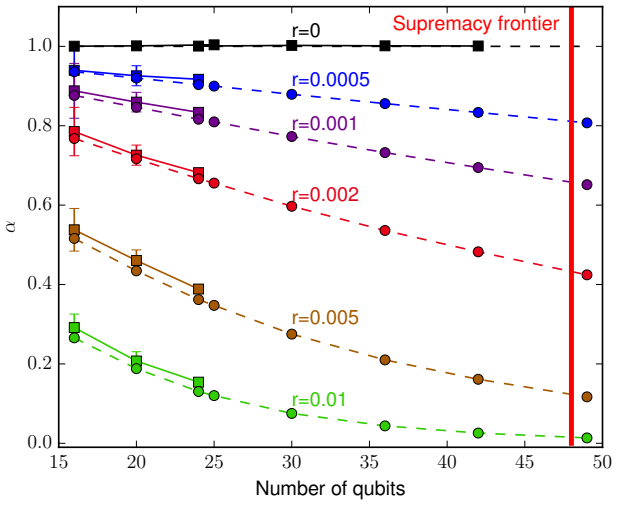


Figure 1: The circuit fidelity α as a function of the number of qubits. Different colors correspond to different Pauli error rates $r_2 = r_{\text{init}} = r_{\text{mes}} = r$ and $r_1 = r/10$. The circle markers correspond to the estimated fidelity, Eq. (14). The square markers correspond to the average cross entropy difference among 100 instances, Eq. (9). The circuit depth is 25. The red line, at 48 qubits, is an estimate of the largest size that can be simulated with state-of-the-art supercomputers. Using state-of-the-art superconducting circuits we expect $\alpha \gtrsim 0.1$ for a 7×7 circuit. Error bars correspond to the std among 100 instances.

References

[1] A. Ambainis and J. Emerson. Quantum t-designs: t-wise independence in the quantum world. In *CCC'07*, pages 129–140. IEEE, 2007.

[2] L. Arnaud and D. Braun. Efficiency of producing random unitary matrices with quantum circuits. *Phys. Rev. A*, 78(6):062329, 2008.

[3] R. Barends et al. Digital quantum simulation of fermionic models with a superconducting circuit. *Nat. Comm.*, 6:7654, July 2015.

[4] S. Bravyi and D. Gosset. Improved classical simulation of quantum circuits dominated by Clifford gates. *arXiv:1601.07601*, 2016.

[5] W. G. Brown and L. Viola. Convergence rates for arbitrary statistical moments of random quantum circuits. *Phys. Rev. Lett.*, 104(25):250501, 2010.

[6] O. C. Dahlsten, R. Oliveira, and M. B. Plenio. The emergence of typical entanglement in two-party random processes. *J. Phys. A*, 40(28):8081, 2007.

[7] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory. Pseudo-random unitary operators for quantum information processing. *Science*, 302(5653):2098–2100, 2003.

[8] A. W. Harrow and R. A. Low. Random quantum circuits are approximate 2-designs. *Comm. Math. Phys.*, 291(1):257–302, 2009.

[9] E. Knill et al. Randomized benchmarking of quantum gates. *Phys. Rev. A*, 77(1):012307, 2008.

[10] I. L. Markov and Y. Shi. Simulating quantum computation by contracting tensor networks. *SICOMP*, 38(3):963–981, Jan. 2008.

[11] C. Porter and R. Thomas. Fluctuations of nuclear reaction widths. *Phys.Rev.*, 104(2):483, 1956.

Factoring with Qutrits: Application of Improved Circuit Synthesis on Two Ternary Architectures

Alex Bocharov[1] * Shawn X. Cui[2] † Martin Roetteler[1] ‡ Krysta M. Svore[1] §

[1] *Microsoft Research*
[2] *University of California, Santa Barbara*

Abstract. In two recent research papers we have developed a novel approach to synthesis of reversible classical circuits, and in particular integer arithmetic circuits, on ternary quantum computers and applied the approach to emulating Shor's period finding function in two different universal quantum ternary bases. We have done comparative analysis of the overall structure and cost of the period finding function in these bases, one of which is a ternary analog of the Clifford+$\pi/8$ and the other comes from the topological quantum computer based on non-Abelian metaplectic anyon framework. Significant benefits of the latter framework have been demonstrated.

Keywords: integer factorization, ternary reversible circuit, circuit synthesis, topological qutrit

1 Introduction and Background

Shor's quantum algorithm for integer factorization [16] is a striking case of the exponential speed-up promised by a quantum computer over the best-known classical algorithms. Since Shor's original paper, many explicit circuit constructions over qubits for performing the algorithm have been developed and analyzed. This includes the computer-assisted synthesis of the underlying quantum circuits for the binary case (see the following and references therein: [1, 2, 9, 13, 14, 15, 17, 18, 19]).

Research in prospective devices for fault-tolerant scalable quantum computing uncovered the importance of non-binary and in particular, ternary quantum frameworks. A recent ambitious proposal for the metaplectic topological quantum computer (MTQC), in particular [10, 11] offers native topological protection of quantum information and quantum gates from local decoherence as an added value over already very nice efficient logical circuit synthesis story [4, 3]. The MTQC creates an inherently ternary quantum computing environment; for example the common binary CNOT gate is no longer a Clifford gate in that environment.

We studied The compilation and synthesis of ternary circuits over two quantum bases: the Clifford + $R_{|2\rangle}$ basis [4] and the Clifford + P_9 basis [5], where $R_{|2\rangle}$ and P_9 are both non-Clifford single qutrit gates defined as:

$$R_{|2\rangle} = \mathrm{diag}(1, 1, -1) \tag{1}$$

$$P_9 = \mathrm{diag}(e^{-2\pi\, i/9}, 1, e^{2\pi\, i/9}). \tag{2}$$

Clifford + $R_{|2\rangle}$ The Clifford + $R_{|2\rangle}$ basis [11], also called metaplectic basis, can be obtained from a MTQC by braiding of certain metaplectic non-abelian anyons and projective measurement. The gate $R_{|2\rangle}$ is produced by injection of the magic state

$$|\psi\rangle = |0\rangle - |1\rangle + |2\rangle. \tag{3}$$

The injection circuit is coherent probabilistic, succeeds in three iterations on average and consumes three copies of the magic state $|\psi\rangle$ on average. The $|\psi\rangle$ state is produced by a relatively inexpensive protocol that uses topological measurement and consequent intra-qutrit projection (see [11], Lemma 5). This protocol requires only three qutrits and produces an exact copy of $|\psi\rangle$ in 9/4 trials on average. This is much better than any state distillation method, especially because it produces $|\psi\rangle$ with fidelity 1.

In [4] we have developed effective compilation methods to compile efficient circuits in the metaplectic basis. In particular, given an arbitrary two-level Householder reflection r and a precision ε, then r is effectively approximated by a metaplectic circuit of $R_{|2\rangle}$-count at most $C\,\log_3(1/\varepsilon) + O(\log(\log(1/\varepsilon)))$, $C \leq 8$. It is shown in [3] that the P_9 gate specifically requires $C = 6$.

Clifford + P_9 The Clifford + P_9 basis is a natural generalization of the binary $\pi/8$ gate. It is the ternary case of the general multi-qudit basis proposed independently in [12] and [8]. The P_9 gate can be realized by a certain deterministic measurement-assisted circuit [8] given a copy of the *magic* state

$$\mu = e^{-2\pi\, i/9}|0\rangle + |1\rangle + e^{2\pi\, i/9}|2\rangle, \tag{4}$$

which further can be obtained from the usual magic state distillation protocol. Specifically, it requires $O(\log^3(1/\delta))$ raw magic states of low fixed fidelity in order to distill a copy of the magic state μ at fidelity $1 - \delta$.

In [5] we have explored a novel approach to synthesis of reversible ternary classical circuits over the Clifford+P_9 basis. We have synthesized explicit circuits to express classical reflections and other important classical non-Clifford gates in this basis, which we subsequently used to build efficient ternary implementations of integer adders and their extensions.

In [6] we have further optimized these implementations under the assumption of binary-encoded data and applied the resulting solutions to emulating of the modular exponentiation period finding (which is the quantum part of the Shor's integer factorization algorithm). We have performed the comparative cost analysis of optimized so-

*alexeib@microsoft.com
†cuixsh@gmail.com
‡martinro@microsoft.com
§ksvore@microsoft.com

lutions between the "generic" Clifford+P_9 architecture and the MTQC architecture (the Clifford + $R_{|2\rangle}$) using magic state counts as the cost measure. We have shown that the cost of emulating the entire binary circuit for the period finding is almost directly proportional to the cost of emulating the three-qubit Toffoli gate and the latter is proportional to the cost of the P_9 gate. We have further pointed out that known distillation protocols for the latter are somewhat more costly than best known distillation protocols (e.g. Bravyi-Kitaev, [7]) for the binary $\pi/8$ gate, but demonstrated that on an MTQC computer specifically the magic state for the P_9 gate can be prepared (with a metaplectic circuit) rather than distilled which leads to asymptotically lower magic state cost: *linear* in fidelity bit size for preparation vs. cubic for distillation. Thus the prospective MTQC architecture is proven to be the most cost-effective known architecture for integer factorization in terms of the overall logical cost. Expected native topological protection of quantum information and gates in the MTQC architecture clearly only adds value to it.

2 Overview of main results

In [6] we have investigated in some detail the cost of implementing Shor's integer factorization algorithm [16] on the two ternary architectures, Clifford + P_9 and Clifford + $R_{|2\rangle}$, using fairly straightforward emulation of known binary circuits and modifications thereof in ternary logic. One technical hurdle to overcome on that path: the binary CNOT gate cannot be emulated by a ternary Clifford circuit and its cost is roughly the same as that of Toffoli gate. The other key problem was to emulate the binary Toffoli gate efficiently. In course of solving these problems we have made the following useful observation: *if a binary reflection (such as that Toffoli gate) needs to be emulated only on binary data, then it can be typically done at a fraction of the cost involved in implementing a ternary reflection.* For example, implementing two-level ternary transposition $|110\rangle \leftrightarrow |111\rangle$ is relatively expensive, but its action on binary data only can be emulated exactly at 2/5 of the cost. In particular we have proved the following

Proposition 1 *1) The binary CNOT gate can be emulated exactly by a two-qutrit ternary circuit containing ternary Clifford gates and* **6** P_9 *gates.*

2) The binary Toffoli gate can be emulated exactly either by a four-qutrit ternary circuit containing ternary Clifford gates and **6** P_9 *gates, or by a three-qutrit ternary circuit containing ternary Clifford gates and* **15** P_9 *gates.*

We also found that by a minor rearrangements of controlled adder circuits, the CNOT/Toffoli ratio for the n-qubit additive shift is constrained to $O(1/\log(n))$ and thus up to a small overhead factor of $(1 + O(1/\log(n)))$, the cost of emulation of Shor's period finding function is directly proportional to the cost of emulating the three-qubit Toffoli gate.

We have chosen to use the magic state counts that tally the number of magic states required for binary implementation or, respectively, ternary emulation of the target gates and circuits. For the Clifford+$\pi/8$ the magic states consumed by the $\pi/8$ gate are counted and for both ternary bases the instances of the magic state $|\mu\rangle$ consumed by the P_9 gate are counted. The cost bounds for the Toffoli gate are presented in Table 1.

	Clean magic states	Raw resources
Binary	7	$7(2\,\log_2(1/\delta))^{2.5}$
Generic^A P_9	15	$15\log_2^3(1/\delta)$
Generic^B P_9	6	$6\log_2^3(1/\delta)$
Metaplectic	6	$36\log_3(1/\delta)$

Table 1: Resource count factors for three-qubit Toffoli gates. "Generic ^{A}" stands for 3-qutrit emulation of the Toffoli gate and "Generic ^{B}" and "Metaplectic" use 4-qutrit emulation with one clean ancilla prepared with SUM gates.

We note that the ternary emulation of the modular exponentiation circuit based on modified ripple carry additive shift as described in [6] section III, A, has the depth $O(n^3)$ for the n-bit integers and performs all the Toffoli gates sequentially. This means that the required clean ancilla is shared across the circuit and adds just one unit of width that is easily amortized over n. The entire modular exponentiation circuit has the width of *only* $n + 3$ *qutrits* in this case.

In the more sophisticated modular exponentiation circuit based on carry lookahead additive shift ([6] section III, B) several Toffoli gates are performed in parallel in almost any time slice, and therefore as many clean ancillas are required concurrently. The impact of this design on the width of the circuits is presented in the Table 2.

Circuits	Online width	Offline width
Binary QCLA	$3\,n - w(n)$ (qubits)	$7\,n\,(6\,\log_2(n))^{2.5}$
Generic ^{A}	$3\,n - w(n)$ (qutrits)	$15\,n\,(3\,\log_2(n))^3$
Generic ^{B}	$4\,n - w(n)$ (qutrits)	$6\,n\,(3\,\log_2(n))^3$
Metaplectic ^{A}	$3\,n - w(n)$ (qutrits)	$90 \times 3\,n\,\log_3(n)$
Metaplectic ^{B}	$4\,n - w(n)$ (qutrits)	$36 \times 3\,n\,\log_3(n)$

Table 2: Widths comparison for ternary emulations of reduced-depth modular exponentiation circuits. ($w(n)$ is the Hamming weight of n). Generic/metaplectic case ^{A} stands for 3-qutrit emulation of the Toffoli gate and case ^{B} for the 4-qutrit emulation. The last column in metaplectic rows shown the expected average of the probabilistic width.

It is seen from Table 1 and Table 2 that the solutions over the metaplectic architecture are the most cost-effective in both asymptotic and practical sense. The tables compare logical magic state counts and logical widths of known binary solutions and those of their ternary emulation but disregard the cost quantum error correction (QEC). Deeming the QEC cost would have been even more in favor of the metaplectic architecture.

References

[1] S. Beauregard. Circuit for Shor's algorithm using 2n+3 qubits. In *QIC*, 3(2), 2003.

[2] D. Beckman, A. N. Chari, S. Devabhaktuni, J. Preskill. Efficient networks for quantum factoring. In *Phys. Rev. A.*, 54:1034–1063, 1996.

[3] A. Bocharov. A Note on Optimality of Quantum Circuits over Metaplectic Basis. arxiv.org/abs/1606.02315, 2016.

[4] A. Bocharov, S. X. Cui, V. Kliuchnikov, Z. Wang. Efficient topological compilation for weakly-integral anyon model. In *Phys. Rev. A.* 93, 012313, 2016.

[5] A. Bocharov, S. X. Cui, M. Roetteler, K. M. Svore. Improved quantum ternary arithmetics. In *QIC*, 16(9,10): 862-884, 2016. (arxiv.org/abs/1512.03824)

[6] A. Bocharov, M. Roetteler, K. M. Svore. Factoring with Qutrits: Shor's Algorithm on Ternary and Metaplectic Quantum Architectures. arxiv.org/abs/1605.02756, 2016.

[7] S. Bravyi, A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. In *Phys. Rev. A.*, 32(6), 2005.

[8] E. .T. Campbell, H. Anwar, D. E. Browne: Magic-state distillation in all prime dimensions using quantum reed-muller codes. In *Phys. Rev. X.*, 2(4), 041021, 2012.

[9] R. Holevo, J. Watrous. Fast parallel circuits for the quantum Fourier transform. In *FOCS '00 Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, 2000.

[10] S. X. Cui, S-M. Hong, Z. Wang. Universal quantum computation with weakly integral anyons. In *Quantum Information Processing*, 14: 2687–2727, 2014.

[11] S. X. Cui, Z. Wang. Universal quantum computation with metaplectic anyons. In *Journal of Mathematical Physics*, 56(3), 032202, 2015.

[12] M. Howard, J. Vala. Qudit versions of the qubit $\pi/8$ gate. In *Phys. Rev. A.*, 86(2), 022316, 2012.

[13] I. L. Markov, M. Saeedi. Constant-optimized quantum circuits for modular multiplication and exponentiation. In *QIC*, pages 12(5,6), 2012.

[14] I. L. Markov, M. Saeedi. Faster quantum number factoring via circuit synthesis. In *Phys. Rev. A.*, 87(012310), 2013.

[15] R. Van Meter, K. M. Itoh. Fast quantum modular exponentiation. In *Phys. Rev. A.*, 71(052320), 2005.

[16] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp.*, 26(5):1484–1509, 1997.

[17] Y. Takahashi, N. Kunihiro. A quantum circuit for Shors factoring algorithm using 2n+2 qubits. In *QIC*, 6(2), 2006.

[18] V. Vedral, A. Barenco, A. Ekert. Quantum networks for elementary arithmetic operations. In *Phys. Rev. A.*, 54(147), 1995.

[19] C. Zalka. Fast versions of Shor's quantum factoring algorithm. quant-ph/9806084, 1998.

Space-Efficient Error-Reduction for Unitary Quantum Computations*

Bill Fefferman[1] Hirotada Kobayashi[2] Cedric Yen-Yu Lin[1] Tomoyuki Morimae[3] Harumichi Nishimura[4]

[1] *Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD, USA*
[2] *Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan*
[3] *Advanced Scientific Research Leaders Development Unit, Gunma University, Kiryu, Gunma, Japan*
[4] *Graduate School of Information Science, Nagoya University, Nagoya, Aichi, Japan*

Abstract. This paper develops general space-efficient methods for error reduction for unitary quantum computation, i.e. computations without intermediate measurements. Consider a unitary quantum computation with completeness c and soundness s, either with or without a witness. To reduce the error of the computation to at most 2^{-p}, the most space-efficient method known requires extra workspace of $O(p \log[1/(c-s)])$ qubits. We present error-reduction methods that require extra workspace of just $O(\log [p/(c-s)])$ qubits. This in particular gives the first methods of strong amplification for logarithmic-space unitary quantum computations with two-sided error. Consequences include the uselessness of quantum witnesses in bounded-error logspace unitary quantum computations, the PSPACE upper bound for QMA with exponentially small gap, and strong amplification for matchgate computations.

Keywords: space-bounded computation, quantum Merlin-Arthur, error reduction, quantum computing

1 Introduction

A very basic topic in various models of quantum computation is whether computation error can be efficiently reduced. For polynomial-time bounded error quantum computation, the computation error can be made exponentially small via a simple repetition followed by a threshold-value decision. This justifies the choice of 2/3 and 1/3 for the completeness and soundness parameters in the definition of the corresponding complexity class BQP. This is also the case for quantum Merlin-Arthur (QMA) proof systems, another central model of quantum computation that models a quantum analogue of NP (more precisely, MA). The price paid is the enlargement of both the necessary workspace and the witness size linearly in the number of repetitions.

We now restrict attention to *unitary* quantum computations, i.e. computations in which only unitary operations are allowed and in particular intermediate measurements are not allowed. Marriott and Watrous [2] developed a more sophisticated method of error reduction for QMA proof systems, which was subsequently improved by Nagaj, Wocjan, and Zhang [3]. The latter improved method uses phase estimation to estimate the success probability of the original computation, similarly to the quantum counting algorithm (see e.g. [4, Chapter 6.3]). This method reuses both the workspace and the witness every time it applies the original computation and its inverse, and therefore does not increase the witness size. Since the inverse of the original computation needs to be applied, this amplification method works only for unitary computations. To reduce the error probability to 2^{-p}, the method requires $O\left(\frac{p}{c-s}\right)$ applications of the original computation and its inverse, and extra workspace of size $O\left(p \log \frac{1}{c-s}\right)$ to store the phase estimation results, where c and s are respectively the completeness and soundness of the original computation.

This existing in-place amplification method is still insufficient if the workspace size must be logarithmically bounded. No efficient error-reduction method is known that keeps the size of necessary additional workspace logarithmically bounded. This is not limited to the case of QMA proof systems, and in fact efficient error reduction methods are rarely known for space-bounded quantum computations (see [5] for an exception).

2 Main Result

This paper presents a general method of strong and space-efficient error reduction for *unitary* quantum computations. In particular, the method is applicable to logarithmic-space unitary quantum computations and QMA proof systems. All of our results hold for any model of *unitary* space-bounded quantum computations. The unitary model is not the most general (note the standard technique of deferring intermediate measurements requires unallowablly many ancilla qubits in the case of space-bounded computations), but our error amplification results (and other recent progress [6]) make this arguably one of the most reasonable models for space-bounded quantum computation; see [7] for a discussion of other models of space-bounded quantum computation.

Let $\mathbb{N}$ and $\mathbb{Z}^+$ be the sets of positive and nonnegative integers, respectively. Let $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ denote the class of problems having QMA proof systems with completeness c and soundness s, where the verifier performs a *unitary* quantum computation that has no time bound but is restricted to use $l_{\mathsf{V}}(n)$ private qubits and to receive a quantum witness of $l_{\mathsf{M}}(n)$ qubits on every input of length n. The main result of this paper is the following strong and space-efficient error-reduction for such QMA-type computations.

Theorem 1 *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and for any functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, there*

*Full version: arXiv:1604.08192 [1]

exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ *that is logarithmic with respect to* $\frac{p}{c-s}$ *such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}+\delta, l_{\mathsf{M}}](1-2^{-p}, 2^{-p}).$$

In the full version [1] we give three different proofs of this main theorem. In the following we discuss many consequences of our main theorem. Many corollaries are straightforward to show by choosing parameters in Theorem 1 appropriately; see the full version for choices of these parameters and for other omitted consequencess (e.g. space-efficient amplification for QMA and strong amplification for matchgate computation)

3 Implications

Strong amplification for unitary logspace quantum computations The first consequence of Theorem 1 is a remarkably strong error-reducibility for logspace unitary quantum computations. Let $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c,s)$ and $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s)$ denote respectively the class of problems decidable by logspace unitary quantum computations (resp. logspace unitary QMA proof systems with log-size witnesses) with completeness c and soundness s.

Corollary 2 *For any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$ *that is logarithmic-space computable and for any logarithmic-space computable functions* $c, s\colon \mathbb{Z}^+ \to [0,1]$ *satisfying* $c - s \geq 1/q$ *for some polynomially bounded function* $q\colon \mathbb{Z}^+ \to \mathbb{N}$*,*

$$\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c,s) \subseteq \mathrm{Q}_{\mathbf{U}}\mathrm{L}(1-2^{-p}, 2^{-p}).$$
$$\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(1-2^{-p}, 2^{-p}).$$

This in particular justifies defining the classes $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$ and $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ of bounded-error logarithmic-space unitary quantum computations by $\mathrm{BQ}_{\mathbf{U}}\mathrm{L} = \mathrm{Q}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$ and $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$.

Uselessness of quantum witnesses in logarithmic-space unitary QMA By a standard technique of replacing a quantum witness by a completely mixed state Corollary 2 implies the following:

Corollary 3 $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{BQ}_{\mathbf{U}}\mathrm{L}$.

A consequence of the Marriott-Watrous error reduction method [2] was that standard QMA systems are no more powerful than BQP if restricted to use witnesses of logarithmic size. Corollary 3 extends this by stating that logarithmic sized witnesses do not increase the power of logspace unitary quantum computations at all.

Strong amplification for unitary QMAPSPACE Let $\mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ and $\mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ denote respectively the class of problems decidable by poly-space unitary quantum computations (resp. QMA proof systems) with completeness c and soundness s. We have the following scaled-up version of Corollary 2.

Corollary 4 *For any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$ *and for any polynomial-space computable functions* $c, s\colon \mathbb{Z}^+ \to [0,1]$ *satisfying* $c - s \geq 2^{-q}$ *for some polynomially bounded function* $q\colon \mathbb{Z}^+ \to \mathbb{N}$*,*

$$\mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}(c,s) \subseteq \mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}\big(1-2^{-2^p}, 2^{-2^p}\big).$$
$$\mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}(c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}\big(1-2^{-2^p}, 2^{-2^p}\big).$$

Again by replacing the quantum witness by a completely mixed state, the following result follows from Corollary 4 and that unbounded-error poly-space quantum computations can be simulated in PSPACE [8, 9].

Corollary 5 *For any polynomial-space computable functions* $c, s\colon \mathbb{Z}^+ \to [0,1]$ *satisfying* $c - s \geq 2^{-q}$ *for some polynomially bounded function* $q\colon \mathbb{Z}^+ \to \mathbb{N}$*,*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}(c,s) = \mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}(c,s) = \mathrm{PSPACE}.$$

Let $\mathrm{QMA}(c,s)$ be the class of problems having polynomial-time QMA proof systems with completeness c and soundness s. An immediate corollary of Corollary 5 is the following upper bound for QMA proof systems with exponentially small completeness-soundness gap.

Corollary 6 *For any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$ *and for any polynomial-time computable functions* $c, s\colon \mathbb{Z}^+ \to [0,1]$ *satisfying* $c - s \geq 2^{-q}$ *for some polynomially bounded function* $q\colon \mathbb{Z}^+ \to \mathbb{N}$*,*

$$\mathrm{QMA}(c,s) \subseteq \mathrm{PSPACE}.$$

Corollary 6 was also shown independently in [10]. In fact, the first and third authors of the present paper further proved that the converse of Corollary 6 also holds, i.e., PSPACE is characterized by QMA proof systems with exponentially small gap [6].

References

[1] B. Fefferman, H. Kobayashi, C. Y.-Y. Lin, T. Morimae, and H. Nishimura. arXiv:1604.08192.

[2] C. Marriott and J. Watrous. *Computational Complexity*, 14(2):122-152, 2005.

[3] D. Nagaj, P. Wocjan, and Y. Zhang. *Quantum Information and Computation*, 9(11-12):1053-1068, 2009.

[4] M. A. Nielsen and I. L. Chuang. Cambridge University Press, 2000.

[5] J. Watrous. *Journal of Computer and System Sciences*, 62(2):376-391, 2001.

[6] B. Fefferman and C. Y.-Y. Lin. arXiv:1604.01384.

[7] D. van Melkebeek and T. Watson. *Theory of Computing*, 8:1-51, 2012.

[8] J. Watrous. *Journal of Computer and System Sciences*, 59(2):281-326, 1999.

[9] J. Watrous. *Computational Complexity*, 12(1-2):48-84, 2003.

[10] A. Natarajan and X. Wu. Private communication, Jan., 2016.

Hamiltonian quantum computer in one dimension

Tzu-Chieh Wei[1] * John C. Liang[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] *Rumson-Fair Haven Regional High School, 74 Ridge Rd, Rumson, NJ 07760, USA*

Abstract. We consider Hamiltonian quantum computation (HQC) in one dimension, achieved by preparing an appropriate initial product state of qudits and then letting it evolve under a fixed Hamiltonian before measuring individual qudits at some later time. We study the compromise between the locality k and the local Hilbert space dimension d for universal HQC. For geometrically 2-local (i.e., $k = 2$), $d = 8$ is known to be sufficient. We provide a construction for $k = 3$ with $d = 5$. Imposing translation invariance will increase the required d. For this we also construct another 3-local ($k = 3$) Hamiltonian that is invariant under translation of a unit cell of two sites but that requires d to be 8.

Keywords: Hamiltonian quantum computer, quantum walk, quantum cellular automata, locality, local Hilbert space dimension

1 Motivations

Feynman provided an example Hamiltonian able to execute universal quantum computer [1],

$$H_{\text{Feynman}} = \sum_{j=0}^{k-1} \sigma_{j+1}^{+} \sigma_j^{-} A_{j+1} + \text{h.c.}, \qquad (1)$$

but the interaction involves four particles not geometrically local. Operators σ^- and σ^+ act on a set of spin-1/2 particles, representing a discrete unary clock register; A_j's represent all the gates of a circuit.

Key questions to address. In this work we consider the Hamiltonian quantum computer to lie on one spatial dimension, and the interaction in the Hamiltonian involves at most k consecutive sites. In particular, we study the compromise between the locality k and the local Hilbert-space dimension d. As the locality k increases, it is expected that the minimum required d should decrease.

Prior related works. Feynman's idea was used by Kitaev to construct the so-called Local Hamiltonian Problems (LHP) [2] and showed that 5-local LHP is QMA-complete. The locality k for QMA-complete LHP was, in a series of work, reduced to 2 [3, 4], even with nearest-neighbor interactions on two spatial dimensions [5]. In one spatial dimension, it was shown by Aharonov et al. that 2-local 13-state Hamiltonians are QMA-complete [6], and the local dimension d is recently reduced to 8 by Hallgren et al. [7].

In terms of one-dimensional Hamiltonian quantum computer, there have been various constructions, for example, the continuous-time quantum cellular automata by Vollbrecht and Cirac [8], by Kay [9], and by Nagaj and Wocjan [10] as well as the universal quantum walk by Chase and Landahl [11]. The 1D Hamiltonians in these constructions are nearest-neighbor two-body (or geometrically 2-local), but involve the dimension of local Hilbert space ranging from $d = 8$ [11] and higher [8, 9, 10].

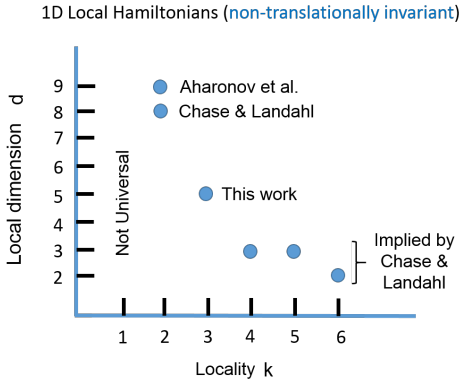


Figure 1: (color online) The status of locality k vs. local Hilbert-space dimension (level) d for universal quantum computation (BQP) in one spatial dimension.

2 Results and some details

Main results. Here we study the compromise between the locality k and the local dimension d in one spatial dimension; the results are summarized in Figs. 1 and 2. In our technical paper [12], we provide two constructions: (i) one that uses a 5-state 3-local (or spin-2 nearest and next-nearest-neighbor interacting) Hamiltonian but is non-translation invariant, and (ii) 8-state 3-local Hamiltonian that is invariant under translation of a unit cell of two sites.

The former is inspired by the design used in 1D QMA LHP [6, 7], whose focus was on 2-locality.In terms of complexity, one implication is that simulating 1D chains of spin-2 particles with nearest and next-nearest-neighbor interaction is BQP-complete. Our second construction is inspired by the translation invariant constructions in Refs. [8, 9, 10] and in particular the work by Nagaj and Wocjan [10]. We explicitly modify a particular scheme with $d = 20$ in Ref. [10] and reduce d to 8. Our results

*tzu-chieh.wei@stonybrook.edu

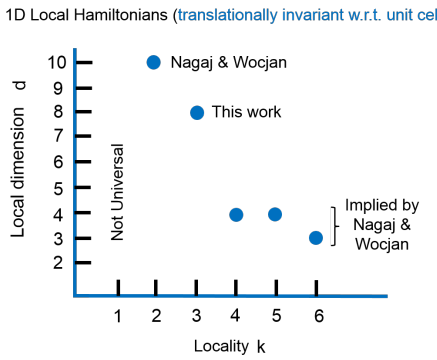


Figure 2: (color online) The translation invariant case.

are summarized schematically in Fig. 1 and Fig. 2.

Detailed construction. Due to the space limitation, it suffices for the purpose of demonstration to focus on our first construction having $k = 3$ and $d = 5$. We refer the other construction that is translation invariant ($k = 3$ and $d = 8$) to our technical paper [12]. On odd/even sites host different groups of states, respectively,

$$\{\triangleright, \triangleleft, \circlearrowleft, \bullet, +\}, \quad \{\square^{[0]}, \square^{[1]}, \blacktriangleright^{[0]}, \blacktriangleright^{[1]}, \bigcirc\}.$$

(We can regard the system as consisting of the same kind of particles on all sites, but their interactions have two different preferred bases.) There are two kinds of qubits: $\square$ and $\blacktriangleright$, and the superscripts are used to indicate the logical qubit values.

The transition rules are shown in Table 1. In particular, the gate operation occurs in rule 1:

$$1: \qquad \blacktriangleright + \square \longrightarrow U_m(\square + \blacktriangleright) \tag{2}$$

whose backward (or time-reversed) propagation is

$$1^\dagger: \qquad \square + \blacktriangleright \longrightarrow U_m^\dagger(\blacktriangleright + \square). \tag{3}$$

The design of these rules ensure that **there is only one unique forward rule and one unique reverse rule** (except at the beginning and the end), and the probability of ending up at any location (i.e. configuration) can be obtained analytically [10].

A. Rules of transitions:

1:	$\blacktriangleright + \square \longrightarrow U_m(\square + \blacktriangleright)$	
$1^\dagger$:	$\square + \blacktriangleright \longrightarrow U_m^\dagger(\blacktriangleright + \square)$	[backward]
2:	$\blacktriangleright \bullet \vert \bigcirc \longrightarrow \square \circlearrowleft \vert \bigcirc$	
3:	$\circlearrowleft \bigcirc \bullet \longrightarrow \triangleleft \bigcirc \bullet$	
4:	$\square \triangleleft \bigcirc \longrightarrow \bigcirc \triangleleft \square$	
5a:	$+ \bigcirc \triangleleft \longrightarrow \triangleleft \bigcirc +$	
5b:	$\bullet \bigcirc \triangleleft \longrightarrow \bullet \bigcirc \circlearrowleft$	
6a:	$\circlearrowleft \vert \square + \longrightarrow \bullet \vert \blacktriangleright +$	
6b:	$\circlearrowleft : \square + \longrightarrow \bullet : \square \triangleright$	
7a:	$\triangleright \square + \longrightarrow + \square \triangleright$	
7b:	$\triangleright \square \bullet : \longrightarrow + \square \circlearrowleft :$	

B. Example of transitions:

[0]	$[\circlearrowleft \vert \square + \square + \square \bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[1]	$[\bullet \vert \blacktriangleright + \square + \square \bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[2]	$[\bullet \vert \square + \blacktriangleright + \square \bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[3]	$[\bullet \vert \square + \square + \blacktriangleright \bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[4]	$[\bullet \vert \square + \square + \square \circlearrowleft \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[5]	$[\bullet \vert \square + \square + \square \triangleleft \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet]$
[6]	$[\bullet \vert \square + \square + \bigcirc \triangleleft \vert \square \bullet \bigcirc \bullet \bigcirc \bullet]$
[7]	$[\bullet \vert \square + \square \triangleleft \bigcirc + \vert \square \bullet \bigcirc \bullet \bigcirc \bullet]$
	.....
[31]	$[\bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \circlearrowleft \vert \square + \square + \square \bullet]$
[32]	$[\bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet \vert \blacktriangleright + \square + \square \bullet]$
[33]	$[\bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet \vert \square + \blacktriangleright + \square \bullet]$
[34]	$[\bullet \vert \bigcirc \bullet \bigcirc \bullet \bigcirc \bullet \vert \square + \square + \blacktriangleright \bullet]$

Table 1: Transition rules and evolution of configurations.

References

[1] R. Feynman. Quantum mechanical computers Opt. News, **11**, 11 (1985).

[2] A. Yu. Kitaev, A.H. Shen and M.N. Vyalyi. —it Classical and Quantum Computation (AMS, Providence, 2002).

[3] J. Kempe and O. Regev. Quantum Inf. Comput. **3**, 258 (2003).

[4] J. Kempe, A. Kitaev, and O. Regev. SIAM J. Comput. **35**, 1070 (2006).

[5] R. Oliveira and B. Terhal. Quantum Inf. Comput. **8**, 0900 (2008).

[6] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. Commun. Math. Phys. **287**, 41 (2009).

[7] S. Hallgren, D. Nagaj, and S. Narayanaswami. Quantum Inf. Comput. **13**, 0721 (2013).

[8] K. G. H. Vollbrecht and J. I. Cirac. Phys. Rev. Lett. **100**, 010501 (2008).

[9] A. Kay. Phys. Rev. A **78**, 012346 (2008).

[10] D. Nagaj and P. Wocjan. Phys. Rev. A **78**, 032311 (2008).

[11] B. A. Chase and A. J. Landahl. e-print arXiv:0802.1207.

[12] T.-C. Wei and J.-C. Liang. Hamiltonian quantum computer in one dimension. arXiv:1512.06775 and Phys. Rev. A **92**, 062334 (2015).

Nonlocal correlations: Fair and Unfair Strategies in Bayesian Game

Arup Roy[1] * Amit Mukherjee[1] † Tamal Guha[1] ‡ Sibasish Ghosh[2] §
Some Sankar Bhattacharya[1] ¶ Manik Banik[2] ‖

[1] *Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108 , India.*
[2] *Optics and Quantum Information Group, The Institute of Mathematical Sciences, C.I.T Campus, Taramani, Chennai 600 113 , India.*

Abstract. Interesting connection has been established between two apparently unrelated concepts, namely, quantum nonlocality and Bayesian game theory. It has been shown that nonlocal correlations in the form of advice can outperform classical equilibrium strategies in common interest Bayesian games and also in conflicting interest Bayesian games. Classical equilibrium strategies can be of two types, fair and unfair. Whereas in fair equilibrium payoffs of different players are equal, in unfair case they differ. Advantage of nonlocal correlation has been demonstrated over fair strategies, only. In this letter we show that quantum strategies can outperform even the unfair classical equilibrium strategies. For this purpose we consider a class of two players Bayesian games. It becomes that, such games can have only fair equilibria, both fair and unfair equilibria, or only unfair ones. We provide a simple analytic method to characterize the nonlocal correlations that are advantageous over the classical equilibrium strategies in these games. We also show that quantum advice provides better *social optimality solution* (a relevant notion of equilibrium for unfair case) over the clssical one.

Keywords: Nonlocal correlation, Fair and Unfair equilibrium, Correlated Equilibrium, Bell Nonlocality

1 Bayesian Game and equilibria

Undoubtedly one of the most fundamental contradictions of Quantum mechanics (QM) with classical physics gets manifested in its nonlocal behavior. This bizarre feature of QM was first established in the seminal work of J. S. Bell [1], where he has shown that QM is incompatible with the *local-realistic* world view of classical physics. More precisely, Bell showed that measurement statistics of multipartite entangled quantum systems can violate an empirically testable local realistic inequality (in general called Bell type inequalities) which establishes the denial of *local realism* underlying QM. Since Bell's work, nonlocality remains at the center of quantum foundational research and it has been verified in numerous successful experiments. Apart from foundational interest, quantum nonlocality finds practical implications in various device-independent protocols. But, very recently Brunner and Linden have established usefulness of Bell nonlocality in Bayesian game theory [2]. A Bayesian game can be played under classical equilibrium strategies which are of two types, fair equilibrium and unfair equilibrium. Payoffs of different players are equal in a fair equilibrium, but differ in case of an unfair equilibrium. It has been shown that QM can provide advantageous strategies over the best classical strategies in common interest Bayesian games [2] as well as conflicting interesting games [3]. However, such advantages are shown over the fair equilibrium. The aim of this present letter is to establish the quantum advantages over the unfair equilibrium strategies. This study is of important relevance since we provide examples of Bayesian games which can be played under unfair equilibrium strategies, only.

*arup145.roy@gmail.com
†amitisiphys@gmail.com
‡g.tamal91@gmail.com
§sibasish@imsc.res.in
¶somesankar@gmail.com
‖manik11ju@gmail.com

2 The class of games we consider

Let Alice and Bob are two players involved in the game. Alice's and Bob's types/inputs are denoted as $x_A \in \mathcal{X}_A$ and $x_B \in \mathcal{X}_B$, respectively. For each type they take some actions/outputs denoted as $y_A \in \mathcal{Y}_A$ and $y_B \in \mathcal{Y}_B$ and accordingly they are given payoffs/utilities denoted as u_A and u_B, respectively, where $u_i : \mathcal{X}_A \times \mathcal{X}_B \times \mathcal{Y}_A \times \mathcal{Y}_B \to \mathbb{R}$, for $i \in \{A, B\}$. For the class of games considered here, $\mathcal{X}_A = \mathcal{X}_B = \mathcal{Y}_A = \mathcal{Y}_B = \{0, 1\}$ and the utilities are given in Table-1. In accordance with the parameter κ and τ of Table-1 let us denote such a game as $\mathcal{G}(\kappa, \tau)$. Whenever $\kappa < \tau$, there is a conflict between Alice and Bob in choosing their actions.

In the case of correlated strategies, i.e., when the parties are given some common advice, the average payoff is calculated as:

$$F_i = \sum_{x,y} P(x)P(y|x)u_i(x, y). \tag{1}$$

Here $P(x)$ is the probability distribution over the Alice's and Bob's joint type $x \equiv (x_A, x_B)$ which is considered to be uniform for the class of games introduced above. $P(y|x)$ denote the conditional probability of the joint action $y \equiv (y_A, y_B)$ given the type x, i.e., the probability that Alice takes action y_A and Bob takes action y_B given their joint type (x_A, x_B). To play the game $\mathcal{G}(\kappa, \tau)$ each of Alice and Bob can take one of the following four pure classical strategies:

$$g_i^1(x_i) = 0;\ g_i^2(x_i) = 1;\ g_i^3(x_i) = x_i;\ g_i^4(x_i) = x_i \oplus 1;$$

where $g_i^1(x_i) = 0$ means that i^{th} party takes the action 0 whatever be the type and similarly for the other

	$x_A \wedge x_B = 0$		$x_A \wedge x_B = 1$	
	$y_B = 0$	$y_B = 1$	$y_B = 0$	$y_B = 1$
$y_A = 0$	$(1, \kappa)$	$(0, 0)$	$(0, 0)$	$(3/4, 3/4)$
$y_A = 1$	$(0, 0)$	$(1/2, \tau)$	$(3/4, 3/4)$	$(0, 0)$

Table 1: Utility table for the game $\mathcal{G}(\kappa, \tau)$. Both κ and τ are positive.

cases; $\oplus$ denotes modulo 2 sum. For the conflicting case (i.e. $\tau > \kappa$) there are three equilibrium strategies $eq_1 \equiv (g_A^1, g_B^3)$, $eq_2 \equiv (g_A^3, g_B^4)$, and $eq_3 \equiv (g_A^4, g_B^2)$ whenever $\kappa < \frac{3}{4}$, with corresponding payoffs being $(F_A^{eq_1}, F_B^{eq_1}) = \left(\frac{11}{16}, \frac{3}{16} + \frac{\kappa}{2}\right)$, $(F_A^{eq_2}, F_B^{eq_2}) = \left(\frac{9}{16}, \frac{3}{16} + \frac{\kappa+\tau}{4}\right)$, and $(F_A^{eq_3}, F_B^{eq_3}) = \left(\frac{7}{16}, \frac{3}{16} + \frac{\tau}{2}\right)$. For $\kappa > \frac{3}{4}$, there are also three equilibrium strategies $eq_1' \equiv (g_A^1, g_B^1)$, eq_2, and eq_3 with payoff for the strategy eq_1' being $(F_A^{eq_1'}, F_B^{eq_1'}) = \left(\frac{3}{4}, \frac{3\kappa}{4}\right)$. For the parameter value $\kappa > 1$, all the three equilibria are unfair and in every case Bob's payoff is greater than that of Alice. Note that in this case ($\kappa > 1$) even no fair correlated equilibrium strategy is possible. The case where $\kappa + \tau = 3/2$ give a fair equilibrium strategy as occurred in the conflicting game of [3]. When $\tau < \kappa$ the game turns out to be a common interest game. In this case there is only one equilibrium strategy, (g_A^1, g_B^3) when $\kappa < \frac{3}{4}$ and (g_A^1, g_B^1) otherwise, with pay-off being $\left(\frac{11}{16}, \frac{3}{16} + \frac{\kappa}{2}\right)$ and $\left(\frac{3}{4}, \frac{3\kappa}{4}\right)$, respectively. Since any classical (local realistic) advice can be written as $P(y_A, y_B|x_A, x_b) = \int d\lambda P(y_A|x_A, \lambda) P(y_B|x_B, \lambda)$, with λ being a local variable (also called hidden variable by the quantum foundation community), convexity ensures that using any such advice it is not possible to overcome the equilibrium payoffs. However in quantum world there are no-signaling correlations that are not of this local realistic form (thus called nonlocal) and hence there may be a possibility to overcome the classical equilibrium payoffs.

3 $2 - 2 - 2$ no-signaling correlations

: For the two-party scenario with two two-outcome measurements for each party, we denote the joint probability distribution as $P(ab|ij)$, where the outcomes $a, b \in \{+, -\}$ and the measurement settings $i, j \in \{0, 1\}$. We can express the joint distribution as:

$$\begin{aligned}&(P(++|ij), P(+-|ij), P(-+|ij), P(--|ij))\\ &\equiv (c_{ij}, m_{ij} - c_{ij}, n_{ij} - c_{ij}, 1 - n_{ij} - m_{ij} + c_{ij}),\end{aligned} \quad (2)$$

Here $m_{ij} := P(++|ij) + P(+-|ij)$ and $n_{ij} := P(++|ij) + P(-+|ij)$ denote the corresponding marginal probabilities of Alice and Bob, with positivity imposing the restrictions, $\max\{0, m_{ij} + n_{ij} - 1\} \leq c_{ij} \leq \min\{m_{ij}, n_{ij}\}\ \forall\ ij$. According to no-signaling Alice's marginal outcome probability should not depend on Bob's measurement settings and vice versa, which can be expressed as $m_{00} = m_{01} := m_0$, $m_{10} = m_{11} := m_1$, $n_{00} = n_{10} := n_0$, $n_{01} = n_{11} := n_1$. The celebrated Bell-CHSH expression is given by, $\mathbb{B} = \langle 00\rangle + \langle 01\rangle + \langle 10\rangle - \langle 11\rangle$, where $\langle ij\rangle := P(++|ij) - P(+-|ij) - P(-+|ij) + P(--|ij)$. A no-signaling probability distribution has a local realistic description if and only if it satisfies the Bell-CHSH inequality, i.e., *iff* $|\mathbb{B}| \leq 2$. In terms of probabilities, the Bell-CHSH expression becomes,

$$\mathbb{B} = 2 + 4(c_{00} + c_{01} + c_{10} - c_{11}) - 4(m_0 + n_0). \quad (3)$$

4 Our result and discussion

In the Bayesian game described above, the two players can be commonly advised by a general no-signaling correlation. Then, Alice's and Bob's average payoffs, respectively, read:

$$F_A^{NS} = \frac{1}{16}\left[3 + 3/2\mathbb{B} + 2(m_0 + n_0) + (m_1 + n_1)\right], \quad (4)$$

$$\begin{aligned}F_B^{NS} = \frac{1}{16}&\left[(10\tau - 2\kappa) + (\tau + \kappa)\mathbb{B} + 4(\kappa - \tau)(m_0 + n_0)\right.\\ &\left.+(3 - 4\tau)(m_1 + n_1) + 4\left(\kappa + \tau - 3/2\right)c_{11}\right].\end{aligned} \quad (5)$$

A no-signaling nonlocal advice outperforms some classical equilibrium payoff (F_A^{eq}, F_B^{eq}) if $F_i^{NS} > F_i^{eq}$, for $i = A, B$.

We show that such nonlocal correlations can outperform the unfair classical equilibrium strategies of such Bayesian games (see [4] for detail). Furthermore we find that unlike for the case of fair strategy the notion of quantum equilibrium is not a valid one for unfair strategies. In this case a stronger refinement of the equilibrium concept, known as social optimality. Given a quantum advice, the choice of measurement settings (strategies), one by each player, will be called social optimality if the sum of all players' payoffs is maximum. We also show that quantum advice can provide unfair social optimal strategies better than the classical one. Although we have considered a particular class but our analysis points out the effectiveness of nonlocal advice over any classical correlation. We have also completely characterize the no-signaling advices providing advantage in these games over the fair and unfair classical equilibrium strategies.

References

[1] J. S. Bell. On the Einstein Podolsky Rosen Paradox Physics *1* (3): 195200 (1964). J. S. Bell, Speakable and Unspeakable in Quantum Mechanics (Cambridge University Press, 1987).

[2] N. Brunner and N. Linden. *Connection between Bell nonlocality and Bayesian game theory.* Nature Communications **4**, 2057 (2013).

[3] A. Pappa *et al.* Nonlocality and Conflicting Interest Games Phys. Rev. Lett. **114**, 020401 (2015).

[4] A. Roy *et al.* Nonlocal correlations: Fair and Unfair Strategies in Bayesian Game. arXiv:1601.02349, 2016.

Bell Correlations in Many-Body Systems

Jean-Daniel Bancal[1] * Roman Schmied[2] Baptiste Allard[2] Matteo Fadel[2]
Valerio Scarani[3 4] Philipp Treutlein[2] Nicolas Sangouard[1]

[1] *Quantum Optics Theory Group, Department of Physics, University of Basel, Klingelbergstrasse 82, 4056 Basel*
[2] *Quantum Atom Optics Lab, Department of Physics, University of Basel, Klingelbergstrasse 82, 4056 Basel*
[3] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[4] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

Abstract. Bell inequality violations have been demonstrated in systems involving up to fourteen particles, but testing a Bell inequality becomes increasingly challenging as the number of parties involved increases. Yet, nonlocal correlations constitute a resource for device-independent information processing. Here, we construct a Bell correlation witness, and show that it can be used to demonstrate that a state is Bell correlated in situations where no Bell test can be performed. We report on an experimental violation of the witness with about 480 atoms in a Bose-Einstein condensate. This opens the way for the study of Bell nonlocality in many-body systems.

The violation of a Bell inequality is the key to device-independent information processing. This allows one to achieve tasks with one of the strongest form of security known today. Security both against powerful adversaries and in face of experimental uncertainties such as systematic measurement errors. Device-independent quantum key distribution (QKD) is an early example of device-independent information processing [1]. Today, more such tasks are known, including the certification of quantum computation [2], of quantum states and measurements [3], and randomness generation [4].

While most device-independent protocols rely on the violation of bipartite Bell inequalities, new forms of correlations are known to arise in presence of a larger number of parties [5]. Testing a Bell inequality on many parties is however technically challenging. Indeed, a Bell test requires addressing of individual particles, which is seldom possible when dealing with more than a few tens of particles. The number of measurements that need to be performed also increases rapidly with the number of parties, and multipartite Bell inequalities typically involve many-body correlations functions, which are difficult to evaluate on systems involving many particles.

Building on the result of [6], we consider here the situation in which well-characterized collective measurements are performed on an ensemble of particles. Using the few-body correlator inequality from [6], we construct a witness operator for Bell correlated quantum states. This witness only involves up to the second moment of two collective measurements (see [7] for more details). It is thus amenable to experimental test on large systems.

We test this witness on a Bose-Einstein Condensate (BEC) of about 480 Rubidium atoms prepared in a spin-squeezed state. An experimental violation of the witness by 3.8 standard deviations is observed (see figure 1), thus demonstrating that the atoms share Bell correlations, i.e. the state of the atoms is able to violate a Bell inequality.

The witness introduced here constitutes an easy way to certify that a many-body quantum system can be used for a device-independent task. This opens questions about the possible use of many-body quantum systems for device-independent information processing. More efforts are also needed to further characterize many-body nonlocal states. Finally, this result brings Bell correlations into the field of quantum many-body physics, where entanglement is already known to be responsible for enhanced metrologic precisions [8].

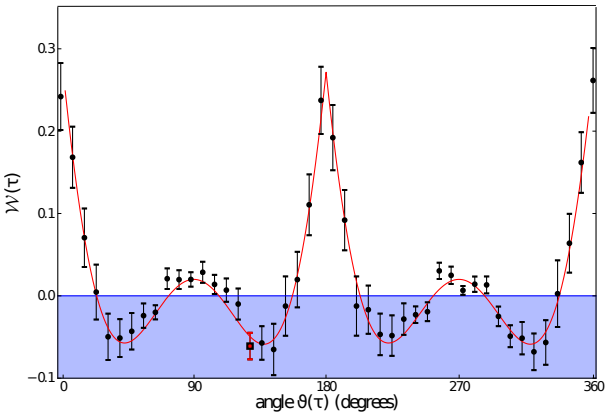


Figure 1: Experimental value of the witness $\mathcal{W}$ upon variation of a parameter θ (see [7] for more details). Non-Bell-correlated states can only achieve a value of $\mathcal{W} \geq 0$. The red dot is 3.8 standard deviations from the bound, demonstrating that the measured state can useful for device-independent tasks.

References

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[2] B. W. Reichardt, F. Unger, U. Vazirani **496**, 456460 (2013).

[3] T. H. Yang, T. Vértesi, J-D. Bancal, V. Scarani, M. Navascus, Phys. Rev. Lett. **113**, 040401 (2014).

*jdbancal.physics@gmail.com

[4] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature **464**, 1021 (2010).

[5] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).

[6] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, A. Acín, Science **344**, 1256 (2014).

[7] R. Schmied, J-D. Bancal, B. Allard, M. Fadel, V. Scarani, P. Treutlein, N. Sangouard, arXiv:1604.06419.

[8] C. Gross, T. Zibold, E. Nicklas, J. Estève, M. K. Oberthaler, Nature **464**, 1165 (2010).

Reliable and robust entanglement witness

Xiao Yuan[1] * Quanxin Mei[1] Shan Zhou[1] Xiongfeng Ma[1] †

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

Abstract. Theoretically, witnessing entanglement is by measuring a special Hermitian observable, called entanglement witness (EW), which has non-negative expected outcomes for all separable states but can have negative expectations for certain entangled states. In practice, an EW implementation may suffer from two problems. The first one is *reliability*. Due to unreliable realization devices, a separable state could be falsely identified as an entangled one. The second problem relates to *robustness*. A witness may be suboptimal for a target state and fail to identify its entanglement. To overcome the reliability problem, we employ a recently proposed measurement-device-independent entanglement witness scheme, in which the correctness of the conclusion is independent of the implemented measurement devices. In order to overcome the robustness problem, we optimize the EW to draw a better conclusion given certain experimental data. With the proposed EW scheme, where only data post-processing needs to be modified comparing to the original measurement-device-independent scheme, one can efficiently take advantage of the measurement results to maximally draw reliable conclusions.

Keywords: entanglement witness, measurement device independent

1 Introduction

Witnessing the existence of entanglement is an important and necessary step for quantum information processing. In theory, entanglement can be witnessed by measuring a Hermitian observable W, whose output expectation for any separable state σ is non-negative, $\mathrm{Tr}(W\sigma) \geq 0$, but can be negative for certain entangled state ρ, $\mathrm{Tr}(W\rho) < 0$. In this case, we call W an entanglement witness (EW) for state ρ. In general, W can be obtained by a linear combination of product observables, which can be measured locally on the subsystems.

In reality, EW implementation may suffer from two problems. The first one is *reliability*. That is, one might conclude unreliable results due to imperfect experimental devices. If the realization devices are not well calibrated, the practically implemented observable W' may deviate from the original theoretical design W, which can even be not a witness. That is, there may exist some separable states σ, such that $\mathrm{Tr}[\sigma W'] < 0 \leq \mathrm{Tr}[\sigma W]$. Branciard et al. proposed the measurement-device-independent entanglement witness (MDIEW) scheme [1], in which entanglement can be witnessed without assuming the realization devices. The MDIEW scheme is based on an important discovery that any entangled state can be witnessed in a nonlocal game with quantum inputs [2]. In the MDIEW scheme, it is shown that an arbitrary conventional EW can be converted to be an MDIEW, which has been experimentally tested [3].

The second problem lies on the *robustness* of EW implementation. Since each (linear) EW can only identify certain regime of entangled states, a given EW is likely to be ineffective to detect entanglement existing in an unknown quantum state. While a failure of detecting entanglement is theoretically acceptable, in practice, such failure may cause experiment to be highly inefficient. In a way, this problem becomes more serious in the MDIEW scenario, where the measurement devices are assumed to be uncharacterized and even untrusted. In this case, the implemented witness, which may although be designed optimal at the first place, can become a bad one which merely detects no entanglement. However, the observed experimental data may still have enough information for detecting entanglement. Therefore, the key problem we are facing here is that given a set of observed experimental data, what is the best entanglement detection capability one can achieve.

Here, we only briefly review our result and refer to Ref. [4] for details.

2 Reliable entanglement witness

Focus on the bipartite scenario with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, with dimensions $\dim\mathcal{H}_A = d_A$ and $\dim\mathcal{H}_B = d_B$. For a bipartite entangled state ρ_{AB} defined on $\mathcal{H}_A \otimes \mathcal{H}_B$, we can always find a conventional entanglement witness W such that $\mathrm{Tr}[W\rho_{AB}] < 0$ and $\mathrm{Tr}[W\sigma_{AB}] \geq 0$ for any separable state σ_{AB}. Suppose $\{\omega_x^{\mathrm{T}}\}$ and $\{\tau_y^{\mathrm{T}}\}$ to be two bases for Hermitian operators on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Thus, we can decompose W on the basis $\{\omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}}\}$ by $W = \sum_{x,y} \beta^{x,y} \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}}$, where $\beta^{x,y}$ are real coefficients and the transpose is for later convenience.

An MDIEW can be obtained by

$$J = \sum_{x,y} \beta_{1,1}^{x,y} p(1,1|\omega_x, \tau_y) \tag{1}$$

where $\beta_{1,1}^{x,y} = \beta^{x,y}$ and $p(1,1|\omega_x, \tau_y)$ is the probability of outputting $(a = 1, b = 1)$ with input states (ω_x, τ_y). In the MDIEW design, Alice (Bob) performs Bell state measurement on ρ_A (ρ_B) and ω_x (τ_y).

As shown in Ref. [1], J is linearly proportional to the conventional witness when the measurement is projecting onto the maximally entangled state $|\Phi_{AA}^+\rangle = 1/\sqrt{d_A}\sum_i |ii\rangle$ and $|\Phi_{BB}^+\rangle = 1/\sqrt{d_B}\sum_j |jj\rangle$, $J = \mathrm{Tr}[W\rho_{AB}]/d_A d_B$. Thus, J defined in Eq. (1) witnesses

*yuanxiao12@mails.tsinghua.edu.cn

†xma@tsinghua.edu.cn

entanglement. Furthermore, it can be proved that such a witness is independent of the measurement devices.

3 Robust MDIEW

Now, we present a method to optimize the MDIEW given a fixed observed experiment data $p(1,1|\omega_x,\tau_y)$.

Problem (formal): For a given probability distribution $p(1,1|\omega_x,\tau_y)$*, minimize*

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x,\tau_y) \tag{2}$$

over all $\beta^{x,y}$ *satisfying* $\sum_{x,y} \beta^{x,y} \mathrm{Tr}\left[\sigma_{AB}(\omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}})\right] \geq 0$*, for any separable state* σ_{AB} *and* $\mathrm{Tr}\left[\sum_{x,y} \beta^{x,y} \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}}\right] = 1$.

A possible solution to this problem is to try all entanglement witnesses to find the optimal one. However, it is proved that the problem of accurately finding such an optimal witness is NP-hard. Thus, our problem is also intractable for the most general case. The key for the problem being intractable is that there is no efficient way to characterize an arbitrary entanglement witness. In the bipartite case, an operator is an witness if and only if $\mathrm{Tr}[\sigma_{AB} W] \geq 0$ for any separable state σ_{AB}. As σ_{AB} can always be decomposed as a convex combination of separable states as $|\psi\rangle_A |\phi\rangle_B$, the condition can be equivalently expressed as $\langle\psi|_A \langle\phi|_B W |\psi\rangle_A |\phi\rangle_B \geq 0$, for any pure states $|\psi\rangle_A$ and $|\phi\rangle_B$. The constraints for a witness W are very difficult to describe in the most general case, which makes our problem hard.

While, this problem can be resolved if we allow certain failure errors. A Hermitian operator W_ϵ is defined as an ϵ-level entanglement witness, when

$$\mathrm{Prob}\left\{\mathrm{Tr}[\sigma W_\epsilon] < 0 | \sigma \in S\right\} \leq \epsilon, \tag{3}$$

where S is the set of separable states. That is, the operator W_ϵ has a probability less than ϵ to detect a randomly selected separable quantum state to be entangled. Intuitively, ϵ can be regarded as a failure error probability. We refer to Ref. [5] for a rigorous definition. It is shown that the ϵ-level optimal EW can be found efficiently for any given entangled state ρ. In particular, constrained on $\mathrm{Tr}[W_\epsilon] = 1$ and W_ϵ to be an ϵ-level EW, one can run a semi-definite programming (SDP) to minimize $\mathrm{Tr}[W_\epsilon \rho]$.

Following the method proposed in Ref. [5], we can solve the minimization problem given in Eq. (2) by allowing a certain failure probability ϵ. First, we relax the constraints. Instead of requiring being non-negative for all separable states, we randomly generate N separable states $\{|\psi\rangle_A^i |\phi\rangle_B^i\}$ and require that

$$\sum_{x,y} \beta^{x,y} \langle \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}} \rangle^i \geq 0, \forall i \in \{1,2,\ldots,N\}, \tag{4}$$

where $\langle \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}} \rangle^i = \langle\psi|_A^i \langle\phi|_B^i \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}} |\psi\rangle_A^i |\phi\rangle_B^i$. Then the problem can be expressed as

Problem (ϵ*-level): given a probability distribution* $p(1,1|\omega_x,\tau_y)$*, minimize*

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x,\tau_y) \tag{5}$$

over all $\beta^{x,y}$ *satisfying* $\sum_{x,y} \beta^{x,y} \langle \omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}} \rangle^i \geq 0, \forall i \in \{1,2,\ldots,N\}$*, for* N *randomly generated separable states* $\{|\psi\rangle_A^i |\phi\rangle_B^i\}$ *and* $\sum_{x,y} \beta^{x,y} \mathrm{Tr}\left[\omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}}\right] = 1$.

Note that

$$W_B = \langle\psi|_A W_\epsilon |\psi\rangle_A \geq 0, \forall |\psi\rangle_A, \tag{6}$$

where $W_B \geq 0$ indicates that W_B has non-negative eigenvalues. Therefore, we only need to generate N states $|\psi\rangle_A^i$, for $i = 1,2,\ldots,N$, and the problem is

Problem (ϵ*-level, SDP): given a probability distribution* $p(1,1|\omega_x,\tau_y)$*, minimize*

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x,\tau_y) \tag{7}$$

over all $\beta^{x,y}$ *satisfying* $\sum_{x,y} \beta^{x,y} \langle\psi|_A^i \omega_x^{\mathrm{T}} |\psi\rangle_A^i \tau_y^{\mathrm{T}} \geq 0, \forall i \in \{1,2,\ldots,N\}$*, for* N *randomly generated states* $\{|\psi\rangle_A^i\}$ *and* $\sum_{x,y} \beta^{x,y} \mathrm{Tr}\left[\omega_x^{\mathrm{T}} \otimes \tau_y^{\mathrm{T}}\right] = 1$.

Then, we can run an SDP to solve this problem. It is worth to remark that the problem can be similarly solved in the multipartite case.

References

[1] C. Branciard, D. Rosset, Y. C. Liang, N. Gisin. Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States. Phys. Rev. Lett. 110, 060405, 2013.

[2] F. Buscemi. All Entangled Quantum States Are Nonlocal. Phys. Rev. Lett. 108, 200401, 2012.

[3] P. Xu, X. Yuan, L. K. Chen, H. Lu, X. C. Yao, X. Ma, Y. A. Chen, and J. W. Pan. Implementation of a Measurement-Device-Independent Entanglement Witness. Phys. Rev. Lett. 112, 140506, 2014.

[4] X. Yuan, Q. X. Mei, S. Zhou, and X. M. Ma. Reliable and robust entanglement witness. Phys. Rev. A 93, 042317, 2016.

[5] F. G. S. L. Brandão, R. O. Vianna Separable Multipartite Mixed States: Operational Asymptotically Necessary and Sufficient Conditions. Phys. Rev. Lett. 93, 220503, 2014.

Separability of Bosonic States

Nengkun Yu[1 2 3 *]

[1] *Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

[2] *Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada*

[3] *Department of Mathematics & Statistics, University of Guelph, Guelph, Ontario, Canada*

Abstract. The structural relation between multipartite entanglement and symmetry is one of the central mysteries of quantum mechanics. In this paper, we study the separability of quantum states in bosonic system. We show that mixture of multi-qubit Dicke state is separable if and only if its partial transpose is positive semi-definite, which confirms the hypothesis of [Wolfe, Yelin, Phys. Rev. Lett. (2014)]. We generalize this result to a class of bosonic states in $d \otimes d$ system and show that for general d, determine its separability is NP-hard although verifiable conditions for separability is easily derived in case $d = 3, 4$.

Keywords: Bosonic States, Dicke States, Separability, NP-Hard

Quantum entanglement has been regarded as a resource of cryptography and metrology. Therefore, it is a fundamental problem to qualitatively test whether a given state is entangled or not. In multipartite systems, a quantum state is called *fully* separable, not entangled, if it can be written as a statistical mixture of product states. Although it is known to be NP-Hard of testing separability [1], a considerable number of different separability criterions have been discovered (see the references in [4, 3]), including the famous Positive Partial Transpose(PPT) criterion [2]. One widely used tool of detecting entanglement is entanglement witnesses [5, 6]. Another key concept for entanglement detection is symmetry. The k-symmetric extension provides a hierarchy of separability criteria [7, 8, 9, 11, 10], which converges exactly to the set of separable states when k goes to infinity.

Due to the essential role of symmetry played in entanglement theory, it becomes of great interest to study the relation between multipartite entanglement and symmetry, more precisely, the entanglement of bosonic system. For N-qubit bosonic system, a natural basis is N-qubit Dicke states(unormalized),

$$|D_{N,n}\rangle := \binom{N}{n} P_{\text{sym}}\big(|0\rangle^{\otimes n} \otimes |1\rangle^{\otimes N-n}\big),$$

with P_{sym} being the projection onto the Bosonic (fully symmetric) subspace, *i.e.*, $P_{\text{sym}} = \frac{1}{N!}\sum_{\pi\in S_N} U_\pi$, the sum extending over all permutation operators U_π of the N-qubit systems. Dicke states are particularly suitable for the cold atomic systems, where the particle number is usually thousands. Considerable efforts have been devoted to study entanglement of Dicke states, theoretically [12, 13, 14, 15, 16, 17], and experimentally [19, 18, 20, 21]. The separability of bosonic states, especially the role of PPT in the separability of bosonic system, has attracted lot of attention. Eckert *et.al* prove that there is no PPT entanglement in three-qubit bosonic system [12]. After 10 years, the existence of four-qubit bosonic PPT entanglement is demonstrated in Ref. [22]. Particularly, analytical criteria of the separability of mixture of Dicke states(MDS) is highly desired, and has been pursued extensively [23, 24, 25, 26, 27]. For instance, in Ref. [25], Quesada *et.al*. provided the analytical expression for the best separable approximation of MDS by using the idea introduced by Lewenstein *et.al*. in [26]. In Ref. [27], Wolfe and Yelin proposed the hypothesis that MDS is separable if and only if it is PPT, according to their ideas on generating sufficient separability criteria numerically.

In this paper, we confirm the validity of the hypothesis that PPT indicates separability of mixture of Dicke state(MDS). The idea is also generalized to proved that the separability of mixture of bipartite high dimensional Dicke states is NP-complete, although very simple criterion is given when the local dimension is 3 or 4.

More precisely, we provide an analytical necessary and sufficient condition for N-qubit separability of the MDS, which was called diagonal symmetric states in previous literatures [23, 22, 24, 25, 27],

$$\rho = \sum_{n=0}^{N} \chi_n |D_{N,n}\rangle\langle D_{N,n}|.$$

Theorem 1 *The MDS $\rho = \sum_{n=0}^{N} \chi_n |D_{N,n}\rangle\langle D_{N,n}|$ is separable if and only if the following two Hankel Matrices [29] M_0, M_1 are positive semi-definite, i.e.,*

$$M_0 := \begin{pmatrix} \chi_0 & \cdots & \chi_{m_0} \\ \cdots & \cdots & \cdots \\ \chi_{m_0} & \cdots & \chi_{2m_0} \end{pmatrix} \geq 0, \tag{1}$$

$$M_1 := \begin{pmatrix} \chi_1 & \cdots & \chi_{m_1} \\ \cdots & \cdots & \cdots \\ \chi_{m_1} & \cdots & \chi_{2m_1-1} \end{pmatrix} \geq 0, \tag{2}$$

where $m_0 := [\frac{N}{2}]$ and $m_1 := [\frac{N+1}{2}]$.

Theorem 2 *N-qubit MDS $\rho = \sum_{n=0}^{N} \chi_n |D_{N,n}\rangle\langle D_{N,n}|$ is separable if and only if it is PPT. More precisely, ρ is separable if and only if it is PPT under the partial transpose of $m_0 = [\frac{N}{2}]$ subsystems.*

*nengkunyu@gmail.com

These techniques to study the multi-qubit Dicke states can be generalized to study the mixture of higher dimensional bipartite Dicke states,

$$\rho = \sum_{i,j=1}^{d} \chi_{i,j} |\psi_{i,j}\rangle\langle\psi_{i,j}|,$$

with $|\psi_{i,j}\rangle := \begin{cases} |ii\rangle & \text{if } i = j, \\ |ij\rangle + |ji\rangle & \text{otherwise.} \end{cases}$ being some basis of $d \otimes d$ symmetric subspace.

Recall the known hardness result on testing the membership of completely positive matrices in Ref. [28], we have

Theorem 3 *It is NP-Hard to decide whether* $\rho = \sum_{i,j=1}^{d} \chi_{i,j} |\psi_{i,j}\rangle\langle\psi_{i,j}|$ *is separable. On the other hand, for* $d = 3, 4$*, it is separable if and only if* $\chi = (\chi_{ij})_{d\times d}$ *is semi-definite positive.*

In this paper, we study the separability of bosonic state. We prove the validity of the hypothesis of Ref. [27] by demonstrating an analytical condition for the separability of mixture of N-qubit Dicke states. These techniques are also applied on the mixture of $d \otimes d$ Dicke states, and hardness result is showed. We hope that our techniques for certifying entanglement witness and positive polynomials, may prove useful in furthering the understanding of entanglement.

References

[1] L. Gurvits, Journal of Computer and System Sciences, **69**, 3 (2004).

[2] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[3] L.M. Ioannou, Quant. Inf. Comp. **7**, 335 (2007).

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81** 865-942,(2009).

[5] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **283**, 1 (2001).

[6] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[7] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88** 187904,(2002).

[8] M. Christandl, R. Konig, G. Mitchison, and R. Renner, Comm. Math. Phys **273** 473-498,(2007).

[9] G. Chiribella, Lecture Notes in Computer Science **6519** 9-25,(2011).

[10] A. W. Harrow, arXiv preprint arXiv:1308.6595 (2013).

[11] F. G. S. L. Brãndao, and M. Christandl, Phys. Rev. Lett. **109** 160502,(2012).

[12] K. Eckert, J. Schliemann, D. Bruss and M. Lewenstein, Annals of Physics **299**, 88-127 (2002).

[13] N. Yu, Phys. Rev. A **87**, 052310 (2013); N. Yu, E. Chitambar, C. Guo, and R. Duan, Phys. Rev. A **81**, 014301 (2010); N. Yu, C. Guo, and R. Duan, Phys. Rev. Lett **112**, 160401 (2014).

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

[15] R. Hübener, M. Kleinmann, T-C Wei, C. González-Guillén, and O. Gühne, Phys. Rev. A **80**, 032324 (2009).

[16] T. Bastin, S. Krins, P. Mathonet, M. Godefroid, L. Lamata, and E. Solano, Phys. Rev. Lett **103**, 070503 (2009); T. Bastin, C. Thiel, J. vonZanthier, L. Lamata, E. Solano, and G.S. Agarwal, Phys. Rev. Lett. **102**, 053601 (2009).

[17] W. Wieczorek, N. Kiesel, C. Schmid, and H. Weinfurter, Phys. Rev. A **79**, 022311 (2009).

[18] M. Cramer, A. Bernard, N. Fabbri, L. Fallani, C. Fort, S. Rosi, F. Caruso, M. Inguscio and M.B. Plenio, Nature Communications **4**, 2161 (2013).

[19] A.S. Sørensen, and K. Mølmer, Phys. Rev. Lett. **86**, 4431 (2001).

[20] B. Lücke, J. Peise, G. Vitagliano, J. Arlt, L. Santos, G. Tóth, and C. Klempt, Phys. Rev. Lett. **112**, 155304 (2014).

[21] R. McConnell, H. Zhang, J. Hu, S. Ćuk, and V. Vuletić, Nature **519**, 439-442 (2015).

[22] J. Tura, R. Augusiak, P. Hyllus, M. Kus, J. Samsonowicz and M. Lewenstein, Phys. Rev. A **85**, 060302(R) (2012).

[23] G. Tóth and O. Gühne, Applied Physics B **98**, 617 (2009); G. Tóth and O. Gühne, Phys. Rev. Lett **102**, 170503 (2009); O. Gühne and G. Tóth, Physics Reports **474**, 1 (2009).

[24] L. Novo, and T. Moroder, and O. Gühne, Phys. Rev. A **88**, 012305 (2013).

[25] R. Quesada, and A. Sanpera, Phys. Rev. A **89**, 052319 (2014).

[26] M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).

[27] E. Wolfe, S.F. Yelin, Phys. Rev. Lett. **112**, 140402 (2014); E. Wolfe, arXiv:1409.2517(2014);E. Wolfe, S.F. Yelin, arXiv:1405.5288 (2014).

[28] H. Diananda, Mathematical Proceedings of the Cambridge Philosophical Society, **58**, 17 (1961).

[29] J. R. Partington, An Introduction to Hankel Operators,London Mathematical Society Student Texts 13, Cambridge University Press (1988).

A geometric approach to entanglement quantification with polynomial measures

Bartosz Regula[1] * Gerardo Adesso[1] †

[1] *School of Mathematical Sciences, The University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*

Abstract. We show that the entanglement of any rank-2 state quantified with any polynomial measure of entanglement can be expressed as a geometric problem on the corresponding Bloch sphere. This setting provides novel insight into the properties of entanglement and allows us to relate different polynomial measures to each other, simplifying their quantification. In particular, using the geometric structure of the concurrence, we show that the convex roof of any polynomial measure can be quantified exactly for rank-2 states which have only one or two unentangled states in their range. We give explicit examples by quantifying the three-tangle exactly for several representative classes of rank-2 three-qubit states. We also show how this method can be used to obtain analytical results for more complex systems if one can exploit symmetries in their geometry. We provide a direct application of the result by investigating the monogamy relations of multi-qubit systems.

Keywords: entanglement measures, convex roof, entanglement monogamy

1 Introduction

Ever since the use of entanglement was recognised as a useful resource in many quantum information protocols, there has been a consistent effort to develop a comprehensive framework for entanglement quantification [1]. However, the promising results in quantifying bipartite entanglement did not easily generalise to systems of more parties, where even for the three-qubit case we only have analytical results in very few, special cases. In particular, the complex optimisation problems involved in the quantification of multipartite entanglement are a major obstacle to obtaining a full understanding of the properties of entanglement in general.

A particular class of well-studied and often-used measures of entanglement are the *polynomial measures*, such as the concurrence of two qubits, the three-tangle of three qubits, or generalised measures for any number of qubits and qudits. Their quantification for mixed states involves the difficult optimisation problem of evaluating the so-called *convex roof*, that is, minimising the entanglement over all possible pure-state decompositions. While the concurrence of any two-qubit state can be quantified exactly, the framework for quantification of entanglement of more qubits is in its infancy, and exact results have only been obtained in very few, special cases.

In this work [2, 3], we develop a *geometric* approach to understanding and quantifying convex roof-extended polynomial measures of entanglement, establishing a link between geometric and algebraic methods for entanglement quantification. Our approach reveals common relations between different polynomial measures on pure states and allows for a simplification of the problem of evaluating their convex roof on mixed states.

2 Results

Any rank-2 quantum system can be visualised in the well-known graphical representation called the Bloch sphere. We show that for any such state, the quantification of its entanglement corresponds to a geometric problem of measuring distances on the Bloch sphere. This approach allows the entanglement of all rank-2 states to enjoy a convenient visual representation, which considerably simplifies the study and understanding of their properties.

We first investigate the properties of the concurrence, derive its geometric structure in detail (see Fig. 1), and use geometric methods to fully quantify its convex roof. We then show that for all rank-2 states which have only one or two unentangled states in their range (their Bloch sphere), the geometric structure of all polynomial measures of entanglement is identical to that of the concurrence. We call such states *one-root* and *two-root* states, respectively. This result allows us to quantify the convex roof exactly, not just for the concurrence, but also for the three-tangle and for any other polynomial measure of any degree.

Using the geometric approach, we provide ex-

*bartosz.regula@gmail.com

†gerardo.adesso@nottingham.ac.uk

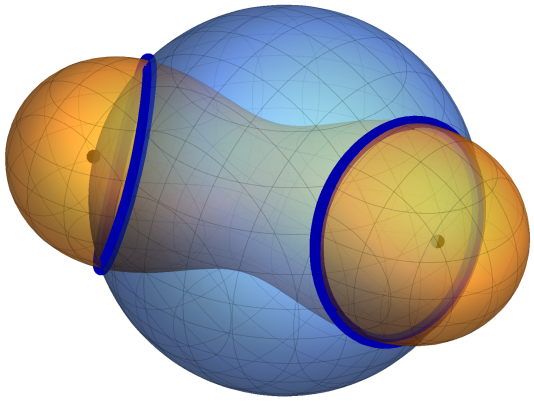


Figure 1: The curves of constant entanglement for the concurrence (or any other polynomial measure in two-root states). The curves obtained as the intersection of the surface with the Bloch sphere show all states with a given value of entanglement.

act, easily computable formulas for the entanglement of all one-root and two-root mixed states. We additionally prove an even stronger geometric result, showing that for all polynomial entanglement measures of degree 2, the entanglement of one-root states does not depend on the chosen convex decomposition and becomes trivial to compute.

Further, we show that several classes of four-qubit states have marginals which are one- or two-root states, meaning that the simplified entanglement properties are a common occurrence among all rank-2 three-qubit systems. We show a direct physical application of the relevant classes of states by investigating the monogamy of entanglement. In particular, we introduce a generalised form of the well-known Coffman-Kundu-Wootters monogamy relation [4] in which we consider multipartite entanglement in addition to the bipartite one, and we show that among four-qubit states this stronger form of monogamy is violated only for a small subset of states. Interestingly, all of the states in the violating subset have one-root marginals, allowing us to quantify exactly the three-partite entanglement in these states [5]. The exact quantification of the convex roof thanks to the simplified properties of one-root states is therefore crucial to understanding monogamy relations in systems of many qubits, proving the relevance of the geometric methods introduced in our work.

Lastly, we show that the geometric approach can be used beyond one- and two-root states, employing the case of the mixtures of GHZ and W states as an example. We rederive known results for this class of states [6] in the new approach, justifying its use in a broader range of states and showing that the geometric methods can be extremely helpful if the Bloch sphere of a the considered state enjoys certain symmetries.

3 Discussion

We introduced a geometric approach to characterising and quantifying convex roof-extended polynomial measures of entanglement, showing a relation between different measures and allowing for a simplification of the problem of quantifying their convex roof. While geometric methods have been employed in the study of entanglement, their application to quantifying polynomial measures of entanglement has not been explored before. We showed that this approach provides novel insight into the structure of entanglement for rank-2 states, allowing us to derive many simplified properties of such states and quantify their entanglement exactly in many relevant cases of three-qubit states as well as more complex systems.

We investigated the particularly simplified cases of one-root and two-root states, for which we can quantify the convex roof of any polynomial measure exactly. We showed that states of this type, in addition to being crucial in studying the generalised monogamy relations of entanglement, are a common occurrence among quantum states and thus of high importance in quantum information.

Our approach not only provides a convenient visual representation for the properties of entanglement, allowing us to introduce geometric insights and results into the problem of entanglement quantification, but also has immediate applications in the theory of quantum correlations.

References

[1] C. Eltschka and J. Siewert, J. Phys. A: Math. Theor. **47**, 424005 (2014).

[2] B. Regula and G. Adesso, Phys. Rev. Lett. **116**, 070504 (2016).

[3] B. Regula and G. Adesso, (2016), arXiv:1606.06184 [quant-ph] .

[4] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[5] B. Regula, A. Osterloh, and G. Adesso, Phys. Rev. A **93**, 052338 (2016).

[6] R. Lohmayer, A. Osterloh, J. Siewert, and A. Uhlmann, Phys. Rev. Lett. **97**, 260502 (2006).

An Improved Semidefinite Programming Upper Bound on Distillable Entanglement and Nonadditivity of Rains' Bound

Xin Wang[1] * Runyao Duan[1 2] †

[1] *Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), NSW 2007, Australia*

[2] *UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

Abstract. A new additive and semidefinite programming (SDP) computable entanglement measure is introduced to upper bound the amount of distillable entanglement in bipartite quantum states by PPT operations. This quantity is always smaller than or equal to the logarithmic negativity, the previously best known SDP bound on distillable entanglement, and the inequality is strict in general. By using similar techniques, a succinct SDP characterization of the one-copy PPT-assisted deterministic distillation rate for any bipartite state is also obtained. We also resolve two open problems in entanglement theory by showing that the Rains' bound is neither additive nor equal to the asymptotic relative entropy of entanglement. Finally, we introduce an SDP quantity not only to lower bound the entanglement cost of general bipartite states, but also to upper bound the PPT-assisted deterministic distillation rate.

Keywords: distillable entanglement, entanglement measure, entanglement cost, Rains' bound

Introduction One basic entanglement measure is the entanglement of distillation, denoted by E_D, which characterizes the rate at which one can obtain maximally entangled states from an entangled state by local operations and classical communication (LOCC) [1, 2]. Entanglement cost E_C [1, 3] is another fundamental measure in entanglement theory, which quantifies the rate for converting maximally entangled states to the given state by LOCC. Since both distillable entanglement and the entanglement cost are important but difficult to compute [4], it is of great importance to find the best approach to efficiently evaluate them.

Improved SDP upper bound on distillable entanglement The logrithmic negativity of a quantum state ρ_{AB} is given by $E_N(\rho_{AB}) := \log_2 \min \|\rho_{AB}^{T_B}\|_1$ [5, 6] . We now introduce a new SDP quantity E_W as follows:

$$E_W(\rho_{AB}) = \log_2 \min \|X_{AB}^{T_B}\|_1, \quad \text{s.t.} \quad X_{AB} \geq \rho_{AB}.$$

Theorem 1 *The function $E_W(\cdot)$ has the following properties:*

i) ***Additivity*** *under tensor product: $E_W(\rho_{AB} \otimes \sigma_{A'B'}) = E_W(\rho_{AB}) + E_W(\sigma_{A'B'})$.*

ii) ***Upper bound on PPT distillable entanglement****: $E_\Gamma(\rho_{AB}) \leq E_W(\rho_{AB})$.*

iii) ***Detecting*** *genuine PPT distillable entanglement: $E_W(\rho_{AB}) > 0$ if and only if ρ_{AB} is PPT distillable.*

iv) ***Entanglement monotone under PPT operations****: $E_W(\Lambda(\rho_{AB})) \leq W(\rho_{AB})$ for any $\Lambda \in$ LOCC (and PPT).*

v) ***Improved bound over logarithmic negativity****: $E_W(\rho_{AB}) \leq E_N(\rho_{AB})$, and the inequality can be strict.*

It is worth pointing out that E_N has all properties i) to iv). In particular, for $\rho_{AB}^{(\alpha)} = \sum_{m=0}^{2} |\psi_m\rangle\langle\psi_m|/3$ $(0 < \alpha \leq 0.5)$ with $|\psi_0\rangle = \sqrt{\alpha}|01\rangle + \sqrt{1-\alpha}|10\rangle$, $|\psi_1\rangle = \sqrt{\alpha}|02\rangle + \sqrt{1-\alpha}|20\rangle$, and $|\psi_2\rangle = \sqrt{\alpha}|12\rangle + \sqrt{1-\alpha}|21\rangle$, we have $E_W(\rho_{AB}^{(\alpha)}) < E_N(\rho_{AB}^{(\alpha)})$.

Nonadditivity of Rains' bound The Rains' bound is arguably the best known upper bound of distillable entanglement [7]. As it is is proved to be equal to the asymptotic relative entropy of entanglement for Werner states [8] and orthogonally invariant states [9], one open problem is whether these two quantities always coincide. Another open problem is whether Rains' bound is additive [9].

We resolve the above two open problems by introducing a class of two-qubit states ρ_r whose clos-

*xin.wang-8@student.uts.edu.au

†runyao.duan@uts.edu.au

est separable states can be derived by the result in Ref. [10]. Thus, the Rains' bound of ρ_r is exactly given. Then we apply the algorithm in Refs. [11, 12] to demonstrate the gap between $R(\rho_r^{\otimes 2})$ and $2R(\rho_r)$. The example is $\rho_r = \frac{1}{8}|00\rangle\langle 00| + x|01\rangle\langle 01| + \frac{7-8x}{8}|10\rangle\langle 10| + \frac{32r^2-(6+32x)r+10x+1}{4\sqrt{2}}(|01\rangle\langle 10| + |10\rangle\langle 01|)$ with $x = r + \frac{32r^2-10r+1}{256r^2-160r+33} + \frac{(16r-5)y^{-1}}{32\ln(5/8-y)-32\ln(5/8+y)}$, $y = (4r^2 - 5r/2 + 33/64)^{1/2}$.

Theorem 2 *For* $0.45 \leq r \leq 0.548$, *we have* $R(\rho_{r_0})^{\otimes 2} < 2R(\rho_{r_0})$. *Meanwhile,* $E_R^{\infty}(\rho_{r_0}) < R(\rho_{r_0})$.

It is now reasonable to define the asymptotic Rains' bound, i.e., $R^{\infty}(\rho) = \inf_{n\geq 1} \frac{1}{n} R(\rho^{\otimes n})$. Clearly R^{∞} would be a better upper bound for the distillable entanglement. How to evaluate this quantity remains open.

Deterministic distillation rate The deterministic entanglement distillation concerns about how to distill maximally entangled states exactly. The one-copy PPT-assisted deterministic distillation rate can be formalized as an SDP.

Theorem 3 *For bipartite state* ρ_{AB},

$$\begin{aligned} E_{\Gamma,0}^{(1)}(\rho_{AB}) = &\max_R -\log_2 \|R_{AB}^{T_B}\|_{\infty}, \\ &s.t.\ P_{AB} \leq R_{AB} \leq \mathbb{1}_{AB}, \end{aligned} \tag{1}$$

where P_{AB} *is the projection onto* $\mathrm{supp}(\rho_{AB})$. *And the asymptotic rate is given by* $E_{\Gamma,0}(\rho) := \sup_{n\geq 1} E_{\Gamma,0}^{(1)}(\rho^{\otimes n})/n = \lim_{n\geq 1} E_{\Gamma,0}^{(1)}(\rho^{\otimes n})/n$.

For a bipartite quantum state ρ_{AB}, we define

$$\begin{aligned} E_M(\rho_{AB}) = &-\log_2 \max \mathrm{Tr}\, P_{AB} V_{AB}, \\ &\text{s.t. } \mathrm{Tr}\,|V_{AB}^{T_B}| = 1, V_{AB} \geq 0. \end{aligned} \tag{2}$$

We further show that $E_M(\rho)$ is not only the upper bound of the deterministic distillation rate of ρ, but also a lower bound for the asymptotic Rains' bound.

Theorem 4 *For any bipartite state* ρ, $E_{\Gamma,0}(\rho) \leq E_M(\rho) \leq R^{\infty}(\rho) \leq E_C(\rho)$.

The last inequality is from Ref. [13]. Interestingly, E_M also gives the PPT-assisted deterministic distillation rate for many special cases.

Conclusions We present a new and improved SDP upper bound E_W to the distillable entanglement. This quantity enjoys additional nice properties such as additivity under tensor product and monotonicity under both LOCC and PPT operations. Furthermore, we show that the Rains' bound is neither additive nor equal to the asymptotic relative entropy of entanglement by constructing a class of two-qubit states. We also introduce the asymptotic Rains' bound and give an SDP lower bound E_M for it, which provides an efficiently computable lower bound for the entanglement cost of general bipartite states for the first time. Finally, we provide a refined SDP for the one-copy PPT-assisted distillation rate and show that E_M is the best upper bound for the asymptotic rate. Proof details of our main results can be found in arxivs: 1601.07940 and 1605.00348.

We were grateful to A. Winter, Y. Huang, M. Tomamichel for helpful suggestions and M. Plenio and J. Eisert for communicating references to us. This work was partly supported by the Australian Research Council (Grant Nos. DP120103776 and FT120100449).

References

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

[2] E. M. Rains, *Phys. Rev. A* **60**, 173 (1999).

[3] P. M. Hayden, M. Horodecki, and B. M. Terhal, *J. Phys. A. Math. Gen.* **34**, 6891 (2001).

[4] Y. Huang, *New J. Phys.*, **16**, 33027 (2014).

[5] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).

[6] M. B. Plenio, *Phys. Rev. Lett.* **95**, 090503 (2005).

[7] E. M. Rains, *IEEE Trans. Inf. Theory* **47**, 2921 (2001).

[8] K. Audenaert et al, *Phys. Rev. Lett.* **87**, 217902 (2001).

[9] K. Audenaert, B. De Moor, K. G. H. Vollbrecht, and R. F. Werner, *Phys. Rev. A* **66**, 32310 (2002).

[10] A. Miranowicz and S. Ishizaka, *Phys. Rev. A* **78**, 32310 (2008).

[11] Y. Zinchenko, S. Friedland, and G. Gour, *Phys. Rev. A* **82**, 52336 (2010).

[12] M. W. Girard, Y. Zinchenko, S. Friedland, and G. Gour, *Phys. Rev. A* **91**, 29901 (2015).

[13] M. Hayashi, Quantum Information (Springer, 2006).

Extendability, complete extendability and a measure of entanglement for Gaussian states

B. V. Rajarama Bhat[1] * K. R. Parthasarathy[2] † Ritabrata Sengupta[2] ‡

[1] *Theoretical Statistics and Mathematics Unit, Indian Statistical Institute, Bengalore Centre, 8th Mile, Mysore Road RVCE Post, Bangalore 560 059, India*

[2] *Theoretical Statistics and Mathematics Unit, Indian Statistical Institute, Delhi Centre, 7 S J S Sansanwal Marg, New Delhi 110 016, India*

Abstract. Motivated by the notions of k-extendability and complete extendability of the state of a finite level quantum system as described by Doherty et al (Phys. Rev. A, 69:022308), we introduce parallel definitions in the context of Gaussian states and using only properties of their covariance matrices derive necessary and sufficient conditions for their complete extendability. It turns out that the complete extendability property is equivalent to the separability property of a bipartite Gaussian state. We also give proof for this in general bipartite quantum states (need not be of finite dimensions). We further show that maximum extendability number can be used as a measure of entanglement for Gaussian states.

Following the proof of quantum de Finetti theorem as outlined in Hudson and Moody (Z. Wahrscheinlichkeitstheorie und Verw. Gebiete, 33(4):343–351), we show that separability is equivalent to complete extendability for a state in a bipartite Hilbert space where at least one of which is of dimension greater than 2. This, in particular, extends the result of Fannes, Lewis, and Verbeure (Lett. Math. Phys. 15(3): 255–260) to the case of an infinite dimensional Hilbert space whose C* algebra of all bounded operators is not separable.

Keywords: Gaussian state, exchangeable Gaussian state, extendability, entanglement, measure of entanglement.

1 Introduction

One of the most important problems in quantum mechanics as well as quantum information theory is to determine whether a given bipartite state is separable or entangled [5]. There are several methods in tackling this problem leading to a long list of important publications. A detailed discussion on this topic is available in the survey articles by Horodecki et al [3], and Gühne and Tóth [2]. One such condition which is both necessary and sufficient for separability in finite dimensional product spaces is complete extendability [1].

Definition 1 *Let $k \in \mathbb{N}$. A state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be k-extendable with respect to system B if there is a state $\tilde{\rho} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B^{\otimes k})$ which is invariant under any permutation in $\mathcal{H}_B^{\otimes k}$ and $\rho = \mathrm{Tr}_{\mathcal{H}_B^{\otimes(k-1)}} \tilde{\rho}$, $k \geq 2$.*

A state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be completely extendable if it is k-extendable for all $k \in \mathbb{N}$.

The following theorem of Doherty, Parrilo, and Spedalieri [1] emphasizes the importance of the notion of complete extendability.

Theorem A:[1] A bipartite state $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable if and only if it is completely extendable with respect to one of its subsystems.

In this paper we have introduced concept of extendability of Gaussian states. We have further shown that any state in a bipartite Fock space is extendable if and only if it is separable. We have reduced these conditions in terms of simple matrix inequalities which in principle can be solved by computer programmes.

2 Gaussian extendability

Definition 2 (Gaussian extendability) *Let $k \in \mathbb{N}$. A Gaussian state ρ_g in $\Gamma(\mathbb{C}^m) \otimes \Gamma(\mathbb{C}^n)$ is said to be Gaussian k-extendable with respect to the second system if there is a Gaussian state $\tilde{\rho_g}$ in $\Gamma(\mathbb{C}^m) \otimes \Gamma(\mathbb{C}^n)^{\otimes k}$ which is invariant under any permutation in $\Gamma(\mathbb{C}^n)^{\otimes k}$ and $\rho_g = \mathrm{Tr}_{\Gamma(\mathbb{C}^n)^{\otimes(k-1)}} \tilde{\rho_g}$, $k \geq 2$.*

A Gaussian state ρ_g in $\Gamma(\mathbb{C}^m) \otimes \Gamma(\mathbb{C}^n)$ is said to be Gaussian completely extendable if it is Gaussian k-extendable for every $k \in \mathbb{N}$.

Theorem 3 *Let ρ be a bipartite Gaussian state in $\Gamma(\mathbb{C}^m) \otimes \Gamma(\mathbb{C}^n)$ with covariance matrix $S = \begin{bmatrix} A & B \\ B^T & C \end{bmatrix}$, where A and C are marginal covariance matrices of the first and second system respectively. Then ρ is completely extendable with respect to the second system if and only if there exists a real positive matrix θ such that*

$$C + \frac{\imath}{2} J_{2n} \geq \theta \geq B^T \left(A + \frac{\imath}{2} J_{2m} \right)^{-} B, \qquad (1)$$

where $\left(A + \frac{\imath}{2} J_{2m}\right)^{-}$ is the Moore-Penrose inverse of $A + \frac{\imath}{2} J_{2m}$.

Theorem 4 *Any separable Gaussian state in a bipartite system is completely extendable.*

*bhat@isibang.ac.in

†krp@isid.ac.in

‡rb@isid.ac.in

Theorem 5 *Any two-mode quantum Gaussian state ρ is completely extendable if and only if it is separable.*

Theorem 6 *If a state ρ (not necessarily Gaussian) on a bipartite Fock space is completely extendable, then it is separable.*

3 Complete extendability and separability in general case

Consider a separable Hilbert space $\mathfrak{h}$ and denote $\mathcal{B} = \mathcal{B}(\mathfrak{h})$ the C* algebra of all bounded operators on $\mathfrak{h}$. Let $\mathcal{B}_n = \mathcal{B}(\mathfrak{h}^{\otimes n}) = \mathcal{B}^{\otimes n}$ be the n-fold tensor product of copies of $\mathcal{B}$. Let $\mathcal{B}^\infty$ be the C* inductive limit of $\mathcal{B}_n$ and $\mathfrak{S}$ denote the set of all states in $\mathcal{B}^\infty$ equipped with the weak* topology. Then $\mathfrak{S}$ is a compact convex set. For any $\omega \in \mathfrak{S}$, define

$$\omega_n(X) = \omega(i_n(X)), \quad X \in \mathcal{B}_n.$$

Then ω_n is a state in $\mathcal{B}_n$ for all n and

$$\omega_{n-1}(X) = \omega_n(X \otimes I), \quad \forall X \in \mathcal{B}_{n-1},\, n = 2, 3, \cdots .$$

in other words $\{\omega_n\}$ is a consistent family of states in $\{\mathcal{B}_n\}$, $n = 2, 3, \cdots$ with the projective limit ω.

Conversely, let ω_n be a state in $\mathcal{B}_n$ for each $n = 1, 2, 3, \cdots$ such that $\omega_n(X \otimes I) = \omega_{n-1}(X \otimes I)$, $\forall X \in \mathcal{B}_{n-1}$, $n = 2, 3, \cdots$. Then there exists a unique state ω in $\mathcal{B}^\infty$ such that

$$\omega(i_n(X)) = \omega_n(X), \quad \forall X \in \mathcal{B}_n,\, n = 1, 2, 3, \cdots .$$

Definition 7 *A state ω in $\mathcal{B}^\infty$ is said to be* locally normal *if each ω_n in $\mathcal{B}_n$, $n = 1, 2, \cdots$ is determined by a density operator ρ_n, $n = 1, 2, \cdots$, i.e., a positive operator ρ_n of unit trace in $\mathfrak{h}^{\otimes n}$ satisfying*

$$\omega_n(X) = \operatorname{Tr} \rho_n X, \quad X \in \mathcal{B}_n,\, n = 1, 2, \cdots .$$

Then the relative trace of ρ_n in $\mathfrak{h}^{\otimes n}$ over the last copy of $\mathfrak{h}$ is equal to ρ_{n-1} for each $n = 2, 3, \cdots$.

Definition 8 *A state in $\mathcal{B}^\infty$ is said to be* exchangeable *if for any permutation π of $\{1, 2, \cdots, n\}$ and operators $X_j \in \mathcal{B}$, $i = 1, 2, \cdots, n$*

$$\begin{aligned} & \omega_n(X_{\pi(1)} \otimes X_{\pi(2)} \otimes \cdots \otimes X_{\pi(n)}) \\ = \;& \omega_n(X_1 \otimes X_2 \otimes \cdots \otimes X_n) \\ = \;& \omega(i_n(X_1 \otimes X_2 \otimes \cdots \otimes X_n)). \end{aligned}$$

We shall now describe a version of quantum de Finetti theorem due to Hudson and Moody [4] (see also Størmer [6] for an abstract C* algebraic version) which we shall make use of in our analysis of complete extendability - separability problem. To this end denote by $\mathcal{R}_\mathfrak{h}$ the set of all density operators on $\mathfrak{h}$. Viewing $\mathcal{R}_\mathfrak{h}$ as a subset of the dual of $\mathcal{B} = \mathcal{B}_\mathfrak{h}$, equip it with the relative topology inherited from the weak* topology. Let $\mathcal{P}_\mathfrak{h}$ denote the set of all probability measures on the Borel σ-algebra of $\mathcal{R}_\mathfrak{h}$.

Theorem 9 *[Hudson and Moody] A locally normal state ω on $\mathcal{B}^\infty$ is exchangeable if and only if there exists a probability measure P_ω in $\mathcal{P}_\mathfrak{h}$ such that*

$$\omega(i_n(X)) = \int_{\mathcal{R}_\mathfrak{h}} \operatorname{Tr} \rho^{\otimes n} X \, P_\omega(\mathrm{d}\,\rho), \quad \forall X \in \mathcal{B}_n,\, n = 1, 2, \cdots .$$

The correspondence $\omega \to P_\omega$ between the set of locally normal and exchangeable states and the set $\mathcal{P}_\mathfrak{h}$ of probability measures on $\mathcal{R}_\mathfrak{h}$ is bijective.

Remark 1 *Theorem 9 shows that exchanbeability property automatically implies that every finite dimensional projection of ω, namely ω_n, is separable. It is natural to expect that complete extendeability would force separability.*

Theorem 10 *Let $\mathfrak{h}_0$, $\mathfrak{h}$ be Hilbert spaces with $\dim \mathfrak{h}_0 > 2$ and ρ be a density operator in $\mathfrak{h}_0 \otimes \mathfrak{h}$. Let $\mathcal{B}_{n]} = \mathcal{B}(\mathfrak{h}_0 \otimes \mathfrak{h}^{\otimes n})$, $n = 0, 1, 2, \cdots$. Suppose there exist density operators ρ_n in $\mathfrak{h}_0 \otimes \mathfrak{h}^{\otimes n}$, $n = 1, 2, \cdots$ satisfying the following properties:*

1. *$\rho_1 = \rho$ and*

   $$\operatorname{Tr} \rho_n (X \otimes I) = \operatorname{Tr} \rho_{n-1} X, \quad X \in \mathcal{B}_{n]},$$

   I being the identity in $\mathfrak{h}$, $n = 1, 2, \cdots$.

2. *For any $X_0 \in \mathcal{B}(\mathfrak{h}_0)$, $Y_j \in \mathcal{B}(\mathfrak{h})$, $j = 1, 2, \cdots, n$ and any permutation π of $\{1, 2, \cdots, n\}$*

   $$\operatorname{Tr} \rho_n \, X_0 \otimes Y_1 \otimes \cdots \otimes Y_n = \operatorname{Tr} \rho_n \, X_0 \otimes Y_{\pi(1)} \otimes \cdots \otimes Y_{\pi(n)}.$$

Then ρ is separable in $\mathfrak{h}_0 \otimes \mathfrak{h}$. Furthermore ρ_n is separable in $\mathfrak{h}_0 \otimes \mathfrak{h}^{\otimes n}$, $n = 1, 2, \cdots$.

Results of this paper are taken from *http://arxiv.org/abs/1601.02365. The last theorem will be posted soon in a separate preprint.*

References

[1] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. Phys. Rev. A*, 69:022308, Feb 2004.*

[2] Otfried Gühne and Géza Tóth. Entanglement detection. Phys. Rep.*, 474(1-6):1–75, 2009.*

[3] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. Rev. Mod. Phys.*, 81(2):865–942, Jun 2009.*

[4] R. L. Hudson and G. R. Moody. Locally normal symmetric states and an analogue of de Finetti's theorem. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 33(4):343–351, 1975/76.*

[5] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition, 2010. Cambridge Books Online.*

[6] Erling Størmer. Symmetric states of infinite tensor products of C-algebras.* J. Functional Analysis*, 3:48–68, 1969.*

A lower bound on expected communication cost of quantum state redistribution

Anurag Anshu
Centre for Quantum Technologies,
National University of Singapore
a0109169@u.nus.edu

June 8, 2016

1 Introduction

Compression of information is a central concept in information theory, originating in the pioneering work of Shannon [Sha]. Shannon showed that in *asymptotic and i.i.d.* setting, compression of messages upto the *Shannon entropy* of the source could be achieved with arbitrarily small error. This result was soon extended to the one-shot setting by Huffman [Huf52], who gave a zero error coding scheme, now known as the Huffman coding scheme, that achieved a compression of *expected length* of the message upto Shannon entropy of the source.

The notion of expected length of the message was further explored in the work by [HJMR10]. They considered the following task: Alice and Bob know a joint distribution $p(x, y)$. Alice is given an input x and Bob needs to output the conditional distribution $p(y|x)$. They gave a nearly tight characterization of the communication requirement of this task in terms of the *mutual information* ($\mathrm{I}(X : Y)$), showing that the *expected communication cost* for this task is upper bounded by $\mathrm{I}(X : Y) + 2\log \mathrm{I}(X : Y) + \mathcal{O}(1)$ and lower bounded by $\mathrm{I}(X : Y)$. Their result also gave an operational interpretation to the *relative entropy* through a task where Alice is given a distribution P, both Alice and Bob are given a distribution Q and they need to jointly sample from a distribution P' that satisfies $\|P' - P\|_1 \leq \varepsilon$. In the work [BR11], the task was simplified to the case where only Bob knows Q and the authors gave an interactive protocol with expected communication cost $\mathrm{D}(P\|Q) + \sqrt{\mathrm{D}(P\|Q)} + \mathcal{O}(\log \frac{1}{\varepsilon})$. Not only did these results give elegant operational interpretation to fundamental information theoretic quantities in one-shot setting, they also had implications for direct sum results in communication complexity. Following theorem was shown in [BR11] (with analogous result for product input distribution shown earlier in [HJMR10]):

Theorem 1.1 (Corollary 2.5, Braverman and Rao [BR11]; see also Result 3, [HJMR10])**.** *Let C be the communication complexity of the best protocol for computing a relation f with error δ on inputs drawn from a distribution μ. Then any r round protocol computing $f^{\otimes n}$ on the distribution $\mu^{\otimes n}$ with error $\delta - \varepsilon$ must involve at least $\Omega(n(C - r \cdot \log(\frac{1}{\varepsilon}) - O(\sqrt{C \cdot r})))$ communication.*

In quantum information theory, two-party communication protocols are typically of two kinds: non-coherent protocols and coherent protocols. In non-coherent protocols, a well known example

of which is the Schumacher compression [Sch95], the parties do not need to maintain a quantum correlation with the Referee. There are various one-shot protocols that are formulated in non-coherent setting and also have applications for direct sum results in one-way quantum communication complexity ([JRS05, JRS08, AJM+14]).

In the case of coherent protocols, the parties are required to maintain a quantum correlation with the Referee. This is seen, for example, in the case of Quantum state merging [HOW07], where Alice (A), Bob (B) and Referee (R) share a pure tripartite quantum state Ψ_{RAB} and Alice needs to send her register A to Bob (with the aid of shared entanglement) such that the final state between Referee and Bob is $\Psi_{RA'B}$ (where register $A' \equiv A$ held by Bob). A generalization of Quantum state merging is the task of Quantum state redistribution, which very nicely captures the round by round interaction of quantum communication protocols.

Quantum state redistribution : A pure state Ψ_{RBCA} is shared between Alice (A,C), Bob(B) and Referee(R). For a given $\varepsilon > 0$, which we shall henceforth identify as 'error', Alice needs to transfer the system C to Bob, such that the final state Ψ'_{RBC_0A} (where register $C_0 \equiv C$ is with Bob), satisfies $\mathrm{P}(\Psi'_{RBC_0A}, \Psi_{RBC_0A}) \leq \varepsilon$. Here, $\mathrm{P}(.,.)$ is the purified distance.

This task has been well studied in literature in asymptotic setting ([DY08, Opp08, YBW08, YD09]), giving an operational interpretation to the quantum conditional mutual information (denoted as $\mathrm{I}(R:C|B)_\Psi$), and more recently in one shot-setting ([DHO16, BCT16, AJD14]). It has been used by Touchette [Tou15] as a natural framework to define the notion of *quantum information complexity* (inspired by the notion of *Information complexity*, formally introduced in [Bra12]), with application to direct sum result in bounded-round entanglement assisted quantum communication complexity. Following is the main theorem in [Tou15]:

Theorem 1.2 (Touchette [Tou15], Theorem 3)**.** *Let C be the quantum communication complexity of the best entanglement assisted protocol for computing a relation f with error δ on inputs drawn from a distribution μ. Then any r round entanglement assisted protocol computing $f^{\otimes n}$ on the distribution $\mu^{\otimes n}$ with error $\delta - \varepsilon$ must involve at least $\Omega(n((\frac{\varepsilon}{r})^2 \cdot C - r))$ quantum communication.*

This theorem uses the one-shot upper bound of $\mathcal{O}(\frac{\mathrm{I}(R:C|B)_\Psi}{\varepsilon^2})$ on worst case quantum communication cost for Quantum state redistribution (as obtained in [Tou15] using the one-shot results in [BCT16]), which leads to a stronger dependence on the number of rounds, in comparision to Theorem 1.1. A natural way to improve upon the theorem is to consider the expected communication cost of Quantum state redistribution.

Our results

In this work, we study the expected communication cost of Quantum state redistribution; taking inspiration from the elegant one-shot operational interpretations of fundamental information theoretic quantities provided in [Huf52],[HJMR10] and [BR11], and to explore the possibility of improvement of Theorem 1.2. We find that, in contrast to the classical case, the expected communication cost is not much better than the worst case communication cost. Our main theorem is the following.

Theorem 1.3. *Fix a $p < 1$ and an $\varepsilon \in [0, (\frac{1}{70})^{\frac{4}{1-p}}]$. There exists a pure state Ψ_{RBCA} (that depends on ε) such that, any interactive entanglement assisted communication protocol for its quantum state redistribution with error ε requires expected communication cost at least $\mathrm{I}(R:C|B)_\Psi \cdot (\frac{1}{\varepsilon})^p$.*

For the special case where registers A, B are absent, which is also known as Quantum state transfer and is the one-shot coherent analogue of Schumacher compression [Sch95], we obtain a similar result with slightly better constants.

Theorem 1.4. *Fix a $p < 1$ and any $\varepsilon \in [0, (\frac{1}{2})^{\frac{15}{1-p}}]$. There exists a pure state Ψ_{RC} (that depends on ε) such that, any interactive entanglement assisted communication protocol for its quantum state transfer with error ε requires expected communication cost at least $S(\Psi_R) \cdot (\frac{1}{\varepsilon})^p$.*

Note that Theorem 1.4 in itself is sufficient to given a lower bound on expected communication cost of Quantum state redistribution, as Quantum state transfer is a special case. But the state Ψ_{RBCA} that we consider in Theorem 1.3 has all registers R, A, B, C non-trivial and correlated with each other. Thus, Quantum state redistribution of Ψ_{RBCA} cannot be reduced to the sub-case of Quantum state transfer by any local operation, giving robustness to the bound.

A result similar to Theorem 1.4, but in the context of non-coherent quantum protocols, has been obtained recently in [AGHY16]. This can be viewed as a complementary work in the following sense: on one hand, it is stronger since non-coherent quantum protocols are less restrictive that coherent quantum protocols. On the other hand, it is weaker due to the presence of round dependence (Theorem 1.2, [AGHY16]) and error that depends on input size (Theorem 1.3, [AGHY16]), none of which are present in Theorem 1.4. Moreover, this work does not provide an analogue of Theorem 1.3.

Our technique and organization

We discuss our technique for the case of Quantum state transfer, for simplicity. For some $\beta > 1$, we choose the pure state Ψ_{RC} in such a way that its smallest eigenvalue is $\frac{1}{d\beta}$ and entropy of Ψ_R is at most $\frac{2\log(d)}{\beta}$ (d being dimension of register R, see Lemma A.15). Let ω_{RC} be a maximally entangled state defined as $|\omega\rangle_{RC} = \frac{\Psi_R^{-\frac{1}{2}}}{\sqrt{d}} |\Psi\rangle_{RC}$. For any interactive protocol $\mathcal{P}$ for quantum state transfer of Ψ_{RC} with error ε and expected communication cost C (formally described in Appendix B), we obtain an expression that serves as a *transcript* of the protocol, encoding the unitaries applied by Alice and Bob and the probabilities of measurement outcomes (Corollary B.5, see also Lemma B.3). This expression takes ideas from the technique of *convex-split*, introduced in [AJD14], for one-way Quantum state redistribution protocols.

Then, crucially relying on the facts that Ψ_{RC} is a pure state and the register R is untouched by the protocol (which allows the operation $\rho \to \Psi_R^{-\frac{1}{2}} \rho \Psi_R^{-\frac{1}{2}}$ to be performed on the register R, see Lemmas C.3 and C.4), we construct a new interactive protocol $\mathcal{P}'$ which achieves quantum state transfer of the state ω_{RC} with error $\sqrt{\beta\varepsilon} + \sqrt{\mu}$ (for any $\mu < 1$) and worst case quantum communication cost at most $\frac{C}{\mu}$ (Lemmas C.5 and C.6). Suitably choosing the parameters ε, β and μ and using known lower bound on worst case communication cost for state transfer of ω_{RC}, we obtain the desired result. Same technique also extends to quantum state redistribution. Details appear in Appendix C (and can also be found in the arXiv version [Ans15])

Some questions related to our work are as follows.

1. What are some applications of Theorems 1.3 and 1.4 in quantum information theory? An immediate application is that we obtain a lower bound on worst case communication cost of Quantum state redistribution, since worst case communication cost is always larger than expected communication cost of a protocol.

2. Is it possible to improve the direct sum result for entanglement assisted quantum information complexity obtained in [Tou15]? The work [AGHY16] provides yet another limitation to such an improvement. But it may be possible to compress the whole protocol, rather than round-by-round compression, along the lines similar to [BBCR10].

Acknowledgment

I thank Rahul Jain for many valuable discussions and comments on arguments in the manuscript. I also thank Dave Touchette, Penghui Yao and Venkatesh Srinivasan for helpful discussions.

This work is supported by the Core Grants of the Center for Quantum Technologies (CQT), Singapore.

References

[AGHY16] Anurag Anshu, Ankit Garg, Aram Harrow, and Penghui Yao. Lower bound on expected communication cost of quantum huffman coding. 2016. http://arxiv.org/abs/1605.04601.

[AJD14] Anurag Anshu, Rahul Jain, and Vamsi Devabathini. Near optimal bounds on quantum communication complexity of single-shot quantum state redistribution. 2014. http://arxiv.org/abs/1410.3031.

[AJM+14] Anurag Anshu, Rahul Jain, Priyanka Mukhopadhyay, Ala Shayeghi, and Penghui Yao. A new operational interpretation of relative entropy and trace distance between quantum states. http://arxiv.org/abs/1404.1366, 2014.

[AL70] Huzihiro Araki and Elliott H. Lieb. Entropy inequalities. *Communications in Mathematical Physics*, 18:160–170, 1970.

[Ans15] Anurag Anshu. A lower bound on expected communication cost of quantum state redistribution. http://arxiv.org/abs/1506.06380, 2015.

[BBCR10] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. In *Proceedings of the forty-second ACM symposium on Theory of computing*, STOC '10, pages 67–76, New York, NY, USA, 2010. ACM.

[BCF+96] Howard Barnum, Carlton M. Cave, Christopher A. Fuch, Richard Jozsa, and Benjamin Schmacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76:2818–2821, 1996.

[BCT16] M. Berta, M. Christandl, and D. Touchette. Smooth entropy bounds on one-shot quantum state redistribution. *IEEE Transactions on Information Theory*, 62(3):1425–1439, March 2016.

[BR11] Mark Braverman and Anup Rao. Information equals amortized communication. In *Proceedings of the 52nd Symposium on Foundations of Computer Science*, FOCS '11, pages 748–757, Washington, DC, USA, 2011. IEEE Computer Society.

[Bra12] Mark Braverman. Interactive information complexity. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, STOC '12, pages 505–524, New York, NY, USA, 2012. ACM.

[DHO16] Nilanjana Datta, Min-Hsiu Hsieh, and Jonathan Oppenheim. An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution. *Journal of Mathematical Physics*, 57(5), 2016.

[DY08] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Phys. Rev. Lett.*, 100, 2008.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31:291–294, 1973.

[HJMR10] Prahladh Harsha, Rahul Jain, David Mc.Allester, and Jaikumar Radhakrishnan. The communication complexity of correlation. *IEEE Transcations on Information Theory*, 56:438–449, 2010.

[HOW07] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269:107–136, 2007.

[Huf52] David Huffman. A method for the construction of minimum-redundancy codes. *Proceedings of IRE*, 40(9):1098–1101, 1952.

[JRS05] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Prior entanglement, message compression and privacy in quantum communication. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, Washington, DC, USA, 2005. IEEE Computer Society.

[JRS08] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Optimal direct sum and privacy trade-off results for quantum and classical communication complexity. http://arxiv.org/abs/0807.1267, 2008.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40:147–151, 1975.

[Opp08] Jonathan Oppenheim. State redistribution as merging: introducing the coherent relay. http://arxiv.org/abs/0805.1065, 2008.

[Sch95] Benjamin Schumacher. Quantum coding. *Phys. Rev. A.*, 51:2738–2747, 1995.

[Sha] Claude Elwood Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423.

[Tom12] Marco Tomamichel. A framework for non-asymptotic quantum information theory, 2012. PhD Thesis, ETH Zurich.

[Tom15] Marco Tomamichel. Quantum information processing with finite resources - mathematical foundations. 2015. http://arxiv.org/abs/1504.00233.

[Tou15] Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC '15, pages 317–326, New York, NY, USA, 2015. ACM.

[Uhl76] A. Uhlmann. The 'transition probability' in the state space of a*-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[Wat11] John Watrous. Theory of Quantum Information, lecture notes, 2011. https://cs.uwaterloo.ca/ watrous/LectureNotes.html.

[YBW08] Ming-Yong Ye, Yan-Kui Bai, and Z. D. Wang. Quantum state redistribution based on a generalized decoupling. *Physical Review A*, 78, 2008.

[YD09] Jon T. Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55:5339–5351, 2009.

A Preliminaries

In this section we present some notations, definitions, facts and lemmas that we will use in our proofs.

Information theory

For a natural number n, let $[n]$ represent the set $\{1, 2, \ldots, n\}$. For a set S, let $|S|$ be the size of S. A *tuple* is a finite collection of positive integers, such as $(i_1, i_2 \ldots i_r)$ for some finite r. We let log represent logarithm to the base 2 and ln represent logarithm to the base e. The ℓ_1 norm of an operator X is $\|X\|_1 \stackrel{\text{def}}{=} \text{Tr}\sqrt{X^\dagger X}$ and ℓ_2 norm is $\|X\|_2 \stackrel{\text{def}}{=} \sqrt{\text{Tr}XX^\dagger}$. A quantum state (or just a state) is a positive semi-definite matrix with trace equal to 1. It is called *pure* if and only if the rank is 1. Let $|\psi\rangle$ be a unit vector. We use ψ to represent the state and also the density matrix $|\psi\rangle\langle\psi|$, associated with $|\psi\rangle$.

A sub-normalized state is a positive semidefinite matrix with trace less than or equal to 1. A *quantum register* A is associated with some Hilbert space $\mathcal{H}_A$. Define $|A| \stackrel{\text{def}}{=} \dim(\mathcal{H}_A)$. We denote by $\mathcal{D}(A)$, the set of quantum states in the Hilbert space $\mathcal{H}_A$ and by $\mathcal{D}_{\leq}(A)$, the set of all subnormalized states on register A. State ρ with subscript A indicates $\rho_A \in \mathcal{D}(A)$.

For two quantum states ρ and σ, $\rho \otimes \sigma$ represents the tensor product (Kronecker product) of ρ and σ. Composition of two registers A and B, denoted AB, is associated with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If two registers A, B are associated with the same Hilbert space, we shall denote it by $A \equiv B$. Let ρ_{AB} be a bipartite quantum state in registers AB. We define

$$\rho_B \stackrel{\text{def}}{=} \text{Tr}_A(\rho_{AB}) \stackrel{\text{def}}{=} \sum_i (\langle i| \otimes \mathbb{1}_B)\rho_{AB}(|i\rangle \otimes \mathbb{1}_B),$$

where $\{|i\rangle\}_i$ is an orthonormal basis for the Hilbert space A and $\mathbb{1}_B$ is the identity matrix in space B. The state ρ_B is referred to as the marginal state of ρ_{AB} in register B. Unless otherwise stated, a missing register from subscript in a state will represent partial trace over that register. A quantum map $\mathcal{E} : A \to B$ is a completely positive and trace preserving (CPTP) linear map

(mapping states from $\mathcal{D}(A)$ to states in $\mathcal{D}(B)$). A completely positive and trace non-increasing linear map $\tilde{\mathcal{E}} : A \to B$ maps quantum states to sub-normalised states. The identity operator in Hilbert space $\mathcal{H}_A$ (and associated register A) is denoted I_A. A *unitary* operator $U_A : \mathcal{H}_A \to \mathcal{H}_A$ is such that $U_A^\dagger U_A = U_A U_A^\dagger = I_A$. An *isometry* $V : \mathcal{H}_A \to \mathcal{H}_B$ is such that $V^\dagger V = I_A$ and $VV^\dagger = I_B$. The set of all unitary operations on register A is denoted by $\mathcal{U}(A)$.

Definition A.1. We shall consider the following information theoretic quantities. Let $\varepsilon \geq 0$.

1. **generalized fidelity** For $\rho, \sigma \in \mathcal{D}_{\leq}(A)$,
$$\mathrm{F}(\rho, \sigma) \stackrel{\text{def}}{=} \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \mathrm{Tr}(\rho))(1 - \mathrm{Tr}(\sigma))}.$$
2. **purified distance** For $\rho, \sigma \in \mathcal{D}_{\leq}(A)$,
$$\mathrm{P}(\rho, \sigma) = \sqrt{1 - \mathrm{F}^2(\rho, \sigma)}.$$
3. **ε-ball** For $\rho_A \in \mathcal{D}(A)$,
$$\mathcal{B}^\varepsilon(\rho_A) \stackrel{\text{def}}{=} \{\rho'_A \in \mathcal{D}(A) | \ \mathrm{P}(\rho_A, \rho'_A) \leq \varepsilon\}.$$
4. **entropy** For $\rho_A \in \mathcal{D}(A)$,
$$\mathrm{H}(A)_\rho \stackrel{\text{def}}{=} -\mathrm{Tr}(\rho_A \log \rho_A).$$
5. **relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$,
$$\mathrm{D}(\rho_A \| \sigma_A) \stackrel{\text{def}}{=} \mathrm{Tr}(\rho_A \log \rho_A) - \mathrm{Tr}(\rho_A \log \sigma_A).$$
6. **max-relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$,
$$\mathrm{D}_{\max}(\rho_A \| \sigma_A) \stackrel{\text{def}}{=} \inf\{\lambda \in \mathbb{R} : 2^\lambda \sigma_A \geq \rho_A\}.$$
7. **mutual information** For $\rho_{AB} \in \mathcal{D}(AB)$,
$$\mathrm{I}(A : B)_\rho \stackrel{\text{def}}{=} \mathrm{D}(\rho_{AB} \| \rho_A \otimes \rho_B) = \mathrm{H}(A)_\rho + \mathrm{H}(B)_\rho - \mathrm{H}(AB)_\rho .$$
8. **conditional mutual information** For $\rho_{ABC} \in \mathcal{D}(ABC)$,
$$\mathrm{I}(A : B|C)_\rho \stackrel{\text{def}}{=} \mathrm{I}(A : BC)_\rho - \mathrm{I}(A : C)_\rho = \mathrm{I}(B : AC)_\rho - \mathrm{I}(B : C)_\rho .$$
9. **max-information** For $\rho_{AB} \in \mathcal{D}(AB)$,
$$\mathrm{I}_{\max}(A : B)_\rho \stackrel{\text{def}}{=} \inf_{\sigma_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma_B) .$$
10. **smooth max-information** For $\rho_{AB} \in \mathcal{D}(AB)$,
$$\mathrm{I}^\varepsilon_{\max}(A : B)_\rho \stackrel{\text{def}}{=} \inf_{\rho' \in \mathcal{B}^\varepsilon(\rho)} \mathrm{I}_{\max}(A : B)_{\rho'} .$$

11. **conditional min-entropy** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{H}_{\min}(A|B)_{\rho} \stackrel{\text{def}}{=} -\inf_{\sigma_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| I_A \otimes \sigma_B) .$$

12. **conditional max-entropy** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{H}_{\max}(A|B)_{\rho_{AB}} \stackrel{\text{def}}{=} -\mathrm{H}_{\min}(A|R)_{\rho_{AR}} ,$$

where ρ_{ABR} is a purification of ρ_{AB} for some system R.

13. **smooth conditional min-entropy** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{H}^{\varepsilon}_{\min}(A|B)_{\rho} \stackrel{\text{def}}{=} \sup_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} \mathrm{H}_{\min}(A|B)_{\rho'} .$$

14. **smooth conditional max-entropy** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{H}^{\varepsilon}_{\max}(A|B)_{\rho} \stackrel{\text{def}}{=} \inf_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} \mathrm{H}_{\max}(A|B)_{\rho'} .$$

We will use the following facts.

Fact A.2 (Triangle inequality for purified distance, [Tom12])**.** For states $\rho^1_A, \rho^2_A, \rho^3_A \in \mathcal{D}(A)$,

$$\mathrm{P}(\rho^1_A, \rho^3_A) \leq \mathrm{P}(\rho^1_A, \rho^2_A) + \mathrm{P}(\rho^2_A, \rho^3_A).$$

Fact A.3 (Purified distance and trace distance, [Tom12], Proposition 3.3)**.** For subnormalized states ρ_1, ρ_2

$$\frac{1}{2}\|\rho_1 - \rho_2\|_1 \leq \mathrm{P}(\rho_1, \rho_2) \leq \sqrt{\|\rho_1 - \rho_2\|_1}.$$

Fact A.4 (Uhlmann's theorem)**.** [[Uhl76]] Let $\rho_A, \sigma_A \in \mathcal{D}(A)$. Let $|\rho\rangle_{AB}$ be a purification of ρ_A and $|\sigma\rangle_{AC}$ be a purification of σ_A. There exists an isometry $V : \mathcal{H}_C \to \mathcal{H}_B$ such that,

$$\mathrm{F}(|\theta\rangle\langle\theta|_{AB}, |\rho\rangle\langle\rho|_{AB}) = \mathrm{F}(\rho_A, \sigma_A),$$

where $|\theta\rangle_{AB} = (I_A \otimes V)|\sigma\rangle_{AC}$.

Fact A.5 (Monotonicity of quantum operations)**.** [[Lin75, BCF+96], [Tom12], Theorem 3.4] For states ρ, σ, and quantum operation $\mathcal{E}(\cdot)$,

$$\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1 \leq \|\rho - \sigma\|_1 , \mathrm{P}(\rho, \sigma) \leq \mathrm{P}(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \text{ and } \mathrm{F}(\rho, \sigma) \leq \mathrm{F}(\mathcal{E}(\rho), \mathcal{E}(\sigma)).$$

In particular, for a trace non-increasing completely positive map $\tilde{\mathcal{E}}(\cdot)$,

$$\mathrm{P}(\rho, \sigma) \leq \mathrm{P}(\tilde{\mathcal{E}}(\rho), \tilde{\mathcal{E}}(\sigma)).$$

Fact A.6 (Join concavity of fidelity)**.** [[Wat11], Proposition 4.7] Given quantum states $\rho_1, \rho_2 \ldots \rho_k, \sigma_1, \sigma_2 \ldots \sigma_k \in \mathcal{D}(A)$ and positive numbers $p_1, p_2 \ldots p_k$ such that $\sum_i p_i = 1$. Then

$$\mathrm{F}(\sum_i p_i \rho_i, \sum_i p_i \sigma_i) \geq \sum_i p_i \mathrm{F}(\rho_i, \sigma_i).$$

Fact A.7. Let $\rho, \sigma \in \mathcal{D}(A)$ be quantum states. Let $\alpha < 1$ be a positive real number. If $\mathrm{P}(\alpha\rho, \alpha\sigma) \leq \varepsilon$, then

$$\mathrm{P}(\rho, \sigma) \leq \varepsilon \sqrt{\frac{2}{\alpha}}.$$

Proof. $\mathrm{P}(\alpha\rho, \alpha\sigma) \leq \varepsilon$ implies $\mathrm{F}(\alpha\rho, \alpha\sigma) \geq \sqrt{1-\varepsilon^2} \geq 1-\varepsilon^2$. But, $\mathrm{F}(\alpha\rho, \alpha\sigma) = \alpha \|\sqrt{\rho}\sqrt{\sigma}\|_1 + (1-\alpha)$. Thus,

$$\mathrm{F}(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1 \geq 1 - \frac{\varepsilon^2}{\alpha}.$$

Thus, $\mathrm{P}(\rho, \sigma) \leq \sqrt{1 - (1 - \frac{\varepsilon^2}{\alpha})^2} \leq \sqrt{\frac{2\varepsilon^2}{\alpha}}$. □

Fact A.8 (Fannes inequality)**.** [[Fan73]] Given quantum states $\rho_1, \rho_2 \in \mathcal{D}(A)$, such that $|A| = d$ and $\mathrm{P}(\rho_1, \rho_2) = \varepsilon \leq \frac{1}{2\mathrm{e}}$,

$$|S(\rho_1) - S(\rho_2)| \leq \varepsilon \log(d) + 1.$$

Fact A.9 (Subadditivity of entropy)**.** [[AL70]] For a quantum state $\rho_{AB} \in \mathcal{D}(AB)$, $|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$.

Fact A.10 (Concavity of entropy)**.** [[Wat11], Theorem 10.9] For quantum states $\rho_1, \rho_2 \ldots \rho_n$, and positive real numbers $\lambda_1, \lambda_2 \ldots \lambda_n$ satisfying $\sum_i \lambda_i = 1$,

$$S(\sum_i \lambda_i \rho_i) \geq \sum_i \lambda_i S(\rho_i).$$

Fact A.11. For a quantum state ρ_{ABC}, it holds that

$$\mathrm{I}(A:C)_\rho \leq 2S(\rho_C),$$

$$\mathrm{I}(A:C|B)_\rho \leq \mathrm{I}(AB:C)_\rho \leq 2S(\rho_C).$$

Proof. From Fact A.9, $\mathrm{I}(A:C)_\rho = S(\rho_A) + S(\rho_C) - S(\rho_{AC}) \leq 2S(\rho_C)$. □

Fact A.12. For a bipartite quantum state ρ_{AB}, $\mathrm{I}^\varepsilon_{\max}(A:B)_\rho \geq -\mathrm{H}^\varepsilon_{\min}(A|B)_\rho$.

Proof. Let σ_B be the state achieved in infimum in the definition of $\mathrm{I}_{\max}(A:B)_\rho$. Let $\lambda \stackrel{\text{def}}{=} \mathrm{I}_{\max}(A:B)_\rho$. Consider,

$$\rho_{AB} \leq 2^\lambda \rho_A \otimes \sigma_B \leq 2^\lambda I_A \otimes \sigma_B.$$

Thus, we have

$$-\mathrm{H}_{\min}(A|B)_\rho = \inf_{\sigma'_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| I_A \otimes \sigma'_B) \leq \mathrm{D}_{\max}(\rho_{AB} \| I_A \otimes \sigma_B) \leq \lambda = \mathrm{I}_{\max}(A:B)_\rho.$$

This gives,

$$\inf_{\rho'_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} - \mathrm{H}_{\min}(A|B)_{\rho'} \leq \mathrm{I}^\varepsilon_{\max}(A:B)_\rho.$$

□

Fact A.13. For a *classical-quantum* state ρ_{AB} of the form $\rho_{AB} = \sum_j p(j) |j\rangle\langle j|_A \otimes \sigma^j_B$, it holds that $\mathrm{I}_{\max}(A:B)_\rho \leq \log(|B|)$.

Proof. By definition, $\mathrm{I}_{\max}(A:B)_\rho \leq \mathrm{D}_{\max}\left(\rho_{AB}\middle\|\rho_A \otimes \frac{\mathrm{I}_B}{|B|}\right)$. Also,

$$\rho_{AB} = \sum_j p(j)\,|j\rangle\langle j|_A \otimes \sigma_B^j \leq |B| \sum_j p(j)\,|j\rangle\langle j|_A \otimes \frac{\mathrm{I}_B}{|B|} = |B|\rho_A \otimes \frac{\mathrm{I}_B}{|B|}.$$

Thus, the fact follows. □

Fact A.14. For a *classical-quantum* state $\rho_{ABC} = \sum_j p(j)\,|j\rangle\langle j|_A \otimes \rho_{BC}^j$, it holds that $\mathrm{I}(AB:C)_\rho \geq \sum_j p(j)\mathrm{I}(B:C)_{\rho^j}$

Proof. Consider,

$$\begin{aligned}
\mathrm{I}(AB:C)_\rho &= S(\rho_{AB}) + S(\rho_C) - S(\rho_{ABC}) \\
&= S(\sum_j p(j)\,|j\rangle\langle j|_A \otimes \rho_B^j) + S(\sum_j p(j)\rho_C^j) - S(\sum_j p(j)\,|j\rangle\langle j|_A \otimes \rho_{BC}^j) \\
&= \sum_j p(j)S(\rho_B^j) + S(\sum_j p(j)\rho_C^j) - \sum_j p(j)S(\rho_{BC}^j) \\
&\geq \sum_j p(j)S(\rho_B^j) + \sum_j p(j)S(\rho_C^j) - \sum_j p(j)S(\rho_{BC}^j) \quad \text{(Fact A.10)} \\
&= \sum_j p(j)\mathrm{I}(B:C)_{\rho^j}
\end{aligned}$$

□

Lemma A.15. *Fix a $\beta \geq 1$ and an integer $d > 1$. There exists a probability distribution $\mu = \{e_1, e_2 \ldots e_d\}$, with $e_1 \geq e_2 \ldots \geq e_d$, such that $e_d = \frac{1}{d\beta}$ and entropy $S(\mu) \leq 2\frac{\log(d)}{\beta}$*

Proof. Set $e_2 = e_3 = \ldots e_d = \frac{1}{d\beta}$. Then $e_1 = 1 - \frac{d-1}{d\beta}$. Using $x\log(\frac{1}{x}) \leq \frac{\log(e)}{e} < 1$ for all $x > 0$, we can upper bound the entropy of the distribution as

$$\sum_i e_i \log(\frac{1}{e_i}) = (1 - \frac{d-1}{d\beta})\log(\frac{1}{1-\frac{d-1}{d\beta}}) + \frac{d-1}{d\beta}\log(d\beta) < 2 + \frac{\log(d)}{\beta} \leq 2\frac{\log(d)}{\beta}.$$

□

B Interactive protocol for quantum state redistribution

In this section, we describe general structure of an interactive protocol for quantum state redistribution and its *expected communication cost*.

Let quantum state $|\Psi\rangle_{RBCA}$ be shared between Alice (A, C), Bob (B) and Referee (R). Alice and Bob have access to shared entanglement $\theta_{E_AE_B}$ in registers E_A (with Alice) and E_B (with Bob). Using quantum teleportation, we can assume without loss of generality that Alice and Bob communicate classical messages, which involves performing a POVM measurement on registers they respectively hold, and sending the outcome of measurement to other party. This allows for the notion of *expected communication cost*.

A r-round interactive protocol $\mathcal{P}$ (where r is an odd number) with error ε and expected communication cost C is as follows (see also Figure 1)

Input: A quantum state $|\Psi\rangle_{RBCA}$, error parameter $\varepsilon < 1$.
Shared entanglement: $|\theta\rangle_{E_A E_B}$.

- Alice performs a measurement $\mathcal{M} = \{M^1_{ACE_A}, M^2_{ACE_A} \ldots\}$. Probability of outcome i_1 is $p_{i_1} \stackrel{\text{def}}{=} \text{Tr}(M^{i_1}_{ACE_A} \Psi_{CA} \otimes \theta_{E_A})$. Let $\phi^{i_1}_{RBACE_A E_B}$ be the global normalized quantum state, conditioned on this outcome. She sends message i_1 to Bob.

- Upon receiving the message i_1 from Alice, Bob performs a measurement

$$\mathcal{M}^{i_1} = \{M^{1,i_1}_{BE_B}, M^{2,i_1}_{BE_B} \ldots\}.$$

  Probability of outcome i_2 is $p_{i_2|i_1} \stackrel{\text{def}}{=} \text{Tr}(M^{i_2,i_1}_{BE_B} \phi^{i_1}_{BE_B})$. Let $\phi^{i_2,i_1}_{RBACE_A E_B}$ be the global normalized quantum state conditioned on this outcome i_2 and previous outcome i_1. Bob sends message i_2 to Alice.

- Consider any odd round $1 < k \leq r$. Let the measurement outcomes in previous rounds be $i_1, i_2 \ldots i_{k-1}$ and global normalized state be $\phi^{i_{k-1}, i_{k-2} \ldots i_1}_{RBACE_A E_B}$. Alice performs the measurement $\mathcal{M}^{i_{k-1}, i_{k-2} \ldots i_2, i_1} = \{M^{1, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{ACE_A}, M^{2, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{ACE_A} \ldots\}$ and obtains outcome i_k with probability $p_{i_k | i_{k-1}, i_{k-2} \ldots i_2, i_1} \stackrel{\text{def}}{=} \text{Tr}(M^{i_k, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{ACE_A} \phi^{i_{k-1}, i_{k-2} \ldots i_1}_{AXE_A})$. Let the global normalized state after outcome i_k be $\phi^{i_k, i_{k-1}, i_{k-2} \ldots i_1}_{RBACE_B E_A}$. Alice sends the outcome i_k to Bob.

- Consider an even round $2 < k \leq r$. Let the measurement outcomes in previous rounds be $i_1, i_2 \ldots i_{k-1}$ and global normalized state be $\phi^{i_{k-1}, i_{k-2} \ldots i_1}_{RBACE_A E_B}$. Bob performs the measurement

$$\mathcal{M}^{i_{k-1}, i_{k-2} \ldots i_2, i_1} = \{M^{1, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{BE_B}, M^{2, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{BE_B} \ldots\}$$

  and obtains outcome i_k with probability

$$p_{i_k | i_{k-1}, i_{k-2} \ldots i_2, i_1} \stackrel{\text{def}}{=} \text{Tr}(M^{i_k, i_{k-1}, i_{k-2} \ldots i_2, i_1}_{BE_B} \phi^{i_{k-1}, i_{k-2} \ldots i_1}_{BE_B}).$$

  Let the global normalized state after outcome i_k be $\phi^{i_k, i_{k-1}, i_{k-2} \ldots i_1}_{RBACE_B E_A}$. Bob sends the outcome i_k to Alice.

- After receiving message i_r from Alice at the end of round r, Bob applies a unitary $U^b_{i_r, i_{r-1} \ldots i_1} : BE_B \to BC_0 T_B$ such that $E_B \equiv C_0 T_B$ and $C_0 \equiv C$. Alice applies a unitary $U^a_{i_r, i_{r-1} \ldots i_1} : ACE_A \to ACE_A$. Let $U_{i_r, i_{r-1} \ldots i_1} \stackrel{\text{def}}{=} U^a_{i_r, i_{r-1} \ldots i_1} \otimes U^b_{i_r, i_{r-1} \ldots i_1}$. Define

$$\left|\tau^{i_r, i_{r-1} \ldots i_1}\right\rangle_{RBACC_0 T_B E_A} \stackrel{\text{def}}{=} U_{i_r, i_{r-1} \ldots i_1} \left|\phi^{i_r, i_{r-1} \ldots i_1}\right\rangle_{RBACE_B E_A}.$$

- For every $k \leq r$, define

$$p_{i_1, i_2 \ldots i_k} \stackrel{\text{def}}{=} p_{i_1} \cdot p_{i_2|i_1} \cdot p_{i_3|i_2, i_1} \cdots p_{i_k | i_{k-1}, i_{k-2} \ldots i_1}.$$

The joint state in registers RBC_0A, after Alice and Bob's final unitaries and averaged over all messages is $\Psi'_{RBC_0A} \stackrel{\text{def}}{=} \sum_{i_r,i_{r-1}\ldots i_1} p_{i_1,i_2\ldots i_r} \tau^{i_r,i_{r-1}\ldots i_1}_{RBC_0A}$. It satisfies $\mathrm{P}(\Psi'_{RBC_0A}, \Psi_{RBC_0A}) \leq \varepsilon$.

The expected communication cost is as follows.

Fact B.1. Expected communication cost of $\mathcal{P}$ is

$$\sum_{i_1,i_2\ldots i_r} p_{i_1,i_2\ldots i_r} \log(i_1 \cdot i_2 \ldots i_r)$$

Proof. The expected communication cost is the expected length of the messages over all probability outcomes. It can be evaluated as

$$\sum_{i_1} p_{i_1} \log(i_1) + \sum_{i_1,i_2} p_{i_1} p_{i_2|i_1} \log(i_2) + \ldots \sum_{i_1,i_2\ldots i_r} p_{i_1,i_2\ldots i_{r-1}} p_{i_r|i_{r-1},i_{r-2}\ldots i_1} \log(i_r)$$

$$= \sum_{i_1,i_2\ldots i_r} p_{i_1,i_2\ldots i_r} (\log(i_1) + \log(i_1) + \ldots \log(i_r)).$$

□

This allows us to define

Definition B.2. Communication weight of a probability distribution $\{p_1, p_2 \ldots p_m\}$ is defined as $\sum_{i=1}^{m} p_i \log(i)$.

The following lemma is a coherent representation of above protocol.

Lemma B.3. *For every $k \leq r$, let $\mathcal{O}_k$ represent the set of all tuples $(i_1, i_2 \ldots i_k)$ which satisfy: $\{i_1, i_2 \ldots i_k\}$ is a sequence of measurement outcomes that occurs with non-zero probability upto k-th round of $\mathcal{P}$.*

There exist registers $M_1, M_2 \ldots M_r$ and isometries

$$\{U_{i_{k-1},i_{k-2}\ldots i_2,i_1} : ACE_A \to ACE_A M_k | k > 1, k \text{ odd}, (i_1, i_2 \ldots i_{k-1}) \in \mathcal{O}_{k-1}\},$$

$$\{U_{i_{k-1},i_{k-2}\ldots i_2,i_1} : BE_B \to BE_B M_k | k \text{ even}, (i_1, i_2 \ldots i_{k-1}) \in \mathcal{O}_{k-1}\}$$

and $U : ACE_A \to ACE_A M_1$, such that

$$|\Psi\rangle_{RBCA} |\theta\rangle_{E_A E_B} = U^\dagger \sum_{i_1,i_2\ldots i_r} \sqrt{p_{i_1,i_2\ldots i_r}} U^\dagger_{i_1} U^\dagger_{i_2,i_1} \ldots U^\dagger_{i_r,i_{r-1}\ldots i_1} \left|\tau^{i_r,i_{r-1}\ldots i_1}\right\rangle_{RBCAC_0T_BE_A} |i_r\rangle_{M_r} \ldots |i_1\rangle_{M_1}.$$

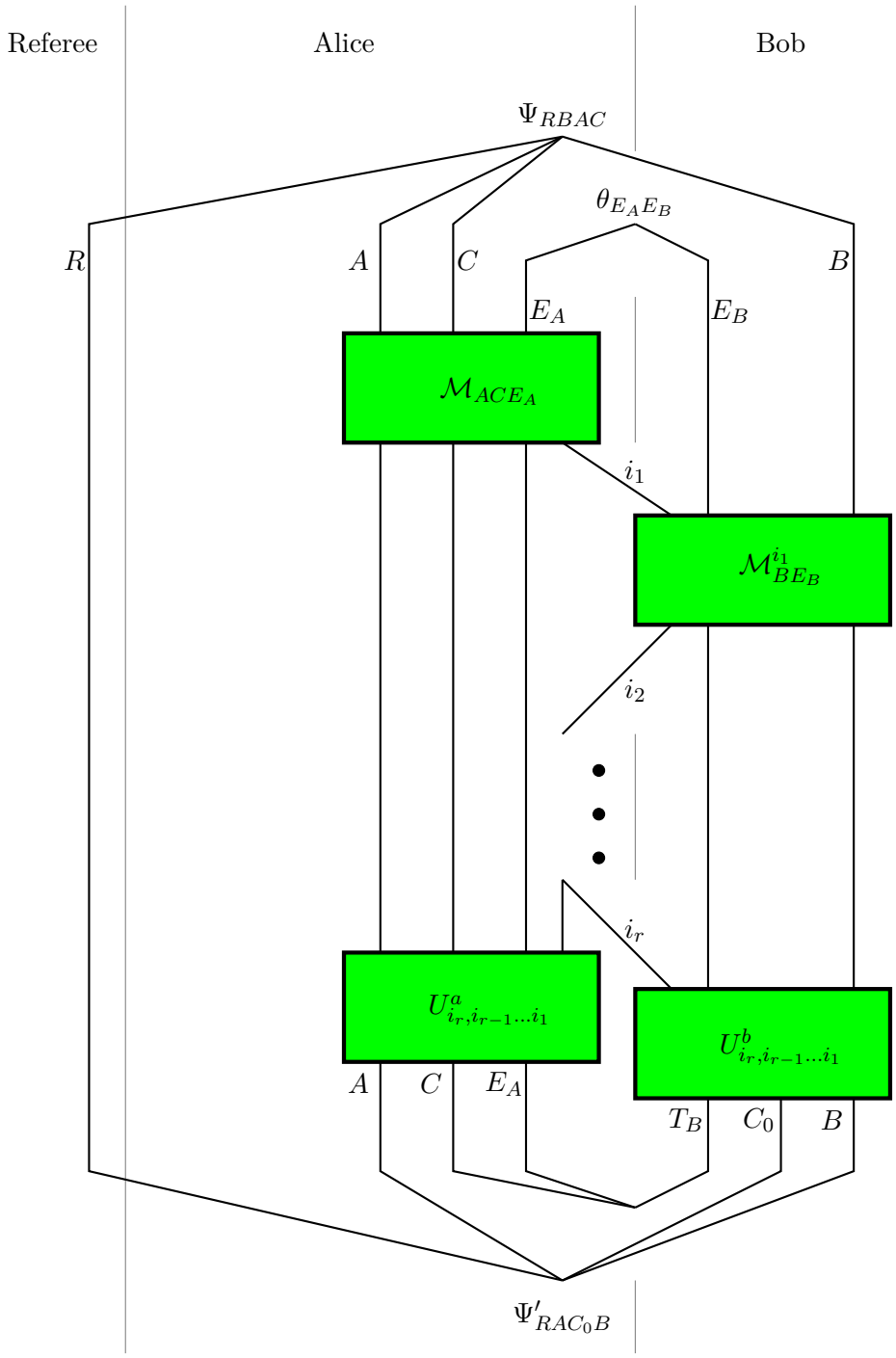


Figure 1: Graphical representation of interactive protocol for Quantum state redistribution. The messages $i_1, i_2 \ldots$ are exchanged by Alice and Bob till round r.

Proof. Fix an odd $k > 1$. Let the messages prior to $k-$th round be $(i_1, i_2 \dots i_{k-1})$. As defined in protocol $\mathcal{P}$, global quantum state before k-th round is $\phi_{RBCAE_AE_B}^{i_{k-1},i_{k-2}\dots i_1}$. Alice performs the measurement

$$\{M_{ACE_A}^{1,i_{k-1},i_{k-2}\dots i_2,i_1}, M_{ACE_A}^{2,i_{k-1},i_{k-2}\dots i_2,i_1} \dots\}.$$

This leads to the following equation (referred to as *convex-split* in [AJD14]):

$$\begin{aligned}
\phi_{RBE_B}^{i_{k-1},i_{k-2}\dots i_1} &= \sum_{i_k} \mathrm{Tr}_{ACE_A}(M_{ACE_A}^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1} \phi_{RBCAE_BE_A}^{i_{k-1},i_{k-2}\dots i_1}) \\
&= \sum_{i_k} p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1} \frac{\mathrm{Tr}_{ACE_A}(M_{ACE_A}^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1} \phi_{RBCAE_BE_A}^{i_{k-1},i_{k-2}\dots i_1} M_{ACE_A}^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1})}{p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1}} \\
&= \sum_{i_k} p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1} \phi_{RBE_B}^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1} \qquad (1)
\end{aligned}$$

A purification of $\phi_{RBE_B}^{i_{k-1},i_{k-2}\dots i_1}$ on registers $RBCAE_BE_A$ is $\phi_{RBCAE_BE_A}^{i_{k-1},i_{k-2}\dots i_1}$. Introduce a register M_k (of sufficiently large dimension) and consider the following purification of

$$\sum_{i_k} p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1} \phi_{RBE_B}^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1}$$

on register $RBCAE_BE_AM_k$:

$$\sum_{i_k} \sqrt{p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1}} \left|\phi^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1}\right\rangle_{RBCAE_BE_A} |i_k\rangle_{M_k}.$$

By Uhlmann's theorem A.4, there exists an isometry $U_{i_{k-1},i_{k-2}\dots i_2,i_1} : ACE_A \to ACE_AM_k$ such that

$$U_{i_{k-1},i_{k-2}\dots i_2,i_1} \left|\phi^{i_{k-1},i_{k-2}\dots i_1}\right\rangle_{RBCAE_BE_A} = \sum_{i_k} \sqrt{p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1}} \left|\phi^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1}\right\rangle_{RBCAE_BE_A} |i_k\rangle_{M_k} \qquad (2)$$

For $k = 1$, introduce register M_1 of sufficiently large dimension. Similar argument implies that there exists an isometry $U : ACE_A \to ACE_AM_1$ such that

$$U |\Psi\rangle_{RBACE_BE_A} = \sum_{i_1} \sqrt{p_{i_1}} \left|\phi^{i_1}\right\rangle_{RBACE_BE_A} |i_1\rangle_{M_1} \qquad (3)$$

For k even, introduce a register M_k of sufficiently large dimension. Again by similar argument, there exists an isometry $U_{i_{k-1},i_{k-2}\dots i_2,i_1} : BE_B \to BE_BM_k$ such that

$$U_{i_{k-1},i_{k-2}\dots i_2,i_1} \left|\phi^{i_{k-1},i_{k-2}\dots i_1}\right\rangle_{RBCAE_BE_A} = \sum_{i_k} \sqrt{p_{i_k|i_{k-1},i_{k-2}\dots i_2,i_1}} \left|\phi^{i_k,i_{k-1},i_{k-2}\dots i_2,i_1}\right\rangle_{RBCAE_BE_A} |i_k\rangle_{M_k} \qquad (4)$$

Now, we recursively use equations 2, 3 and 4. Consider,

$$
\begin{aligned}
&|\Psi\rangle_{RBCA}\,|\theta\rangle_{E_AE_B} = U^\dagger \sum_{i_1} \sqrt{p_{i_1}}\left|\phi^{i_1}\right\rangle_{RBCAE_BE_A} |i_1\rangle_{M_1} \\
= \;& U^\dagger \sum_{i_1} \sqrt{p_{i_1}} U_{i_1}^\dagger \sum_{i_2} \sqrt{p_{i_2|i_1}}\left|\phi^{i_2,i_1}\right\rangle_{RBCAE_BE_A} |i_2\rangle_{M_2}\,|i_1\rangle_{M_1} \\
= \;& U^\dagger \sum_{i_1,i_2} \sqrt{p_{i_1,i_2}} U_{i_1}^\dagger \left|\phi^{i_2,i_1}\right\rangle_{RBCAE_BE_A} |i_2\rangle_{M_2}\,|i_1\rangle_{M_1} \\
= \;& U^\dagger \sum_{i_1,i_2\ldots i_r} \sqrt{p_{i_1,i_2\ldots i_r}} U_{i_1}^\dagger U_{i_2,i_1}^\dagger \ldots U_{i_r,i_{r-1}\ldots i_1}^\dagger \left|\tau^{i_r,i_{r-1}\ldots i_1}\right\rangle_{RBCAB_0T_BE_A} |i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}
\end{aligned}
$$

Last equality follows by recursion. This completes the proof.

□

We introduce the following useful definitions.

Definition B.4. Define the following isometries and unitaries.

- Let $k>1$ be odd. Isometry $U_k : ACE_AM_1M_2\ldots M_{k-1} \to ACE_AM_1M_2\ldots M_{k-1}M_k$,

$$U_k \stackrel{\text{def}}{=} \sum_{i_1,i_2\ldots i_{k-1}} |i_1\rangle\langle i_1|_{M_1} \otimes |i_2\rangle\langle i_2|_{M_2} \otimes \ldots |i_{k-1}\rangle\langle i_{k-1}|_{M_{k-1}} \otimes U_{i_{k-1},i_{k-2}\ldots i_2,i_1}.$$

- For k even, Isometry $U_k : BE_BM_1M_2\ldots M_{k-1} \to BE_BM_1M_2\ldots M_{k-1}M_k$,

$$U_k \stackrel{\text{def}}{=} \sum_{i_1,i_2\ldots i_{k-1}} |i_1\rangle\langle i_1|_{M_1} \otimes |i_2\rangle\langle i_2|_{M_2} \otimes \ldots |i_{k-1}\rangle\langle i_{k-1}|_{M_{k-1}} \otimes U_{i_{k-1},i_{k-2}\ldots i_2,i_1}.$$

- Unitary $U_{r+1}^a : ACE_AM_1M_2\ldots M_r \to ACE_AM_1M_2\ldots M_r$,

$$U_{r+1}^a \stackrel{\text{def}}{=} \sum_{i_1,i_2\ldots i_r} |i_1\rangle\langle i_1|_{M_1} \otimes |i_2\rangle\langle i_2|_{M_2} \otimes \ldots |i_r\rangle\langle i_r|_{M_r} \otimes U^a_{i_r,i_{r-1}\ldots i_1}.$$

- Unitary $U_{r+1}^b : BE_BM_1M_2\ldots M_r \to BC_0T_BM_1M_2\ldots M_r$,

$$U_{r+1}^b \stackrel{\text{def}}{=} \sum_{i_1,i_2\ldots i_r} |i_1\rangle\langle i_1|_{M_1} \otimes |i_2\rangle\langle i_2|_{M_2} \otimes \ldots |i_r\rangle\langle i_r|_{M_r} \otimes U^b_{i_r,i_{r-1}\ldots i_1}.$$

- Unitary $U_{r+1} : ACE_ABE_BM_1M_2\ldots M_r \to ACE_ABC_0T_BM_1M_2\ldots M_r$,

$$U_{r+1} \stackrel{\text{def}}{=} \sum_{i_1,i_2\ldots i_r} |i_1\rangle\langle i_1|_{M_1} \otimes |i_2\rangle\langle i_2|_{M_2} \otimes \ldots |i_r\rangle\langle i_r|_{M_r} \otimes U_{i_r,i_{r-1}\ldots i_1}.$$

This leads to a more convenient representation of Lemma B.3.

Corollary B.5. *It holds that*

$$|\Psi\rangle_{RBCA}\,|\theta\rangle_{E_AE_B} = U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1,i_2\dots i_r} \sqrt{p_{i_1,i_2\dots i_r}}\left|\tau^{i_r,i_{r-1}\dots i_1}\right\rangle_{RBCAC_0T_BE_A} |i_r\rangle_{M_r}\dots|i_1\rangle_{M_1}\,.$$

and

$$\mathrm{P}(\Psi_{RBC_0A}, \sum_{i_1,i_2\dots i_r} p_{i_1,i_2\dots i_r}\tau_{RBC_0A}^{i_r,i_{r-1}\dots i_1}) \le \varepsilon.$$

Proof. The corollary follows immediately using Definition B.4 and Lemma B.3. □

Following lemma is a refined form of above corollary, where we clarify the structure of the states $|\tau^{i_r,i_{r-1}\dots i_1}\rangle_{RBCAC_0T_BE_A}$. Its proof is deferred to Appendix D.

Lemma B.6. *There exists a probability distribution* $\{p'_{i_1,i_2\dots i_r}\}$ *and pure states* $\kappa_{CE_AT_B}^{i_r,i_{r-1}\dots i_1}$ *such that*

$$\mathrm{P}(\Psi_{RBCA}\otimes\theta_{E_AE_B}, U^\dagger U_2^\dagger\dots U_{r+1}^\dagger \sum_{i_1,i_2\dots i_r}\sqrt{p'_{i_1,i_2\dots i_r}}\Psi_{RBC_0A}\otimes\kappa_{CE_AT_B}^{i_r,i_{r-1}\dots i_1}|i_r\rangle_{M_r}\dots|i_1\rangle_{M_1}) \le 2\sqrt{\varepsilon},$$

and the communication weight of $p'_{i_1,i_2\dots i_r}$ *is at most* $\frac{C}{1-\varepsilon}$.

C Lower bound on expected communication cost

In this section, we obtain a lower bound on expected communication cost of quantum state redistribution and quantum state transfer, by considering a class of states defined below.

Let register R be composed of two registers R_A, R', such that $R \equiv R_AR'$. Let d_a be the dimension of registers R_A and A. Let d be the dimension of registers R', C and B.

Definition C.1. Define

$$|\Psi\rangle_{RBCA} \stackrel{\text{def}}{=} \frac{1}{\sqrt{d_a}}\sum_{a=1}^{d_a}|a\rangle_{R_A}|a\rangle_A|\psi^a\rangle_{R'BC}\,,$$

where

$$|\psi^a\rangle_{R'BC} = \sum_{j=1}^{d}\sqrt{e_j}\,|u_j\rangle_{R'}|v_j(a)\rangle_B|w_j(a)\rangle_C$$

with $e_1 \ge e_2 \ge \dots e_d > 0$, $\sum_{i=1}^d e_i = 1$ and $\{|u_1\rangle,\dots|u_d\rangle\}$, $\{|v_1(a)\rangle,\dots|v_d(a)\rangle\}$, $\{|w_1(a)\rangle,\dots|w_d(a)\rangle\}$ form an orthonormal basis (second and third bases may depend arbitrarily on a) in their respective Hilbert spaces.

Define a 'GHZ state': $|\omega^a\rangle_{R'BC} \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}}\sum_{j=1}^d|u_j\rangle_{R'}|v_j(a)\rangle_B|w_j(a)\rangle_C$. Using this, we define $\omega_{RBCA} \stackrel{\text{def}}{=} \frac{1}{\sqrt{d_a}}\sum_{a=1}^{d_a}|a\rangle_{R_A}|a\rangle_A|\omega^a\rangle_{R'BC}$.

For quantum state transfer, we have the following definition.

Definition C.2. Define a pure state

$$\tilde{\Psi}_{RC} \stackrel{\text{def}}{=} \sum_{j=1}^{d} \sqrt{e_j} \left|u_j\right\rangle_R \left|w_j\right\rangle_C .$$

Corresponding maximally entangled state $\omega'_{RC} \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{j=1}^{d} \left|u_j\right\rangle_R \left|w_j\right\rangle_C$.

Following two relations are easy to verify.

$$\left|\omega\right\rangle_{RBCA} = \frac{1}{\sqrt{d_a \cdot d}} \Psi_R^{-\frac{1}{2}} \left|\Psi\right\rangle_{RBCA} \text{ and } \left|\omega'\right\rangle_{RC} = \frac{1}{\sqrt{d}} (\tilde{\Psi}_R)^{-\frac{1}{2}} \left|\tilde{\Psi}\right\rangle_{RC} \tag{5}$$

As noted in Appendix B, the protocol $\mathcal{P}$ achieves quantum state redistribution of Ψ_{RBCA} with error ε and expected communication cost C.

We now use Lemma B.6 to prove the following for the state ω_{RBCA}. Recall that e_d is the smallest eigenvalue of $\psi^a_{R'}$, independent of a.

Lemma C.3. *It holds that*

$$\mathrm{P}(\omega_{RBCA} \otimes \theta_{E_A E_B}, U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1, i_2 \dots i_r} \sqrt{p'_{i_1, i_2 \dots i_r}} \omega_{RBC_0A} \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1} \dots i_1} \left|i_r\right\rangle_{M_r} \dots \left|i_1\right\rangle_{M_1}) \leq \sqrt{\frac{8\varepsilon}{e_d \cdot d}}.$$

Communication weight of distribution $p'_{i_1, i_2 \dots i_r}$ is $\frac{C}{1-\varepsilon}$.

Proof. Define a completely positive map $\tilde{\mathcal{E}} : R \to R$ as $\tilde{\mathcal{E}}(\rho) \stackrel{\text{def}}{=} \frac{e_d}{d_a} (\Psi_R^{-\frac{1}{2}} \rho \Psi_R^{-\frac{1}{2}})$, which is trace non-increasing since $\Psi_R^{-1} \leq \frac{d_a}{e_d} \mathrm{I}_R$. Using equation 5, observe that

$$\tilde{\mathcal{E}}(\Psi_{RBCA}) = e_d \cdot d \cdot \omega_{RBCA}.$$

Consider,

$$\begin{aligned}
2\sqrt{\varepsilon} \;\geq\; & \mathrm{P}(\Psi_{RBCA} \otimes \theta_{E_A E_B}, U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1, i_2 \dots i_r} \sqrt{p'_{i_1, i_2 \dots i_r}} \Psi_{RBC_0A} \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1} \dots i_1} \left|i_r\right\rangle_{M_r} \dots \left|i_1\right\rangle_{M_1}) \\
& \text{(Lemma B.6)} \\
\geq\; & \mathrm{P}(\tilde{\mathcal{E}}(\Psi_{RBCA}) \otimes \theta_{E_A E_B}, U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1, i_2 \dots i_r} \sqrt{p'_{i_1, i_2 \dots i_r}} \tilde{\mathcal{E}}(\Psi_{RBC_0A}) \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1} \dots i_1} \left|i_r\right\rangle_{M_r} \dots \left|i_1\right\rangle_{M_1}) \\
& \text{(Fact A.5)} \\
=\; & \mathrm{P}(d \cdot e_d \cdot \omega_{RBCA} \otimes \theta_{E_A E_B}, d \cdot e_d \cdot U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1, i_2 \dots i_r} \sqrt{p'_{i_1, i_2 \dots i_r}} \omega_{RBC_0A} \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1} \dots i_1} \left|i_r\right\rangle_{M_r} \dots \left|i_1\right\rangle_{M_1})
\end{aligned}$$

Using Fact A.7, we thus obtain

$$\mathrm{P}(\omega_{RBCA} \otimes \theta_{E_A E_B}, U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1, i_2 \dots i_r} \sqrt{p'_{i_1, i_2 \dots i_r}} \omega_{RBC_0A} \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1} \dots i_1} \left|i_r\right\rangle_{M_r} \dots \left|i_1\right\rangle_{M_1}) \leq \sqrt{\frac{8\varepsilon}{d \cdot e_d}}.$$

Furthermore, there is no change in communication weight. This completes the proof. □

Similarly for quantum state transfer, we have the following corollary

Corollary C.4. *It holds that*

$$\mathrm{P}(\omega'_{RC}\otimes\theta_{E_AE_B}, U^\dagger U_2^\dagger\dots U_{r+1}^\dagger \sum_{i_1,i_2\dots i_r}\sqrt{p'_{i_1,i_2\dots i_r}}\omega'_{RC_0}\otimes\kappa_{CE_AT_B}^{i_r,i_{r-1}\dots i_1}|i_r\rangle_{M_r}\dots|i_1\rangle_{M_1}) \leq \sqrt{\frac{8\varepsilon}{e_d\cdot d}}.$$

Communication weight of distribution $p'_{i_1,i_2\dots i_r}$ is $\frac{C}{1-\varepsilon}$.

Now we exhibit an interactive entanglement assisted communication protocol for state-redistribution of ω_{RBCA} with suitably upper bounded worst case communication cost. Proof of this lemma has been deferred to Appendix E.

Lemma C.5. *Fix an error parameter $\mu > 0$. There exists an entanglement assisted r-round quantum communication protocol for state redistribution of ω_{RBCA} with worst case quantum communication cost at most $\frac{2C}{\mu(1-\varepsilon)}$ and error at most $\sqrt{\frac{8\varepsilon}{e_d\cdot d}}+\sqrt{\mu}$.*

Similarly, we have the corollary for quantum state transfer.

Corollary C.6. *Fix an error parameter $\mu > 0$. There exists a r-round communication protocol for state transfer of ω'_{RC} with worst case quantum communication cost atmost $\frac{2C}{\mu(1-\varepsilon)}$ and error at most $\sqrt{\frac{8\varepsilon}{e_d\cdot d}}+\sqrt{\mu}$.*

Next two lemmas obtain lower bound on worst case quantum communication cost of quantum state redistribution of ω_{RBCA} and quantum state transfer of ω'_{RC}.

Lemma C.7. *Let d, the local dimension of register B, be such that $d > 2^{18}$. Then worst case quantum communication cost of any interactive entanglement assisted quantum state redistribution protocol of the state ω_{RBCA}, with error $\delta < \frac{1}{6}$, is at least $\frac{1}{6}\log(d)$.*

Proof. Following lower bound on worst case quantum communication cost for interactive quantum state redistribution of the state ω_{RBCA}, with error δ, has been shown ([BCT16], Section 5, Proposition 2):

$$\frac{1}{2}(\mathrm{I}^\delta_{\max}(R:BC)_\omega - \mathrm{I}_{\max}(R:B)_\omega).$$

Recall, from definition C.1, that $\omega_{RBC} = \frac{1}{d_a}\sum_{a=1}^{d_a}|a\rangle\langle a|_{R_A}\otimes\omega^a_{R'BC}$ is a *classical-quantum* state. Consider,

$$\begin{aligned}
\mathrm{I}^\delta_{\max}(R:BC)_\omega &\geq \inf_{\rho_{RBC}\in\mathcal{B}^\delta(\omega_{RBC})}\mathrm{I}(R:BC)_\rho \\
&\geq \inf_{\rho_R\in\mathcal{B}^\delta(\omega_R)}S(\rho_R)+\inf_{\rho_{BC}\in\mathcal{B}^\delta(\omega_{BC})}S(\rho'_{BC}) - \sup_{\rho_{RBC}\in\mathcal{B}^\delta(\omega_{RBC})}S(\rho_{RBC}) \\
&\geq \mathrm{I}(R:BC)_\omega - 3\delta\log(d) - 3 \quad \text{(Fact A.8)} \\
&\geq \frac{1}{d_a}\sum_a \mathrm{I}(R':BC)_{\omega^a} - 3\delta\log(d) - 3 \quad \text{(Fact A.14)} \\
&= 2\log(d) - 3\delta\log(d) - 3.
\end{aligned}$$

To bound $\mathrm{I}_{\max}(R:B)_\omega$, notice that $\omega_{RB} = \frac{1}{d\cdot d_a}\sum_{a=1}^{d_a}\sum_{j=1}^{d}|a\rangle\langle a|_{R_A}\otimes|u_j\rangle\langle u_j|_{R'}\otimes|v_j(a)\rangle\langle v_j(a)|_B$ is also a *classical-quantum* state. Using Fact A.13, we obtain $\mathrm{I}_{\max}(R:B)_\omega \leq \log(|B|) = \log(d)$.

Thus, communication cost is lower bounded by

$$\frac{1}{2}(\mathrm{I}^{\delta}_{\max}(R:BC)_{\omega} - \mathrm{I}_{\max}(R:B)_{\omega}) \geq \frac{\log(d) - 3\delta\log(d) - 3}{2} = \frac{1-3\delta}{2}\log(d) - 1.5 > \frac{1}{6}\log(d),$$

for $d > 2^{18}$. □

For quantum state transfer, we have following bound.

Lemma C.8. *Worst case quantum communication cost for state transfer of the state ω'_{RC}, with error $\delta < \frac{1}{2}$, is at least $\frac{1}{2}\log(d) + \frac{1}{2}\log(1-\delta^2)$.*

Proof. The following lower bound on worst case interactive quantum communication cost of state transfer of ω'_{RC} has been shown ([BCT16], Section 5, Proposition 2):

$$\frac{1}{2}\mathrm{I}^{\delta}_{\max}(R:C)_{\omega'}.$$

Consider,

$$\begin{aligned}
\mathrm{I}^{\delta}_{\max}(R:C)_{\omega'} &\geq -\mathrm{H}^{\delta}_{\min}(R|C)_{\omega'} \quad \text{(Fact A.12)} \\
&\geq -\mathrm{H}_{\max}(R|C)_{\omega'} + \log(1-\delta^2) \quad \text{(Proposition 6.3, [Tom15])} \\
&= \log(d) + \log(1-\delta^2)
\end{aligned}$$

□

Now we proceed to proof of Theorem 1.3.

Proof: Theorem 1.3. Suppose there exists a r-round communication protocol $\mathcal{P}$ for entanglement assisted quantum state redistribution of the pure state Ψ_{RBCA} with error ε and expected communication cost at most $\mathrm{I}(R:C|B)_{\Psi} \cdot (\frac{1}{\varepsilon})^p$. Then we show a contradiction for $p < 1$.

For a $\beta \geq 1$ to be chosen later, and $d > 2^{18}$, we choose $\{e_1, e_2 \dots e_d\}$ (Definition C.1) as constructed in lemma A.15. Thus,

$$\mathrm{I}(R:C|B)_{\Psi} \leq 2S(\Psi_C) \leq 4\frac{\log(d)}{\beta} \quad \text{(Fact A.11)}.$$

Fix an error parameter μ. From lemma C.5, there exists a communication protocol $\mathcal{P}'$ for quantum state redistribution of ω_{RBCA}, with error at most $\sqrt{\mu} + \sqrt{8\beta\varepsilon}$ and worst case quantum communication cost at most

$$\frac{2 \cdot \mathrm{I}(R:C|B)_{\Psi}}{\mu(1-\varepsilon)} \cdot (\frac{1}{\varepsilon})^p \leq 8\frac{\log(d)}{\beta\mu(1-\varepsilon)} \cdot (\frac{1}{\varepsilon})^p \leq 16\frac{\log(d)}{\beta\mu} \cdot (\frac{1}{\varepsilon})^p.$$

Last inequality holds since $\varepsilon < 1/2$. Let $\beta\mu\varepsilon^p = 128$. Then $\sqrt{\mu} + \sqrt{8\beta\varepsilon} = \sqrt{\mu} + \frac{32}{\sqrt{\mu}}\varepsilon^{\frac{1-p}{2}}$, which is minimized at $\mu = 32 \cdot \varepsilon^{\frac{1-p}{2}}$. This gives $\sqrt{\mu} + \frac{32}{\sqrt{\mu}}\varepsilon^{\frac{1-p}{2}} = 8\sqrt{2} \cdot \varepsilon^{\frac{1-p}{4}}$ and $\beta = 4/\varepsilon^{\frac{1+p}{2}} > 1$.

As in the theorem, let $\varepsilon \in [0, (\frac{1}{70})^{\frac{4}{1-p}}]$. Thus, we have a protocol for state redistribution of ω_{RBCA}, with error at most $8\sqrt{2} \cdot \varepsilon^{\frac{1-p}{4}} < \frac{1}{6}$ and worst case communication at most $\frac{1}{8}\log(d)$, in contradiction with lemma C.7. □

Above argument does not hold for any $p \geq 1$ since we need to simultaneously satisfy $\beta \geq 1$, $8\beta\varepsilon < 1$ and $\mu < 1$.

On similar lines, we prove Theorem 1.4 below.

Proof: Theorem 1.4. Suppose there exists a communication protocol for state transfer of the pure states $\tilde{\Psi}_{RC}$ with error $\varepsilon < \frac{1}{2}$ and expected communication cost at most $S(\tilde{\Psi}_R) \cdot (\frac{1}{\varepsilon})^p$. Then we show a contradiction for $p < 1$.

For a $\beta \geq 1$ to be chosen later, choose a_i as constructed in lemma A.15. Then $S(\tilde{\Psi}_R) \leq 2\frac{\log(d)}{\beta}$.

Fix an error parameter μ. From corollary C.6, there exists a communication protocol for state transfer of ω'_{RC}, with error at most $\sqrt{\mu} + \sqrt{8\beta\varepsilon}$ and worst case quantum communication cost at most

$$\frac{2S(\Psi'_R)}{\mu(1-\varepsilon)} \cdot (\frac{1}{\varepsilon})^p \leq \frac{4\log(d)}{\beta\mu(1-\varepsilon)} \cdot (\frac{1}{\varepsilon})^p \leq \frac{8\log(d)}{\beta\mu} \cdot (\frac{1}{\varepsilon})^p.$$

Let $\beta\mu\varepsilon^p = 16$. Then $\sqrt{\mu} + \sqrt{8\beta\varepsilon} = \sqrt{\mu} + \frac{8\sqrt{2}}{\sqrt{\mu}}\varepsilon^{\frac{1-p}{2}}$, which is minimized at $\mu = 8\sqrt{2}\varepsilon^{\frac{1-p}{2}}$. This gives $\sqrt{\mu} + \sqrt{8\beta\varepsilon} = \sqrt{32\sqrt{2}}\varepsilon^{\frac{1-p}{4}}$ and $\beta = \sqrt{2}/\varepsilon^{\frac{1+p}{2}} > 1$.

As in the theorem, let $\varepsilon \in [0, (\frac{1}{2})^{\frac{15}{1-p}}]$. Thus, we have a protocol for state transfer of ω'_{RC}, with error at most $\sqrt{32}\varepsilon^{\frac{1-p}{4}} < \frac{1}{2}$ and worst case communication at most $\frac{1}{2}\log(d)$, in contradiction with lemma C.8.

□

D Proof of Lemma B.6

Proof. Let $\mathcal{B}$ be the set of tuples $(i_1, i_2 \dots i_r)$ for which $\mathrm{F}^2(\Psi_{RBC_0A}, \tau_{RBC_0A}^{i_r, i_{r-1}\dots i_1}) \leq 1 - \varepsilon$. Let $\mathcal{G}$ be remaining set of tuples. From corollary B.5 and purity of Ψ_{RBC_0A}, it holds that

$$\sum_{i_1, i_2 \dots i_r} p_{i_1, i_2 \dots i_r} \mathrm{F}^2(\Psi_{RBC_0A}, \tau_{RBC_0A}^{i_r, i_{r-1}\dots i_1}) \geq 1 - \varepsilon^2.$$

Thus,

$$(1-\varepsilon) \sum_{(i_1, i_2 \dots i_r) \in \mathcal{B}} p_{i_1, i_2 \dots i_r} + \sum_{(i_1, i_2 \dots i_r) \in \mathcal{G}} p_{i_1, i_2 \dots i_r} \geq 1 - \varepsilon^2,$$

which implies $\sum_{(i_1, i_2 \dots i_r) \in \mathcal{B}} p_{i_1, i_2 \dots i_r} \leq \varepsilon$. Thus we have $\sum_{(i_1, i_2 \dots i_r) \in \mathcal{G}} p_{i_1, i_2 \dots i_r} \geq 1 - \varepsilon$.

Define $p'_{i_1, i_2 \dots i_r} \stackrel{\text{def}}{=} \frac{p_{i_1, i_2 \dots i_r}}{\sum_{i_1, i_2 \dots i_r \in \mathcal{G}} p_{i_1, i_2 \dots i_r}}$, if $(i_1, i_2 \dots i_r) \in \mathcal{G}$ and $p'_{i_1, i_2 \dots i_r} \stackrel{\text{def}}{=} 0$ if $(i_1, i_2 \dots i_r) \in \mathcal{B}$.

For all $(i_1, i_2 \dots i_r) \in \mathcal{G}$, $\mathrm{F}^2(\Psi_{RBC_0A}, \tau_{RBC_0A}^{i_r, i_{r-1}\dots i_1}) \geq 1 - \varepsilon$. Thus by Fact A.4, there exists a pure state $\kappa_{CE_AT_B}^{i_r, i_{r-1}\dots i_1}$ such that

$$\mathrm{F}^2(\Psi_{RBC_0A} \otimes \kappa_{CE_AT_B}^{i_r, i_{r-1}\dots i_1}, \tau_{RBCAC_0T_BE_A}^{i_r, i_{r-1}\dots i_1}) \geq 1 - \varepsilon \tag{6}$$

Consider,

$$\mathrm{P}\Big(\sum_{i_1,i_2\ldots i_r}\sqrt{p_{i_1,i_2\ldots i_r}}\tau^{i_r,i_{r-1}\ldots i_1}_{RBCAC_0T_BE_A}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\,,\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\tau^{i_r,i_{r-1}\ldots i_1}_{RBCAC_0T_BE_A}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\Big)$$
$$= \sqrt{1-\Big(\sum_{i_1,i_2\ldots i_r}\sqrt{p_{i_1,i_2\ldots i_r}p'_{i_1,i_2\ldots i_r}}\Big)^2} = \sqrt{1-\Big(\sum_{i_1,i_2\ldots i_r\in\mathcal{G}}p_{i_1,i_2\ldots i_r}\Big)} \le \sqrt{\varepsilon}$$

and

$$\mathrm{P}\Big(\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\tau^{i_r,i_{r-1}\ldots i_1}_{RBCAC_0T_BE_A}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\,,\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\Psi_{RBC_0A}\otimes\kappa^{i_r,i_{r-1}\ldots i_1}_{CE_AT_B}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\Big)$$
$$= \sqrt{1-\Big(\sum_{i_1,i_2\ldots i_r}p'_{i_1,i_2\ldots i_r}\mathrm{F}(\tau^{i_r,i_{r-1}\ldots i_1}_{RBCAC_0T_BE_A},\Psi_{RBC_0A}\otimes\kappa^{i_r,i_{r-1}\ldots i_1}_{CE_AT_B})\Big)^2} \le \sqrt{\varepsilon} \quad \text{(Equation 6)}$$

These together imply, using triangle inequality for purified distance (Fact A.2),

$$\mathrm{P}\Big(\sum_{i_1,i_2\ldots i_r}\sqrt{p_{i_1,i_2\ldots i_r}}\tau^{i_r,i_{r-1}\ldots i_1}_{RBCAC_0T_BE_A}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\,,\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\Psi_{RBC_0A}\otimes\kappa^{i_r,i_{r-1}\ldots i_1}_{CE_AT_B}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1}\Big)$$
$$\le 2\sqrt{\varepsilon}$$

Thus, from corollary B.5, we have

$$\mathrm{P}(\Psi_{RBCA}\otimes\theta_{E_AE_B},U^\dagger U_2^\dagger\ldots U_{r+1}^\dagger\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\Psi_{RBC_0A}\otimes\kappa^{i_r,i_{r-1}\ldots i_1}_{CE_AT_B}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1})\le 2\sqrt{\varepsilon}.$$

The communication weight of $p'_{i_1,i_2\ldots i_r}$ is

$$\begin{aligned}\sum_{i_1,i_2\ldots i_r}p'_{i_1,i_2\ldots i_r}\log(i_1\cdot i_2\ldots i_r) &\le \frac{1}{1-\varepsilon}\sum_{i_1,i_2\ldots i_r\in\mathcal{G}}p_{i_1,i_2\ldots i_r}\log(i_1\cdot i_2\ldots i_r)\\ &\le \frac{1}{1-\varepsilon}\sum_{i_1,i_2\ldots i_r}p_{i_1,i_2\ldots i_r}\log(i_1\cdot i_2\ldots i_r)=\frac{C}{1-\varepsilon}.\end{aligned}$$

This completes the proof. □

E Proof of Lemma C.5

Proof. From lemma C.3, we have that

$$\mathrm{P}(\omega_{RBCA}\otimes\theta_{E_AE_B},U^\dagger U_2^\dagger\ldots U_{r+1}^\dagger\sum_{i_1,i_2\ldots i_r}\sqrt{p'_{i_1,i_2\ldots i_r}}\omega_{RBC_0A}\otimes\kappa^{i_r,i_{r-1}\ldots i_1}_{CE_AT_B}|i_r\rangle_{M_r}\ldots|i_1\rangle_{M_1})\le\sqrt{\frac{8\varepsilon}{a_d\cdot d}},$$

and

$$\sum_{i_1,i_2\ldots i_r}p'_{i_1,i_2\ldots i_r}\log(i_1\cdot i_2\ldots i_r)\le\frac{C}{1-\varepsilon}.$$

Consider the set of tuples $(i_1, i_2 \dots i_r)$ which satisfy $i_1 \cdot i_2 \dots i_r > 2^{\frac{C}{(1-\varepsilon)\mu}}$. Let this set be $\mathcal{B}'$ and $\mathcal{G}'$ be the set of rest of the tuples. Then

$$\frac{C}{(1-\varepsilon)} > \sum_{i_1,i_2\dots i_r \in \mathcal{B}'} p'_{i_1,i_2\dots i_r} \log(i_1 \cdot i_2 \dots i_r) > \frac{C}{(1-\varepsilon)\mu} \sum_{i_1,i_2\dots i_r \in \mathcal{B}'} p'_{i_1,i_2\dots i_r}.$$

This implies $\sum_{i_1,i_2\dots i_r \in \mathcal{B}'} p'_{i_1,i_2\dots i_r} < \mu$. Define a new probability distribution $q_{i_1,i_2\dots i_r} \stackrel{\text{def}}{=} \frac{p'_{i_1,i_2\dots i_r}}{\sum_{(i_1,i_2\dots i_r)\in\mathcal{G}'} p'_{i_1,i_2\dots i_r}}$ for all $(i_1, i_2 \dots i_r) \in \mathcal{G}'$ and $q_{i_1,i_2\dots i_r} = 0$ for all $(i_1, i_2 \dots i_r) \in \mathcal{B}'$. Consider,

$$\mathrm{P}\Big(\sum_{i_1,i_2\dots i_r} \sqrt{p'_{i_1,i_2\dots i_r}}\omega_{RBC_0A} \otimes \kappa^{i_r,i_{r-1}\dots i_1}_{CE_AT_B} |i_r\rangle_{M_r} \dots |i_1\rangle_{M_1}, \sum_{i_1,i_2\dots i_r} \sqrt{q_{i_1,i_2\dots i_r}}\omega_{RBC_0A} \otimes \kappa^{i_r,i_{r-1}\dots i_1}_{CE_AT_B} |i_r\rangle_{M_r} \dots |i_1\rangle_{M_1}\Big)$$

$$= \sqrt{1 - \Big(\sum_{i_1,i_2\dots i_r} \sqrt{p'_{i_1,i_2\dots i_r} q_{i_1,i_2\dots i_r}}\Big)^2} = \sqrt{1 - \sum_{(i_1,i_2\dots i_r)\in\mathcal{G}'} p'_{i_1,i_2\dots i_r}} \leq \sqrt{\mu}.$$

Thus, triangle inequality for purified distance (Fact A.2) implies

$$\mathrm{P}(\omega_{RBCA} \otimes \theta_{E_AE_B}, U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1,i_2\dots i_r} \sqrt{q_{i_1,i_2\dots i_r}}\omega_{RBC_0A} \otimes \kappa^{i_r,i_{r-1}\dots i_1}_{CE_AT_B} |i_r\rangle_{M_r} \dots |i_1\rangle_{M_1})$$

$$\leq \sqrt{\frac{8\varepsilon}{e_d \cdot d}} + \sqrt{\mu}$$

Defining $\pi_{RBCAE_AE_B} \stackrel{\text{def}}{=} U^\dagger U_2^\dagger \dots U_{r+1}^\dagger \sum_{i_1,i_2\dots i_r \in \mathcal{G}'} \sqrt{q_{i_1,i_2\dots i_r}}\omega_{RBC_0A} \otimes \kappa^{i_r,i_{r-1}\dots i_1}_{CE_AT_B} |i_r\rangle_{M_r} \dots |i_1\rangle_{M_1}$, we have

$$\mathrm{P}(\omega_{RBCA} \otimes \theta_{E_AE_B}, \omega'_{RBCE_AE_B}) \leq \sqrt{\frac{8\varepsilon}{e_d \cdot d}} + \sqrt{\mu} \tag{7}$$

Let $\mathcal{T}$ be the set of all tuples $(i_1, i_2 \dots i_k)$ (with $k \leq r$) that satisfy the following property: there exists a set of positive integers $\{i_{k+1}, i_{k+2} \dots i_r\}$ such that $(i_1, i_2 \dots i_k, i_{k+1} \dots i_r) \in \mathcal{G}'$. Consider the following protocol $\mathcal{P}'$.

Input: A quantum state in registers $RBCAE_AE_B$.

- Alice applies the isometry $U : ACE_A \to ACE_AM_1$ (definition B.4). She introduces a register $M'_1 \equiv M_1$ in the state $|0\rangle_{M'_1}$ and performs the following unitary $W_1 : M_1M'_1 \to M_1M'_1$:

  $W_1 |i\rangle_{M_1} |0\rangle_{M'_1} = |i\rangle_{M_1} |i\rangle_{M'_1}$ if $(i) \in \mathcal{T}$ and $W_1 |i\rangle_{M_1} |0\rangle_{M'_1} = |i\rangle_{M_1} |0\rangle_{M'_1}$ if $(i) \notin \mathcal{T}$.

  She sends M'_1 to Bob.

- Bob introduces a register $M'_2 \equiv M_2$ in the state $|0\rangle_{M'_2}$. If he receives $|0\rangle_{M'_1}$ from Alice, he performs no operation. Else he applies the isometry $U_2 : BE_BM'_1 \to BE_BM'_1M_2$ and

then performs the following unitary $W_2 : M_1' M_2 M_2' \to M_1' M_2 M_2'$:

$$W_1 |i\rangle_{M_1'} |j\rangle_{M_2} |0\rangle_{M_2'} = |i\rangle_{M_1'} |j\rangle_{M_2} |j\rangle_{M_2'} \quad \text{if } (i,j) \in \mathcal{T}$$

and

$$W_1 |i\rangle_{M_1'} |j\rangle_{M_2} |0\rangle_{M_2'} = |i\rangle_{M_1'} |j\rangle_{M_2} |0\rangle_{M_2'} \quad \text{if } (i,j) \notin \mathcal{T}.$$

He sends M_2' to Alice.

- For every odd round $k > 1$, Alice introduces a register $M_k' \equiv M_k$ in the state $|0\rangle_{M_k'}$. If she receives $|0\rangle_{M_{k-1}'}$ from Bob, she performs no further operation. Else, she applies the isometry

$$U_k : ACE_A M_1 M_2' M_3 \dots M_{k-1}' \to ACE_A M_1 M_2' M_3 \dots M_{k-1}' M_k$$

and performs the following unitary $W_k : M_1 M_2' \dots M_{k-1}' M_k M_k' \to M_1 M_2' \dots M_{k-1}' M_k M_k'$:

$$W_k |i_1\rangle_{M_1} |i_2\rangle_{M_2'} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} = |i_1\rangle_{M_1} |i_2\rangle_{M_2'} \dots |i_k\rangle_{M_k} |i_k\rangle_{M_k'} \quad \text{if } (i_1, i_2 \dots i_k) \in \mathcal{T}$$

and

$$W_k |i_1\rangle_{M_1} |i_2\rangle_{M_2'} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} = |i_1\rangle_{M_1} |i_2\rangle_{M_2'} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} \quad \text{if } (i_1, i_2 \dots i_k) \notin \mathcal{T}.$$

She sends M_k' to Bob.

- For every even round $k > 2$, Bob introduces a register $M_k' \equiv M_k$ in the state $|0\rangle_{M_k'}$. If he receives $|0\rangle_{M_{k-1}'}$ from Alice, he performs no further operation.. Else, he applies the isometry $U_k : BE_B M_1' M_2 M_2' \dots M_{k-1}' \to BE_B M_1' M_2 M_2' \dots M_{k-1}' M_k$ and performs the following unitary $W_k : M_1' M_2 \dots M_{k-1}' M_k M_k' \to M_1' M_2 \dots M_{k-1}' M_k M_k'$:

$$W_k |i_1\rangle_{M_1'} |i_2\rangle_{M_2} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} = |i_1\rangle_{M_1'} |i_2\rangle_{M_2} \dots |i_k\rangle_{M_k} |i_k\rangle_{M_k'} \quad \text{if } (i_1, i_2 \dots i_k) \in \mathcal{T}$$

and

$$W_k |i_1\rangle_{M_1'} |i_2\rangle_{M_2} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} = |i_1\rangle_{M_1'} |i_2\rangle_{M_2} \dots |i_k\rangle_{M_k} |0\rangle_{M_k'} \quad \text{if } (i_1, i_2 \dots i_k) \notin \mathcal{T}.$$

He sends M_k' to Alice.

- After round r, if Bob receives $|0\rangle_{M_r'}$ from Alice, he performs no further operation. Else he applies the unitary $U_{r+1}^b : BE_B M_1' M_2 M_2' \dots M_r' \to BC_0 T_B M_1' M_2 M_2' \dots M_r'$. Alice applies the unitary $U_{r+1}^a : ACE_A M_1 M_2' M_3 \dots M_r \to ACE_A M_1 M_2' M_3 \dots M_r$. They trace out all of their registers except A, B, C_0.

Let $\mathcal{E} : RBCAE_A E_B \to RBC_0 A$ be the quantum map generated by $\mathcal{P}'$. For any k, if any of the parties receive the state $|0\rangle_{M_k'}$, let this event be called *abort*.

We show the following claim.

Claim E.1. It holds that $\mathcal{E}(\pi_{RBCAE_AE_B}) = \omega_{RBC_0A}$

Proof. We argue that the protocol never aborts when acting on $\pi_{RBCAE_AE_B}$. Consider the first round of the protocol. Define the projector $\Pi \stackrel{\text{def}}{=} \sum_{i:(i)\notin\mathcal{T}} |i\rangle\langle i|_{M_1}$. From definition B.4, it is clear that the isometry $U_2^\dagger U_3^\dagger \dots U_{r+1}^\dagger$ is of the form $\sum_i |i\rangle\langle i|_{M_1} \otimes V_i$, for some set of isometries $\{V_i\}$. Thus, from the definition of $\pi_{RBCAE_AE_B}$ (in which the summation is only over the tuples $(i_1, i_2 \dots i_r) \in \mathcal{G}'$), it holds that

$$\Pi U \pi_{RBCAE_AE_B} = 0.$$

This implies that Bob does not receive the state $|0\rangle_{M_1'}$ and hence he does not aborts.

Same argument applies to other rounds, which implies that the protocol never aborts. Thus, the state at the end of the protocol is

$$\mathrm{Tr}_{CE_AT_B}(U_{r+1}U_r \dots U_2 U \pi_{RBCAE_AE_B}) = \omega_{RBC_0A}.$$

□

Thus, from equation 7, it holds that

$$\mathrm{P}(\mathcal{E}(\omega_{RBCA} \otimes \theta_{E_AE_B}), \omega_{RBC_0A}) \leq \sqrt{\frac{8\varepsilon}{e_d \cdot d}} + \sqrt{\mu}.$$

Quantum communication cost of the protocol is at most

$$\max_{(i_1,i_2\dots i_r)\in\mathcal{G}'}(\log((i_1+1)\cdot(i_2+1)\dots(i_r+1)) \leq 2 \cdot \max_{(i_1,i_2\dots i_r)\in\mathcal{G}'}(\log(i_1 \cdot i_2 \dots i_r) \leq \frac{2C}{(1-\varepsilon)\mu}.$$

This completes the proof.

□

An approximated single photon state generation from coherent states entangled with qubits by measuring qubits

Fumiaki Matsuoka[1] * Akihisa Tomita[2] †

[1] *Graduate School of Information Science and Technology, Hokkaido University, Kita14-Nishi9, Kita-ku, Sapporo 060-0814, Japan*

Abstract. In an entangled system between coherent states and qubits, a superposition of coherent states is formed by measurement of the qubits. The induced superposition state can be controlled by the initial coherent states, the initial qubit states and the measurement basis, and the magnitude of the entanglement. In this paper, firstly, we briefly explain the entanglement preparation between the coherent states and qubits using the conditional phase shift or the conditional displacement. Then, we show that an approximate single photon state obtained when two weak coherent states are superposed in a distance close to the origin of phase space.

Keywords: Quantum State Control, Conditional Operations, Post-Selection, Single Photon State

1 Introduction

The single photon source [1] is important for quantum information technology such as quantum cryptography [2] and photonic quantum information processing [3]. Quantum key distribution systems often employ weak coherent light as an approximated single photon. However, quantum information processing requires genuine non-classical properties of single photons. Currently, a practical single photon source is not available in terms of generation efficiency, operation temperature, and quality. Therefore, it is important to explore alternative methods for single photon generation for the development of the quantum information technology.

In this paper, we show that an approximated single photon state can be generated by measurement of a qubit from a hybrid system where coherent states are entangled with a qubit. As methods of entanglement preparation, we consider the conditional phase shift and the conditional displacement [4]. A superposition of two coherent states is formed by measuring the qubit. We show that the induced superposition can be regarded as an approximate single photon state, when two coherent states are close and interfere destructively near the origin in phase space.

2 Conditional Operation

In this section, we briefly explain the methods of entanglement preparation using conditional operations [4]. As the first method, we consider the conditional phase shift on a coherent state by a qubit. First, we prepare a control qubit $(|1\rangle_c+|0\rangle_c)/\sqrt{2}$ and a target coherent state $|\alpha\rangle_t$ to obtain the initial state $|i\rangle = |\alpha\rangle_t (|1\rangle_c+|0\rangle_c)/\sqrt{2}$. Then, the control qubit and the target coherent state interacts through the conditional phase shift operation $\hat{U}_p |1\rangle_c \langle 1| + \hat{I} |0\rangle_c \langle c|$ [4], where the phase shift operator is given by $\hat{U}_p = e^{i\theta\hat{n}}$ where θ is phase shift angle and $\hat{n}$ is a photon number operator on the coherent state $|\alpha\rangle_t$. Using the conditional phase shift, the initial state is transformed to the entangled state as follows:

$$|\Psi_p\rangle = \frac{1}{\sqrt{2}}(|1\rangle_c |\alpha e^{i\theta}\rangle_t + |0\rangle_c |\alpha\rangle_t). \quad (1)$$

As the second method, we consider the conditional displacement. First, we generate the initial state $|i\rangle = |\alpha\rangle_t (|1\rangle_c+|0\rangle_c)/\sqrt{2}$ as used in the conditional phase shift. Then, the control qubit and the target coherent state are interacted through the conditional displacement operation $\hat{U}_d |1\rangle_c \langle 1| + \hat{I} |0\rangle_c$ [4], where the displacement operator is given by $\hat{U}_d = e^{\gamma\hat{a}^\dagger - \gamma^*\hat{a}}$. The amount of the displacement reads $\gamma = \alpha - \beta = i\chi t e^{i\phi}$, where χ is the coupling strength between the coherent state and the qubit, and t is the interaction time. The direction of the displacement on the phase space can be selected by the phase ϕ. In the present proposal, we choose $\phi = 0$, since the superposition of two coherent states of different amplitudes is required to generate the approximate single photon state. The conditional displacement transforms the initial state to

$$|\Psi_d\rangle = \frac{1}{\sqrt{2}}(|1\rangle_c |\beta\rangle_t + |0\rangle_c |\alpha\rangle_t). \quad (2)$$

3 Approximated single photon state generation by post-selection of qubit

We show that non-classical photon states can be generated by measurement of a qubit in the entangled system of coherent states and a qubit prepared by a conditional operation mentioned in Sec. II. The post-selection on the qubit to the final state $|f\rangle = (|1\rangle_c - |0\rangle_c)/\sqrt{2}$, *i.e.*, $|-\rangle$ measurement, collapses the coherent state to the superposition of two coherent states with the success probability given by the fidelity between the two states as

$$|\psi_p\rangle = \frac{1}{2\sqrt{P_{sucp}}}(|\alpha e^{i\theta}\rangle_t - |\alpha\rangle_t), \quad (3)$$

where $P_{sucp} = \frac{1}{2}\left[1 - \frac{1}{2}(\langle\alpha e^{i\theta}|\alpha\rangle + \langle\alpha|\alpha e^{i\theta}\rangle)\right]$, for the state entangled by the conditional phase shift (1), and

$$|\psi_d\rangle = \frac{1}{2\sqrt{P_{sucd}}}(|\beta\rangle_t - |\alpha\rangle_t), \quad (4)$$

*matsuoka@optnet.ist.hokudai.ac.jp
†tomita@ist.hokudai.ac.jp

where $P_{sucd} = \frac{1}{2}\left[1 - \frac{1}{2}(\langle\beta|\alpha\rangle + \langle\alpha|\beta\rangle)\right]$, for the state entangled by the control displacement (2). When a distance between two states in the superposition is small, and the states are placed near the origin in phase space, the transformed superposition state can be regarded as a single photon state.

In order to confirm the above claim, we numerically evaluated the detection probabilities as photon number states $|\langle n|\psi_p\rangle|^2$ and $|\langle n|\psi_d\rangle|^2$, when the post-selected states are measured in photon number basis. Figure 1 (a) plots the detection probabilities $|\langle n|\psi_p\rangle|^2$ for $n = 1$ (single photon states: solid line), $n = 2$ (two photon states: dashed line) and $n = 3$ (three photon states: dot-dashed line). Here, we assume that the coherent amplitude of the initial coherent state is $\alpha = 0.1$. Similarly, Fig. 1 (b) plots the detection probabilities $|\langle n|\psi_d\rangle|^2$. Note that when the conditional displacement is used, the detection probability for $n = 0$ (vacuum: dotted line) is appeared. In order to compare the post-selected state and the coherent states, Fig. 1 (c) plots the detection probabilities as photon number states $|\langle n|\alpha\rangle|^2$, when the coherent state is measured in photon number basis. In both conditional operations, the detection probability as single photon state $|\langle 1|\psi_p\rangle|^2$ and $|\langle 1|\psi_d\rangle|^2$ are greatly higher than $|\langle 1|\alpha\rangle|^2$. Moreover, in both conditional operations, there are the points of the detection probability as two photon states equals zero, since superposition becomes odd coherent states at these points.

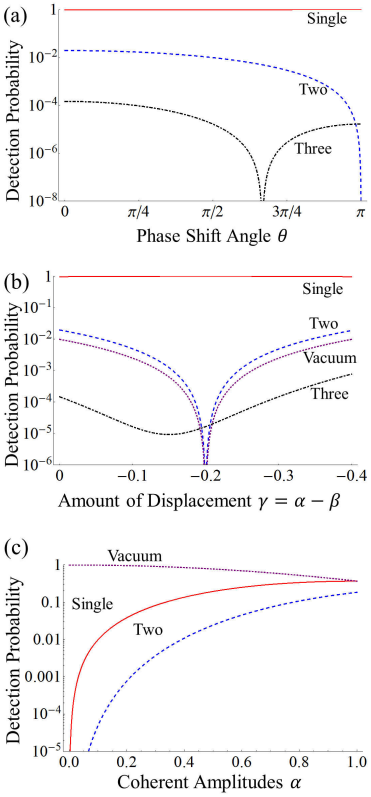


Figure 1: The detection probabilities as photon number states when the post-selected states are measured in photon number basis; (a) conditional phase shift and (b) conditional displacement. (c) The detection probabilities as photon number states when the coherent state is measured.

4 Conclusion

In summary, we have shown that measurement of a qubit in hybrid entangled system between a coherent state and a qubit results in a non-classical state. We have also proposed an application of the method to generate an approximate single photon state. The method works probabilistically, but generates the heralded single photons. The generation requires conditional operation. It is reported that the conditional phase shift can be implemented using superconducting circuits [5] and ions in a solid [6], and that the conditional displacement can be implemented using superconducting circuits [7], ion trap [8] and Rydberg atoms [9]. Further comparison with the conventional single photon generation methods under a practical condition is left for future works.

Acknowledgment

This work was funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan).

References

[1] M. D. Eisaman, *et al.* Invited Review Article: Single-photon sources and detectors. Rev. Sci. Instrum. **82**, 071101, 2011.

[2] V. Scarani, *et al.* The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301, 2009.

[3] P. Kok, *et al.* Linear optical quantum computing with photonic qubits. Rev. Mod. Phys. **79**, 135, 2007.

[4] T. Spiller, *et al.* Quantum computation by communication. New J. Phys. **8**, 30, 2006.

[5] A. Wallraff, *et al.* Approaching Unit Visibility for Control of a Superconducting Qubit with Dispersive Readout. Phys. Rev. Lett. **95**, 060501, 2005.

[6] J. J. Longdell, *et al.* Demonstration of Conditional Quantum Phase Shift Between Ions in a Solid. Phys. Rev. Lett. **93**, 130503, 2004.

[7] B. Vlastakis, *et al.* Deterministically Encoding Quantum Information Using 100-Photon Schrödinger Cat States. Science **342**, Issue 6158, pp. 607-610, 2013.

[8] D. Leibfried, *et al.* Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. Nature **422**, 412-415, 2003.

[9] S. Deleglise, *et al.* Reconstruction of non-classical cavity field states with snapshots of their decoherence. Nature **455**, 510-514, 2008.

Asymptotic Convertibility of Entanglement: A General Approach to Entanglement Concentration and Dilution

Yong Jiao[1] * Eyuri Wakakuwa[2] † Tomohiro Ogawa[2] ‡

[1] *Graduate School of Information Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan.*

[2] *Graduate School of Informatics and Engineering, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan.*

Abstract. We consider asymptotic convertibility of an arbitrary sequence of bipartite pure states into another by local operations and classical communication (LOCC). We adopt an information-spectrum approach to address cases where each element of the sequences is not always in tensor power of a bipartite pure state. We derive necessary and sufficient conditions for the LOCC convertibility of one sequence to another in terms of spectral entropy rates of entanglement of the sequences. Based on these results, we also provide a simple proof for previously known results on the optimal rates of entanglement concentration and dilution of general sequences of pure states.

Keywords: spectral entropy rates, LOCC convertibility, entanglement concentration and dilution

1 Introduction

An entangled quantum state shared between two distant parties is used as a resource for performing nonlocal quantum information processing. When a state is not in the desired form as a resource, we need to transform it by LOCC to a target state with the desired form. Well-known examples of such tasks are entanglement concentration and dilution [1]. Entanglement concentration is a task to obtain a maximally entangled state from copies of a non-maximally entangled state by LOCC, and entanglement dilution is its inverse process. When the initial state is copies of a bipartite pure state, the optimal rates of entanglement concentration and dilution are asymptotically equal to the entanglement entropy [1].

For cases where the initial and target states are not always in tensor power of a bipartite state, the information-spectrum method has been applied to analyze entanglement concentration [2, 3] and entanglement dilution [3]. Originally, the information-spectrum method was developed in classical information theory by Verdú and Han [4, 5], and has been extended to quantum information theory by Nagaoka and Hayashi [6–8]. In the setting of the information-spectrum method, the optimal rates of entanglement concentration and dilution are obtained in terms of spectral entropies [2, 3].

In this contribution, we consider a more general situation in which a general sequence of bipartite pure states $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$ is converted into another general sequence of bipartite pure states $\widehat{\phi}^{AB} = \{\phi_n^{AB}\}_{n=1}^{\infty}$ asymptotically by a sequence of LOCC protocol $\widehat{\mathcal{L}} = \{\mathcal{L}_n\}_{n=1}^{\infty}$. We require that the trace distance between the final state $\mathcal{L}_n(\psi_n^{AB})$ and the target state ϕ_n^{AB} vanishes in the limit of $n \to \infty$. We address a question of when such a conversion is possible. Contrary to the previous approaches, we do not assume that the initial state or the target state is a maximally entangled state.

The main results of this contribution are as follows. First, we prove that $\widehat{\psi}^{AB}$ is asymptotically convertible to $\widehat{\phi}^{AB}$ if the spectral inf-entropy of entanglement of $\widehat{\psi}^{AB}$ is larger than the spectral sup-entropy of entanglement of $\widehat{\phi}^{AB}$. Second, we prove that if $\widehat{\psi}^{AB}$ is asymptotically convertible to $\widehat{\phi}^{AB}$, the spectral inf- and sup-entropy of entanglement of $\widehat{\psi}^{AB}$ is larger than those of $\widehat{\phi}^{AB}$, respectively. If we restrict $\widehat{\phi}^{AB}$ or $\widehat{\psi}^{AB}$ to be a sequence of maximally entangled states, our results are equivalent to those obtained by Hayashi [2] and Bowen-Datta [3], regarding the optimal rates of entanglement concentration and dilution. Our proof based on an application of classical random number generation, which was pointed out by Kumagai and Hayashi [9], is much simpler than those of [2, 3].

2 Main Results

In this section, we present definitions of the problem and state the main results of this contribution. As a shorthand notation, we denote reduced density operators $\mathrm{Tr}_B[|\psi\rangle\langle\psi|^{AB}]$ and $\mathrm{Tr}_A[|\psi\rangle\langle\psi|^{AB}]$ simply by ψ^A and ψ^B, respectively, for a bipartite pure state $|\psi\rangle^{AB}$.

Let $\mathcal{H}_n^A$ and $\mathcal{H}_n^B$ $(n = 1, 2, \dots)$ be arbitrary finite-dimensional Hilbert spaces and consider a general sequence of bipartite systems $\mathcal{H}_n^{AB} = \mathcal{H}_n^A \otimes \mathcal{H}_n^B$ $(n = 1, 2, \dots)$. Let $|\psi_n\rangle^{AB}$ and $|\phi_n\rangle^{AB}$ in $\mathcal{H}_n^{AB}$ be arbitrary pure states for each n, and consider sequences $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$ and $\widehat{\phi}^{AB} = \{\phi_n^{AB}\}_{n=1}^{\infty}$. We ask when $\widehat{\psi}^{AB}$ can be asymptotically converted to $\widehat{\phi}^{AB}$ by LOCC. That is, we seek for conditions under which $|\psi_n\rangle^{AB}$ can be converted to $|\phi_n\rangle^{AB}$ by LOCC for each n, up to a certain error that vanishes in the limit of $n \to \infty$.

Definition 1 *We say that $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$ can be converted to $\widehat{\phi}^{AB} = \{\phi_n^{AB}\}_{n=1}^{\infty}$ asymptotically by LOCC, if there exists a sequence of LOCC $\mathcal{L}_n$ $(n = 1, 2, \dots)$ such*

*shouyu@quest.is.uec.ac.jp

†wakakuwa@quest.is.uec.ac.jp

‡ogawa@is.uec.ac.jp

that

$$\lim_{n\to\infty} \|\mathcal{L}_n(\psi_n^{AB}) - \phi_n^{AB}\|_1 = 0.$$

Here, $\|\cdot\|_1$ is the trace distance of two density operators.

In this contribution, we provide necessary and sufficient conditions for the asymptotic convertibility of two sequences of pure states in terms of *spectral entropy rates*, which are key ingredients in the information-spectrum method and defined as follows. Let $\widehat{\rho} = \{\rho_n\}_{n=1}^{\infty}$ be an arbitrary sequence of density operators, and $\widehat{\sigma} = \{\sigma_n\}_{n=1}^{\infty}$ be an arbitrary sequence of Hermitian operators. Then, for each $\varepsilon \in [0,1]$, the spectral divergence rates are defined by

$$\underline{D}(\varepsilon|\widehat{\rho}||\widehat{\sigma}) = \sup\left\{a \;\middle|\; \liminf_{n\to\infty} \mathrm{Tr}\rho_n\{\rho_n - e^{na}\sigma_n > 0\} \geq 1-\varepsilon\right\},$$
$$\overline{D}(\varepsilon|\widehat{\rho}||\widehat{\sigma}) = \inf\left\{a \;\middle|\; \limsup_{n\to\infty} \mathrm{Tr}\rho_n\{\rho_n - e^{na}\sigma_n > 0\} \leq \varepsilon\right\}.$$

Here, $\{A > 0\}$ denotes the spectral projection corresponding to the positive part of a Hermitian operator A. Using the spectral divergence rates, the spectral entropy rates are defined by

$$\underline{H}(\varepsilon|\widehat{\rho}) := -\overline{D}(\varepsilon|\widehat{\rho}||\widehat{I}), \quad \overline{H}(\varepsilon|\widehat{\rho}) := -\underline{D}(\varepsilon|\widehat{\rho}||\widehat{I})$$

for $\varepsilon \in [0,1]$, where $\widehat{I} = \{I_n\}_{n=1}^{\infty}$ is the sequence of identity operators. Especially, for $\varepsilon = 0$ we write

$$\underline{H}(\widehat{\rho}) = \underline{H}(0|\widehat{\rho}), \quad \overline{H}(\widehat{\rho}) = \overline{H}(0|\widehat{\rho}).$$

For any general sequences of bipartite pure states $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$, consider sequences of reduced states $\widehat{\psi}^{A} = \{\psi_n^{A}\}_{n=1}^{\infty}$ and $\widehat{\psi}^{B} = \{\psi_n^{B}\}_{n=1}^{\infty}$. Then it is easy to see that $\widehat{\psi}^{A}$ and $\widehat{\psi}^{B}$ have the same spectral entropy rates.

The main results of this contribution are as follows.

Theorem 2 (direct part) *Let $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$ and $\widehat{\phi}^{AB} = \{\phi_n^{AB}\}_{n=1}^{\infty}$ be general sequences of pure states on bipartite systems $\mathcal{H}_n^{AB}$ $(n = 1, 2, \dots)$. If $\underline{H}(\widehat{\psi}^{A}) > \overline{H}(\widehat{\phi}^{A})$ holds, then $\widehat{\psi}^{AB}$ can be asymptotically converted into $\widehat{\phi}^{AB}$ by LOCC.*

Theorem 3 (converse part) *Let $\widehat{\psi}^{AB} = \{\psi_n^{AB}\}_{n=1}^{\infty}$ and $\widehat{\phi}^{AB} = \{\phi_n^{AB}\}_{n=1}^{\infty}$ be general sequences of pure states on bipartite systems $\mathcal{H}_n^{AB}$ $(n = 1, 2, \dots)$. If $\widehat{\psi}^{AB}$ can be asymptotically converted into $\widehat{\phi}^{AB}$ by LOCC, it must hold that $\overline{H}(\varepsilon|\widehat{\psi}^{A}) \geq \overline{H}(\varepsilon|\widehat{\phi}^{A})$ and $\underline{H}(\varepsilon|\widehat{\psi}^{A}) \geq \underline{H}(\varepsilon|\widehat{\phi}^{A})$ for every $\varepsilon \in [0,1]$.*

As special cases, the above theorems lead to coding theorems for entanglement concentration [2, 3] and dilution [3]. Letting the target state $|\phi_n\rangle^{AB}$ be a maximally entangled state $|\Phi_{M_n}\rangle^{AB}$, with $M_n = e^{nR}$ be the Schmidt rank of $|\Phi_{M_n}\rangle$ and $R = \underline{H}(\widehat{\psi}^{A}) - \gamma$ $(\forall\gamma > 0)$, the above theorems show that the supremum of the achievable rates of entanglement concentration is equal to $\underline{H}(\widehat{\psi}^{A})$. On the other hand, letting the initial state $|\psi_n\rangle^{AB}$ be a maximally entangled state $|\Phi_{M_n}\rangle$, with $M_n = e^{nR}$ and $R = \overline{H}(\widehat{\phi}^{A}) + \gamma$ $(\forall\gamma > 0)$, we can see that the infimum of the required rates of maximally entangled states is equal to $\overline{H}(\widehat{\phi}^{A})$.

3 Conclusion

We analyzed asymptotic LOCC convertibility of sequences of bipartite pure entangled states and derived necessary and sufficient conditions for a sequence to be asymptotically convertible to another. Applying these results, we also provided a simple proof for the optimal rates of entanglement concentration and dilution in an information-spectrum setting.

References

[1] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations", *Phys. Rev. A* vol. 53, pp. 2046-2052, 1996.

[2] M. Hayashi, "General asymptotic formulas for fixed-length quantum entanglement concentration", *IEEE Trans. Inform. Theory*, vol. 52, pp. 1904–1921, 2006.

[3] G. Bowen and N. Datta, "Asymptotic entanglement manipulation of bipartite pure states", *IEEE Trans. Inform. Theory*, vol. 54, pp. 3677–3686, 2008.

[4] T. S. Han, *Information-Spectrum Methods in Information Theory*, Springer, 2002; Japanese edition: Baifukan-Press, 1998.

[5] S. Verdú and T. S. Han, "A general formula for channel capacity", *IEEE Trans. Inform. Theory*, vol. 40, pp. 1147–1157, 1994.

[6] H. Nagaoka, "On asymptotic theory of quantum hypothesis testing", in Proc. *Symp. Statistical Inference Theory and its Information Theoretical Aspect*, Tokyo, pp. 49–52, 1998 (in Japanese).

[7] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels", *IEEE Trans. Inform. Theory*, vol. 49, pp. 1753–1768, 2003.

[8] H. Nagaoka and M. Hayashi, "An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses", *IEEE Trans. Inform. Theory*, vol. 53, pp. 534–549, 2007.

[9] W. Kumagai and M. Hayashi, "A new family of probability distributions and asymptotics of classical and LOCC conversions", arXiv:1306.4166, 2013.

Attenuated quantum channel with probabilistic transmissivity

Kenshiro KITA[1] * Shinji KOYAMA[1] Minami TANAKA[1] Tsuyoshi Sasaki USUDA[1] †

[1] *School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*

Abstract. In quantum information theory, various results have been obtained regarding free-space quantum communication. However, in realistic quantum communication systems, it is necessary to consider fluctuations in amplitude and phase that are caused by such phenomena as turbulence and interference. In the present paper, we consider a model of an attenuated channel with probabilistic transmissivity and calculate the error probabilities of the homodyne and the optimum quantum receivers for binary phase shift keying coherent-state signals and show that the latter is always superior to the former.

Keywords: Quantum communication, attenuated channel, transmissivity, fading, error probability

1 Introduction

In the research on quantum communication [1], models of free-space, an ideal optical fiber, and transmission in the presence of thermal noise have been demonstrated so far. However, various types of classical noise in realistic quantum communication systems may exist. One that we must consider is the fluctuation of amplitude and phase, which is caused for example by turbulence and interference. Regarding the fluctuation of amplitude, many studies have been conducted for so-called Gaussian channels, which include the well-known pure-loss channel. Hence, we had focused our attention on phase diffusion (e.g., [2]) as a source of non-Gaussian noise and investigated an improvement in a quasi-optimum quantum receiver [3] and the robustness of the optimum quantum receiver [4].

In the present paper, we return to the topic of amplitude fluctuation and consider an attenuated quantum channel in which the transmissivity fluctuates probabilistically [5]. If the transmissivity obeys a non-Gaussian distribution, the amplitude noise is not Gaussian. We consider a normalized Rayleigh distribution and calculate the error probability of a homodyne receiver for binary phase shift keying coherent-state signals and demonstrate that the result approximates that of the well-known classical fading channel. We also calculate the error probability of the optimum quantum receiver and clarify that there is a clear gap between the error probabilities of the homodyne receiver and the optimum quantum receiver.

2 Channel model

Consider an attenuated channel in which the transmissivity is probabilistic due to for example fluctuation and interference.

2.1 Kraus representation of the channel

The Kraus operator of an attenuated channel with transmissivity η $(0 \leq \eta \leq 1)$ is [6]

$$E_k(\eta) = \sum_{n=0}^{\infty} \sqrt{\binom{n}{k}} \sqrt{\eta^{n-k}(1-\eta)^k}\, |n-k\rangle\langle n|\,, \quad (1)$$

where $k \in \mathbb{N}$ (the set of all natural numbers) and $|n\rangle$ is the eigenstate of the number operator having n photons. Suppose η obeys a probability distribution $P(\eta)$. Let ρ be an input state of this channel, i.e., a transmitted quantum state, and let ρ^{out} be an output state, i.e., a received quantum state. Then

$$\rho^{\text{out}} = \int_0^1 \left\{ P(\eta) \sum_{k=0}^{\infty} E_k(\eta) \rho E_k^{\dagger}(\eta) \right\} d\eta. \quad (2)$$

If the transmitted state is a coherent state $\rho = |\alpha\rangle\langle\alpha|$ with coherent amplitude α, Eq. (2) becomes

$$\rho^{\text{out}} = \int_0^1 \left\{ P(\eta)\, |\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha| \right\} d\eta. \quad (3)$$

In the following, we assume the transmitted state is a coherent state. Note that ρ^{out} is a statistical mixture of coherent states $\left|\sqrt{\eta}\alpha\right\rangle$, and therefore $P(\eta)$ can be regarded as a probability distribution of coherent amplitude $\sqrt{\eta}\alpha$.

2.2 Probability distribution of transmissivity

Suppose the probability distribution $P(\eta)$ corresponds to a Rayleigh distribution, which is a well-known non-Gaussian distribution. However, as $0 \leq \eta \leq 1$, we define a truncated and normalized distribution,

$$P(\eta) = \frac{\tilde{P}(\eta)}{\int_0^1 \tilde{P}(\eta) d\eta} = \frac{e^{-\frac{\eta}{\eta_0}}}{\eta_0 \left(1 - e^{-\frac{1}{\eta_0}}\right)}, \quad (4)$$

where η_0 $(0 \leq \eta_0 \leq 1)$ is related to the average of the original Rayleigh distribution $\tilde{P}(\eta) = \frac{1}{\eta_0} e^{-\frac{\eta}{\eta_0}}$ and characterizes the channel.

3 Error performance of BPSK signals

In this section, we derive the error performance of received quantum-state signals passing through the channel defined in the previous section. Assume that the modulation scheme is a binary phase shift keying (BPSK), which is the most fundamental digital modulation. We consider two receivers: a homodyne receiver, which is

*im161005@cis.aichi-pu.ac.jp
†usuda@ist.aichi-pu.ac.jp

the optimum classical receiver, and the optimum quantum receiver. Suppose quantum-state signals are coherent states. Then the transmitted quantum states are $\rho_0 = |\alpha\rangle\langle\alpha|$ and $\rho_1 = |-\alpha\rangle\langle-\alpha|$, which correspond to the classical information bits 0 and 1, respectively.

From Eq. (3), the received quantum states are

$$\rho_0^{(\mathrm{F})} = \int_0^1 P(\eta)\,|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|\,d\eta, \tag{5}$$

$$\rho_1^{(\mathrm{F})} = \int_0^1 P(\eta)\,|-\sqrt{\eta}\alpha\rangle\langle-\sqrt{\eta}\alpha|\,d\eta. \tag{6}$$

Here we assume *a priori* probabilities of signals are equal.

3.1 Homodyne receiver

As the signals are BPSK coherent states, the threshold value in the decision process in the receiver is zero. Hence, the homodyne receiver are formally described by the detection operators

$$\Pi_0 = \int_0^\infty |x_\mathrm{c}\rangle\langle x_\mathrm{c}|\,dx_\mathrm{c}, \quad \Pi_1 = \int_{-\infty}^0 |x_\mathrm{c}\rangle\langle x_\mathrm{c}|\,dx_\mathrm{c}, \tag{7}$$

and the error probability of the homodyne receiver is

$$P_\mathrm{e}^{\mathrm{Hom}} = \frac{1}{2}\left\{\mathrm{Tr}\,\rho_0^{(\mathrm{F})}\Pi_1 + \mathrm{Tr}\,\rho_1^{(\mathrm{F})}\Pi_0\right\} = \mathrm{Tr}\,\rho_0^{(\mathrm{F})}\Pi_1. \tag{8}$$

The second equality in Eq. (8) hold through the symmetry between the signals and detection operators. From Eqs. (5) and (8),

$$P_\mathrm{e}^{\mathrm{Hom}} = \frac{1}{\sqrt{2\pi\sigma^2}}\int_{-\infty}^0\int_0^1 P(\eta)e^{-\frac{(x_\mathrm{c}-\sqrt{\eta}\alpha)^2}{2\sigma^2}}d\eta dx_\mathrm{c}, \tag{9}$$

where $\sigma^2 = \frac{1}{4}$. Moreover, Eq. (9) can be expressed as

$$P_\mathrm{e}^{\mathrm{Hom}} = \frac{1}{2}\int_0^1 P(\eta)\mathrm{erfc}\left(\sqrt{2\eta}\alpha\right)d\eta, \tag{10}$$

where $\mathrm{erfc}\,(x) := \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt$. Note that the above error probability coincides with that of Rayleigh fading in classical theory (e.g., [7]) up to the integral range.

3.2 Optimum quantum receiver

The optimum quantum receiver is the receiver that attains the minimum value of the average probability of error, i.e., the Helstrom bound. For the binary quantum-state signals, the minimum error probability $P_\mathrm{e}^{\mathrm{Opt}}$ is [1]

$$P_\mathrm{e}^{\mathrm{Opt}} = \frac{1}{2}\left\{1 - \frac{1}{2}\,\mathrm{Tr}\left|\rho_0^{(\mathrm{F})} - \rho_1^{(\mathrm{F})}\right|\right\}. \tag{11}$$

3.3 Error performance

Figure 1 displays the error probabilities of the homodyne and the optimum quantum receivers based on Eqs. (10) and (11). A clear difference is seen in the error performance between the two receivers for BPSK signals. Moreover, within the large photon number regime, we find that the error probability of the optimum quantum receiver does not asymptotically approach that of the homodyne receiver, but rather the difference increases. Therefore, it is expected that this difference is maintained in the limit when quantum states are almost classical.

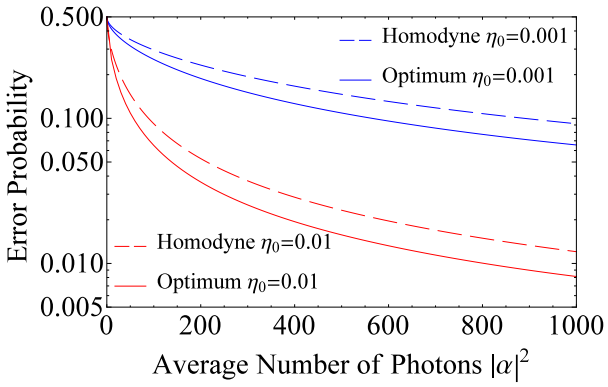


Figure 1: Error probabilities of the homodyne and the optimum quantum receivers.

4 Conclusion

In the present paper, we considered a model of an attenuated quantum channel with probabilistic transmissivity that obeys a non-Gaussian distribution and derived the error performance for the homodyne and the optimum quantum receivers. From the results we computed, superiority in quantum communication is seen over the entire range of the average number of photons. Furthermore, we showed that the error probability for the model almost coincides with that of a classical fading channel at least for the BPSK signals. We expect that the model provides a one-dimensional approximation of a quantum channel describing fading phenomenon [7, 8].

Acknowledgment This work has been supported in part by KAKENHI (Grant Numbers 24360151 and 16H04367).

References

[1] C.W. Helstrom, *Quantum detection and estimation theory*, Academic Press, New York, (1976).

[2] M.G. Genoni, S. Olivares, and M.G.A. Paris, Phys. Rev. Lett. **106**, 153603, (2011).

[3] S. Koyama, K. Nakahira, and T.S. Usuda, Proc. of AQIS2014, pp.185-186, (2014).

[4] S. Koyama and T.S. Usuda, Proc. of ISITA2014, pp.259-263, (2014).

[5] D.Yu. Vasylyev, A.A. Semenov, and W. Vogel, Phys. Rev. Lett. **108**, 220501, (2012).

[6] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, (2000).

[7] S. Stein and J.J. Jones, *Modern communication principle with application to digital signaling*, McGraw-Hill, (1967).

[8] S.D. Personick, Res. Lab. Electron., M. I. T., Cambridge, Tech. Rep. **477**, (1970).

Bridging the theory and experiment for device-independent quantum information

Pei-Sheng Lin[1] * Denis Rosset[1] † Yeong-Cherng Liang[1] ‡

[1] *Department of Physics, National Cheng Kung University, Tainan 701, Taiwan*

Abstract. Device-independent (DI) quantum information processing is a novel paradigm of quantum information where analyses are carried out directly from the observed correlations between measurement outcomes. While DI characterization of quantum states and measurements is intrinsically more robust, there remains an important gap between the theoretical tools developed for such purposes and the experimentally obtained correlations, which generically violate the non-signaling condition. In this work, we discuss some theoretical tools that may allows us to bridge this gap and compare how they perform under various sample sizes. This, in turn, provides insight on the minimal sample size needed for DI characterizations.

Keywords: Device-independent quantum information, finite statistics, quantum correlations

The ability to prepare quantum states of interest reliably and the ability to manipulate them at will are the basic requirements of *all* quantum information processing tasks. Typically, in order to certify that a desired quantum state has been prepared with some reasonable fidelity, quantum state tomography involving a daunting set of local measurements is carried out. If, instead, only specific properties of the quantum state are of interest, then a partial tomography in the form of appropriate witnesses (such as an entanglement witness) is employed.

Although these resource characterization procedures have been in place for a long time, the fact that we always have access to only finite sample size and that they rely on the detailed knowledge of the measurement performed make them susceptible to various systematic errors (see, for instance, [1] and references therein). Developing robust means to characterize quantum state in a practical setting is thus of fundamental importance for the implementation of quantum information processing tasks.

Incidentally, the relatively young field of device-independent quantum information [2, 3] provides a (partial but) natural solution to this problem. Within the paradigm of device-independence, the *analysis* of experimentally observed data is carried out without assuming the Hilbert space dimension of the physical system measured, let alone the measurements giving rise to these observed correlations. As such, this approach is inherently immune to, e.g., possible misalignment systematic error that may take place during the measurement procedure.

While a handful of theoretical techniques (see, e.g., [4, 5, 6]) have been developed for this rapidly emerging area of research, there remains some important gaps between many of these techniques and their actual implementation in physical systems. For example, with the assumption of samples being independent and identically distributed (i.i.d.), the correlations between measurement outcomes — which we represent using a collection of joint conditional probability distributions $\{P(\vec{a}|\vec{x})\}$ — are usually estimated as the observed relative frequencies of measurement outcomes. In the asymptotic limit when the number of sample size $N \to \infty$, quantum theory predicts correlations between measurement outcomes that satisfy the Born rule. (Henceforth, we refer to the set of distributions arising from quantum theory as $\mathcal{Q}$.)

In practice, however, one will always have access only to a finite amount of data. Thus, such estimated correlations always deviate from quantum prediction. In particular, they do not even satisfy the so-called non-signaling conditions [7]. On the other hand, all theoretical tools that have been developed for device-independent quantum information (either implicitly or explicitly) assume that the correlation observed satisfies the no-signaling condition. Our goal here is investigate a few generic set of tools that may allow one to bridge the aforementioned gap when one has access only to finite statistics.

The first of these bridging tools was proposed in [8], and amounts to finding the *nearest quantum approximation* (NQA)—according to certain norm —to the raw correlation $\vec{P}_{\text{Obs}}$ estimated from relative frequencies. In practice, as these does not seem to be a simple characterization of the set of quantum correlations, this amounts to solving some semidefinite program using the superset characterizations of the set of quantum distribution due to Navascués-Pironio-Acín (NPA) [4, 9] or its variant [6]. Hereafter, we refer to these supersets as $\mathcal{Q}_1 \supset \mathcal{Q}_2 \supset \ldots \supset \mathcal{Q}$. Moreover, for simplicity, in looking for the NQA, we use $\mathcal{Q}_1$ as our approximation to the quantum set in all subsequent discussions. In contrast, the second of this method—developed in [10]—first performs a canonical decomposition of any legitimate conditional probability distribution into a non-signaling part and a signaling part, followed by a projection onto the corresponding non-signaling subspace. For convenience, we henceforth refer to these methods, respectively, as the NQA method and the projection method.

Clearly, in the asymptotic limit of infinite sample size, both these methods would recover the prediction given by quantum theory. Their behavior when there is only finite data, in contrast, is not at all evident. In this work,

*yesiamfreeman@phys.ncku.edu.tw
†physics@denisrosset.com
‡ycliang@mail.ncku.edu.tw

we perform a systematic study of the reliability of these methods assuming various sample sizes. In particular, we employ the following two criteria:

(i) *Convergence criterion:* for any *given* quantum distribution $\{P_{\mathcal{Q}}(\vec{a}|\vec{x})\}$, we expect that the post-processed distribution obtained by a reliable bridging method is one that converges to $\{P_{\mathcal{Q}}(\vec{a}|\vec{x})\}$ as the sample size N increases

(ii) *Membership criterion:* since there is *a priori* no guarantee that the post-processed distribution $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ obtained from any of these methods to be in $\mathcal{Q}$, we demand that as N increases, the chance of finding $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ to admit a quantum representation to be increasing (or, at least, non-decreasing).

To quantitatively compare the reliability of these methods, we numerically simulate the outcomes obtained in a Bell-type experiment according to certain ideal quantum distributions $\{P_{\mathcal{Q}}(\vec{a}|\vec{x})\}$, assuming various sample sizes. We then use these simulated data to obtain $\vec{P}_{\text{Obs}}(\vec{a}|\vec{x})$ (by computing the relative frequencies) and post-process each such raw distribution $\vec{P}_{\text{Obs}}(\vec{a}|\vec{x})$ using one of the methods mentioned above to obtain $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$. To evaluate the reliability of these methods against the convergence criterion, the distance of each post-processed distribution to $\{P_{\mathcal{Q}}(\vec{a}|\vec{x})\}$ is computed, for simplicity, using the ℓ_1 norm. And to evaluate the reliability of these methods against the membership criterion, we check for the membership of each $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ against increasingly better approximations of the set of quantum correlations.

As a first example, we performed the simulation using the quantum distribution $\{\vec{P}^{\text{CHSH}}_{\mathcal{Q}}(\vec{a}|\vec{x})\}$ that leads to the maximal Clauser-Horne-Shimony-Holt (CHSH) [11] Bell-inequality violation. For both the projection method and the NQA method (assuming the ℓ_1, ℓ_2 and ℓ_∞ norm), basic fitting suggests that the *average* distance $\sum_{\vec{x},\vec{a}} \left|\vec{P}^{\text{projection}}_{\text{Proc}}(\vec{a}|\vec{x}) - \vec{P}_{\mathcal{Q}}(\vec{a}|\vec{x})\right|$ decreases essentially in all cases as $1/\sqrt{N}$, thereby showing that all these methods have preserved the rate of convergence of $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ to the ideal quantum distribution $\{\vec{P}^{\text{CHSH}}_{\mathcal{Q}}(\vec{a}|\vec{x})\}$.

On the other hand, for the membership test, we see that the NQA method with ℓ_1-norm performs considerably better than the projection method, while the NQA method with ℓ_2-norm has similar performance as the latter. Note that when subjected to the more stringent test of $\mathcal{Q}_2$ compared with $\mathcal{Q}_1$, the chance of finding a $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ within $\mathcal{Q}$ shrinks by a factor of 2 or more for all these methods (while going from or $\mathcal{Q}_2$ to $\mathcal{Q}_3$ makes hardly any difference). Interestingly, for all these methods, we see that the chance of obtaining $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ that lies inside $\mathcal{Q}_k$ for $k = 1, 2, 3$ rapidly converges at about $N \approx 200$. This therefore suggests that for any meaningful device-independent analysis, the minimal sample size needed is of the order of 10^2. In the poster, we will also present the corresponding plots assuming other ideal quantum distributions $\{P_{\mathcal{Q}}(\vec{a}|\vec{x})\}$.

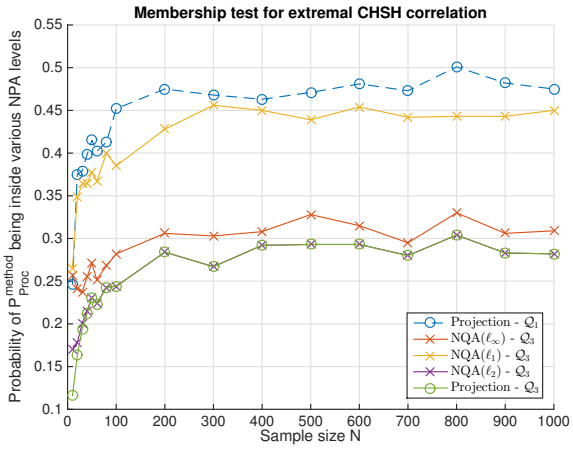


Figure 1: Average probability of finding $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ inside the various supersets of $\mathcal{Q}$, specifically $\mathcal{Q}_k$ for $k \in \{1, 3\}$. Each $\vec{P}^{\text{method}}_{\text{Proc}}(\vec{a}|\vec{x})$ is obtained by simulating the quantum distribution $\vec{P}^{\text{CHSH}}_{\mathcal{Q}}$ according to the sample size shown. The plot for $\vec{P}^{\text{NQM}}_{\text{Proc}}(\vec{a}|\vec{x})$ in conjunction with $\mathcal{Q}_1$ has been omitted as, by definition, each $\vec{P}^{\text{NQM}}_{\text{Proc}}(\vec{a}|\vec{x})$ is a member of $\mathcal{Q}_1$. For clarity, the corresponding plots for $\mathcal{Q}_2$ have been suppressed as they are essentially visually indistinguishable from the plots for $\mathcal{Q}_3$.

References

[1] D. Rosset *et al.*, Phys. Rev. A **86**, 062325 (2012); T. Moroder *et al.*, Phys. Rev. Lett. **110**, 180401 (2013); N. K. Langford, New J. Phys. **15**, 035003 (2013); S. J. van Enk and R. Blume-Kohout, New J. Phys. **15**, 025024 (2013); C. Schwemmer *et al*, Phys. Rev. Lett. **114**, 080403 (2016).

[2] N. Brunner *et al.*, Rev. Mod. Phys. **86**, 419 (2014).

[3] V. Scarani, Acta Phys. Slovaca **62**, 347 (2012).

[4] M. Navascués *et al.*, Phys. Rev. Lett. **98**, 010401 (2007).

[5] J.-D. Bancal *et al.*, *ibid.* **106**, 250404 (2011); Y.-C. Liang *et al.*, **114**, 190401 (2015); S.-L. Chen *et al.*, **116**, 240401 (2016).

[6] T. Moroder *et al.*, Phys. Rev. Lett. **111**, 030501 (2013).

[7] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994); J. Barrett *et al.*, Phys. Rev. A **71**, 022101 (2005).

[8] S. Schwarz *et al.*, New J. Phys. **18**, 035001 (2016).

[9] M. Navascués *et al.*, New J. Phys. **10**, 073013 (2008).

[10] D. Rosset, M.-O. Renou, and N. Gisin (in preparation).

[11] J. F. Clauser *et al.*, Phys. Rev. Let. **23**, 880 (1969).

Device-independent witnesses for entanglement depth: a case study

Jui-Chen Hung[1] * Yeong-Cherng Liang[1] †

[1] *Department of Physics, National Cheng Kung University, Tainan 701, Taiwan*

Abstract. We investigate a generalization of the family of device-independent witnesses for entanglement depth proposed in Liang *et al.* [Phys. Rev. Lett. **14**, 190401 (2015)] and its one-parameter generalizations. Specifically, we compute the device-independent k-producible bounds as a function of the number of parties n and an additional parameter γ for some small values of n. The effectiveness of these generalized witnesses against the original one is compared by determining the robustness of these witnesses against white noise for a few family of genuine multipartite entangled states. We also investigate the quantum violation of these witnesses by the generalized Greenberger-Horne-Zeilinger (GHZ) states.

Keywords: Device-independent quantum information, finite statistics, quantum correlations

With the advent of quantum information, the general perception of quantum entanglement [1] has been shifted from a bizarre feature offered by quantum theory to a useful *resource* for information processing. Indeed, by now, entanglement is a well-recognized resource in various quantum information tasks, from quantum key distributions, quantum communication to quantum computation etc. The reliable preparation of entangled quantum state and the characterization of the corresponding entanglement are thus important steps in these tasks.

Traditional means for characterizing quantum entanglement involves quantum state tomography, or the measurement of so-called entanglement witnesses, namely, Hermitian observables whose expectation value is guaranteed to be non-negative for separable states but which can be negative for at least one entangled state. While the measurement of such witnesses is much more preferably over a full-state tomography, it still shares a common drawback with the latter approach, namely, that it is highly susceptible to various systematic errors [2, 3, 4, 5] (especially in the presence of finite sample size), such as a misalignment systematic error [6]. A possible way to get around this issue is to measure, instead, a so-called device-independent witnesses for entanglement [7], where conclusions are drawn directly from the observed correlations between measurement outcomes, without any assumption of the Hilbert space dimension of the test state, or the measurements being implemented during the test.

In contrast with conventional approach for witnessing entanglement, a device-independent witness relies on the observation of Bell-nonlocal correlations, i.e., correlations that violate some Bell inequality [8, 9]. In a multipartite setting, the strength of violation of these correlations may even be used to witness the entanglement depth [10]—the extent to which the underlying system is many-body entangled—present in the system. See Figure 1 for an illustration of the notion of entanglement depth.

While the possibility to witness entanglement depth using Bell inequalities [11] was already recognized (implicitly) in some earlier works based on the Mermin-Ardehali-Belinskii-Klyshko inequalities [12], it was not until the work of [13] where this was properly formalized. In particular, the following family of device-independent witnesses for entanglement depth applicable to n parties, each allowed to perform two dichotomic measurements was proposed:

$$\mathcal{I}_n^k : 2^{1-n} \sum_{\vec{x}\in\{0,1\}^n} E_n(\vec{x}) - E_n(\vec{1}_n) \overset{k\text{-producible states}}{\leq} \mathcal{S}_k^{\mathcal{Q},*}, \quad (1)$$

where $\vec{x}$ is an n-bit string describing the choice of measurements for each party, $E_n(\vec{x})$ is the full n-partite correlator, i.e., the expectation value of the product of *all* n parties' measurement outcomes (each measurement outcome is assumed to be ± 1), and $\mathcal{S}_k^{\mathcal{Q},*}$ is the maximal possible quantum value of the left-hand-side of Eq. (1) when n is replaced by k. If the measurement statistics observed in an n-party Bell-type experiment gives rise to a value for the left-hand-side of Eq. (1) that is larger than $\mathcal{S}_k^{\mathcal{Q},*}$, then one can immediately conclude that the shared state *cannot* be k-producible [14] and thus must have an entanglement depth of at least $k+1$.

Towards the end of [13], a one-parameter generalization of the above witness was provided:

$$\mathcal{I}_n^k(\gamma) : \frac{\gamma}{2^n} \sum_{\vec{x}\in\{0,1\}^n} E_n(\vec{x}) - E_n(\vec{1}_n) \overset{k\text{-producible states}}{\leq} \mathcal{S}_{k,\gamma}^{\mathcal{Q},*}, \quad (2)$$

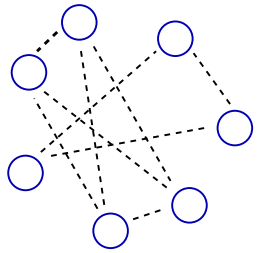


Figure 1: Schematic diagram showing the idea of an entanglement depth. Dashed-lines connecting any two circles symbolically represent that the two subsystems are entangled. The minimal many-body entanglement required to reproduce the quantum state associated with this system is 4, and thus this 7-partite system has an entanglement depth of 4.

*L26041040@mail.ncku.edu.tw
†ycliang@mail.ncku.edu.tw

where $0 < \gamma \leq 2$ and as above, $\mathcal{S}_{k,\gamma}^{\mathcal{Q},*}$ is the maximal quantum value of the left-hand-side of the above inequality when n is replaced by k. Notice that when $\gamma = 2$, the witness of Eq. (2) reduces to the witness of Eq. (1). While it was shown in [13] that Eq. (2) represent a legitimate family of device-independent witnesses for entanglement depth, the explicit form of the right-hand-side of Eq. (2), i.e., $\mathcal{S}_{k,\gamma}^{\mathcal{Q},*}$ has not been determined. The usefulness of these witnesses compared with the witness of Eq. (1) has also not been investigated. In this work, we address some of these issues and also investigate the quantum violation of these witnesses beyond the family of states considered in Ref. [13].

To determine $\mathcal{S}_{k,\gamma}^{\mathcal{Q},*}$, we adopt the ansatz given in [13]: we assume that the n parties share an n-partite Greenberger-Horne-Zeilinger (GHZ) state [15] $|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$, and that each party performs measurement described by the ± 1-outcome observables

$$A_{x_i=0} = \cos\alpha\,\sigma_x + \sin\alpha\,\sigma_y, \tag{3a}$$

$$A_{x_i=1} = \cos(\phi_n + \alpha)\,\sigma_x + \sin(\phi_n + \alpha)\,\sigma_y \tag{3b}$$

where $\alpha = -\frac{n-1}{2n}\phi_n$. The left-hand-side of Eq. (2) then evaluates to $\mathcal{S}_{n,\gamma}^{\mathcal{Q}}(\phi_n) = \gamma\cos^{n+1}\frac{\phi_n}{2} - \cos\left(\frac{n+1}{2}\phi_n\right)$, which can be maximized further over $\phi_n \in [0, \frac{\pi}{2}]$. Carrying this out explicitly, one can verify using a converging hierarchy [16, 17] of semidefinite programs and for $n \leq 5$ that the maximal quantum value of Eq. (2) can indeed be achieved via this ansatz, i.e., $\mathcal{S}_{n,\gamma}^{\mathcal{Q},*} = \max_{\phi_n} \mathcal{S}_n^{\mathcal{Q}}(\phi_n)$.

To compare the effectiveness of the generalized family of witnesses $\mathcal{I}_n^k(\gamma)$ against the original one $\mathcal{I}_n^k(2)$ for witnessing entanglement depth, we carry out numerical optimizations for the maximal quantum violation of these witnesses for the same four families of states considered in [13], namely, $|\mathrm{GHZ}_n\rangle$, the n-partite W-state [18], and the n-partite 1-dimensional cluster states [19] with opened (closed) boundary condition. Unfortunately, for the few values of $\gamma = \frac{\ell}{4}$ with $\ell = \{1, 2, \ldots, 7\}$ that we investigated, there does not seem to be any advantage of $\mathcal{I}_n^k(\gamma)$ compared with that of Eq. (1) (when measured in terms of their white-noise robustness).

Next, we investigate its quantum violation of these witnesses by the high-dimensional generalization of the GHZ state, i.e., $|\mathrm{GHZ}_{n,d}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes n}$. For even d, we consider the modified ansatz

$$A_{x_i=0} = \bigoplus_{j=0}^{\frac{d}{2}-1} \cos\alpha\,\sigma_x^{(2j,2j+1)} + \sin\alpha\,\sigma_y^{(2j,2j+1)}, \tag{4a}$$

$$A_{x_i=1} = \bigoplus_{j=0}^{\frac{d}{2}-1} \cos(\phi_n + \alpha)\,\sigma_x^{(2j,2j+1)} + \sin(\phi_n + \alpha)\,\sigma_y^{(2j,2j+1)} \tag{4b}$$

where the superscripts are used to label the qubit subspace [spanned by $\{|2j\rangle, |2j+1\rangle\}$] at which the Pauli matrices act on. For the same choice of parameters α and ϕ_n, this turns out to give exactly the same quantum value as with $|\mathrm{GHZ}_{n,2}\rangle = |\mathrm{GHZ}_n\rangle$. We thus know that $\mathcal{I}_n^k$ are also good device-independent witnesses for entanglement depth for states that are close to $|\mathrm{GHZ}_{n,d}\rangle$ for arbitrary $n \geq 2$ and arbitrary d even.

References

[1] R. Horodecki *et al*, Rev. Mod. Phys. **81**, 865 (2009).

[2] T. Moroder *et al*, *ibid.* **110**, 180401 (2013).

[3] N. K. Langford, New J. Phys. **15**, 035003 (2013).

[4] S. J. van Enk and R. Blume-Kohout, New J. Phys. **15**, 025024 (2013).

[5] C. Schwemmer *et al*, Phys. Rev. Lett. **114**, 080403 (2016).

[6] D Rosset *et al*, Phys. Rev. A **86**, 062325 (2012).

[7] J.-D. Bancal *et al*, Phys. Rev. Lett. **106**, 250404 (2011).

[8] N. Brunner *et al*, Rev. Mod. Phys. **86**, 419 (2014).

[9] V. Scarani, Acta Phys. Slovaca **62**, 347 (2012).

[10] A. S. Sørensen and K. Mølmer, Phys. Rev. Lett. **86** 4431 (2001).

[11] K. Nagata, M. Koashi, and N. Imoto, *ibid.* **89**, 260401 (2002); S. Yu *et al*, *ibid.* **90**, 080401 (2003).

[12] N. D. Mermin, *ibid.* **65**, 1838 (1990); M. Ardehali, Phys. Rev. A **46**, 5375 (1992); S. M. Roy and V. Singh, *ibid.* **67**, 2761 (1991); A. V. Belinskiĭ and D. N. Klyshko, Phys. Usp. **36** 653 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).

[13] Y.-C. Liang *et al*, Phys. Rev. Lett. **14**, 190401 (2015).

[14] O. Gühne *et al*, New J. Phys. **7**, 229 (2005).

[15] D. M. Greenberger *et al*, Phys. Rev. Lett. **65**, 3373 (1990).

[16] M. Navascués, S. Pironio, and A. Acín, *ibid.* **98**, 010401 (2007); New J. Phys., **10**, 073013 (2008); S. Pironio, M. Navascués, A. Acín, SIAM J. Optim. **20**, 2157 (2010).

[17] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner in *Proceedings of the 23rd IEEE Conference on Computational Complexity* (IEEE Computer Society, College Park, MD, 2008), pp. 199-210.

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

[19] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[20] J. F. Clauser *et al*, Phys. Rev. Lett. **23**, 880 (1969).

[21] N. Gisin and A. Peres, Phys. Lett. A **162**, 15 (1992).

Estimation on the execution time of a quantum computer from the analysis on quantum assembly code

Yongsoo Hwang[1] Byung-Soo Choi[1]

[1] *Electronics and Telecommunications Research Institute, Daejon, 34129, Republic of Korea*

Abstract. We analyze a quantum assembly code translated from a programmed quantum algorithm via a quantum computing compiler. From the analysis result, we estimate the running time of the algorithm on a quantum computer.

Keywords: quantum assembly code, quantum computer compiler, quantum algorithm, fault-tolerant quantum computing

Since the mid-1990s, a quantum computer has attracted much attention because several quantum algorithms such as factoring algorithm and unstructured data search algorithm were proposed [1]. It was proved that the algorithms have relatively low computational complexity than classical algorithms for the same problems. Therefore, it has been widely believed that a quantum computer that executes the algorithms can solve the problems much faster than a classical digital computer, even a supercomputer listed in the TOP500[1].

On the other hand, in the words of Pérez-Delgado and Kok [2], a quantum computer has to execute an efficient quantum algorithm efficiently. However, unfortunately nobody has seen that a quantum computer really finds the answer to the problems faster than a classical digital computer, even a mobile computing device.

To implement a practical quantum computer, we have to overcome a quantum noise problem. Quantum information is very susceptible to quantum noise, and thus it is almost impossible to keep the original state of quantum information long enough for a reliable computing without any protection. The fault-tolerant quantum computing based on a quantum error-correcting code is to date the most promising methodology to fight against quantum noise. The computing protocol allocates huge time (gate) and space (qubit) resource for a reliable quantum computing in spite of quantum noise.

By the way, due to the big overhead, it may be very difficult to keep the efficiency of the quantum computing algorithm in the real situation. In particular, by additional gates for the quantum error correction and fault-tolerant operations, it is very difficult to keep the fast problem-solving ability with the fault-tolerant protocol.

In this work, we try to see how much the fault-tolerant architecture affects the execution of quantum algorithms. For that reason, we first analyze quantum assembly codes translated from programmed quantum algorithms via a quantum computing compiler, and then estimate the running time of the algorithms. As is well known, an assembly code is positioned at the middle of the whole computing procedure from an algorithm to a signal controlling hardware devices. Consequently, we believe that it is reasonable to estimate the running time of a quantum computer from a quantum assembly code rather than a quantum algorithm itself.

A quantum computing compiler translates a programmed quantum algorithm into a quantum assembly code which consists of both of the quantum instructions for qubits and unitary gates and the reduced classical instructions [3, 4]. There are two types of quantum assembly codes, *modular* and *non-modular*. A modular code is made up of one main module and several sub-modules. The pre-defined sub-modules are called with qubit parameters during the execution of the main module. On the contrary, a non-modular code has one main module only. All the functions are stated in the main module without any structure.

There is no difference in the execution between both codes, but for the analysis the modular code is more useful because of its structure and small size. After performing the analysis on the sub-procedures, the results are combined to analyze the main module. From the analysis result, we can estimate the required resource and the running time of the quantum algorithm. In addition, we can also find critical areas that consume much resource.

For this work, we use an open quantum computing compiler *ScaffCC* that supports a programming language Scaffold [4, 5]. By using the compiler, we translate two quantum algorithms, Binary Welded Tree (BWT) and Ground State Estimation (GSE). The BWT is a graph traversal problem that finds a path from an entrance node to an exist node over a welded binary tree. The quantum BWT algorithm is based on quantum random walk, which provides an exponential speed up over a classical algorithm [6]. The GSE algorithm is a quantum simulation algorithm to find the ground state of a molecule [7].

For the analysis, we assume the following quantum system and fault-tolerant protocols. We employ the FCFS (First Come First Served) scheduling over quantum gates and 2D lattice for the qubit arrangement layout. In particular, the two-qubit operation is affected by the layout because qubits have to be re-positioned beforehand by following the layout.

We apply the fault-tolerant quantum computing protocol based on the concatenated Steane code. We differ the gate execution time according to the implementations of a logical gate, *transversal* and *non-transversal*. Further-

[1] http://www.top500.org

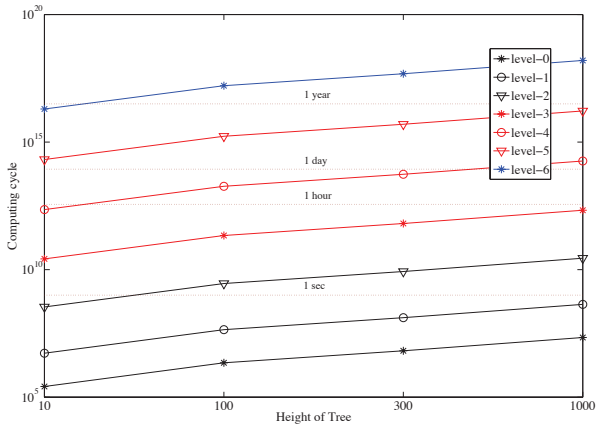


Figure 1: Time units for running BWT algorithm.

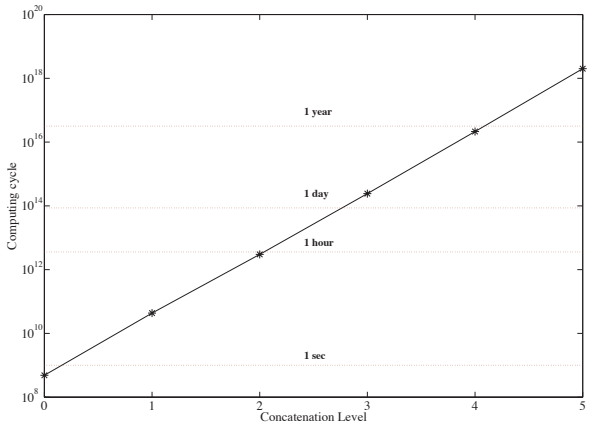


Figure 2: Time units for running GSE (M=04, b=09) algorithm.

more, because the level-1 logical qubit is not enough to satisfy a threshold of a quantum computing component, we vary the level of the concatenation. After each logical operation, the fault-tolerant quantum error correction based on Shor's scheme [8] is applied to logical qubits.

Fig. 1 shows the analysis result on the required time units for running the BWT algorithm. Note that the level-0 indicates an ideal quantum computing without logical operations and quantum error correction. For BWT problem, a critical input value is known as a height 300 [6, 9]. Note that the critical input value is the maximum input value (the height of a binary tree) it is believed that a classical digital computer solves efficiently. Which means that the BWT problem with a tree of height greater than 300 can be solved by a quantum computer faster than a digital computer. From our analysis result, the problem can be solved around 15 hours by a quantum computer under the assumptions: the quantum processor works at 1GHz and the concatenation level is 4. If a concatenation level is higher than 4, the required time increases remarkably, 58 days (level-5) and 15.2 years (level-6). But fortunately such a high concatenation level is not required [10].

Fig. 2 shows the analysis result about GSE (M=04, b=09) algorithms on varying the concatenation level. The critical input value for GSE is known as $M = 208$ [4], but unfortunately we did not analyze it because we could not compile the case due to the lack of classical computing power. For reference, the size of the quantum assembly code is bigger than 2G bytes even when $M = 64$.

References

[1] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[2] Carlos A Pérez-Delgado and Pieter Kok. Quantum computers: Definition and implementations. *Physical Review A*, 83(1):012303, January 2011.

[3] Krysta M Svore, A Aho, Andrew W Cross, and Isaac L Chuang. A Layered Software Architecture for Quantum Computing Design Tools. *Communications of the ACM*, pages 74–83, January 2005.

[4] Ali JavadiAbhari, Shruti Patil, Daniel Kudrow, Jeff Heckey, Alexey Lvov, Frederic T Chong, and Margaret Martonosi. ScaffCC: A Framework for Compilation and Analysis of Quantum Computing Programs. In *11th ACM Conference on Computing Frontiers*, pages 1–10, March 2014.

[5] Ali JavadiAbhari. ScaffCC. `https://github.com/ajavadia/ScaffCC`

[6] Andrew M Childs, Richard Cleve, Enrico Deotto, Sam Gutmann, and Daniel A Spielman. Exponential Algorithmic Speedup by a Quantum Walk. In *The thirty-fifth annual ACM symposium on Theory of computing (STOC03)*, pages 59–68, April 2003.

[7] James D Whitfield, Jacob Bimonte, and Alan Aspuru-Guzik. Simulation of Electronics Structure Hamiltonians Using Quantum Computers. *Journal of Molecular Physics*, 109(5):735–750, March 2011.

[8] Peter W Shor. Fault-tolerant quantum computation. In *37th Symposium on Foundations of Computing, IEEE Computer Society Press*, pages 56–65, January 1996.

[9] Amlan Chakrabarti, ChiaChun Lin, and Niraj K Jha. Design of Quantum Circuits for Random Walk Algorithms. In *2012 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 135–140. IEEE, August 2012.

[10] Tzvetan S Metodi, Darshan D Thaker, Andrew W Cross, Frederic T Chong, and Issac L Chuang. A Quantum Logic Array Microarchitecture: Scalable Quantum Data Movement and Computation. In *2005 International Symposium on Microarchitecture (MICRO-38)*, pages 1–12, September 2005.

Generating tripartite nonlocality from bipartite resources

Zhaofeng Su[1] * Yuan Feng[1] †

[1] *Centre for Quantum Computation and Intelligent Systems, University of Technology Sydney, Australia*

Abstract. Nonlocality is an important resource for quantum information processing. Tripartite nonlocality is more difficult to produce in experiments than bipartite ones. In this paper, we analyze a simple setting to generate tripartite nonlocality from two classes of bipartite resources, namely, two-qubit entangled pure states and Werner states. Upper bounds on the tripartite nonlocality, characterized by the maximal violation of Svetlichny inequalities, are given, and the optimal measurements to achieve these bounds are provided.

Keywords: Quantum information, tripartite nonlocality, Svetlichny inequality, Werner states

1 Motivation

Nonlocality is one of the most fundamental characteristics of quantum mechanics. The nonlocal quantum correlations existing between spatially separated quantum systems have significant advantages over classical correlations, thus serving as an indispensable resource for quantum information processing. In recent years, many novel applications of nonlocality have been developed for quantum computation and quantum communication [1], including communication complexity [2], quantum cryptography [3], randomness generation [4], and device independent quantum computation [5].

The quantum states which exibit nonlocal correlations are called nonlocal states. The nonlocality of a quantum state can be verified by Bell-type inequalities which give upper bounds on all local correlations that admit a local hidden variable (LHV) model [1]. For bipartite quantum systems, a sufficient criterion of being nonlocal is the violation of Clauser-Horner-Shimony-Holt (CHSH) inequality [6], while for tripartite systems, Svetlichny inequality plays a similar role [7].

In the last several decades, nonlocality of bipartite systems has been extensively investigated. However, the problem regarding multipartite nonlocality is much more complicated than the bipartite case, and very few works were presented in the literature. Even the nonlocality of three-qubit states, the simplest multipartite systems, is not well understood. In this special case, Ghose et al. derived an analytical expression of nonlocality for the generalized GHZ states and W states [11]. Later in 2010, Ajoy et al. extended this result to a set of more general GHZ-class states and W-class states [12].

In experiments, it is much harder to produce entangled tripartite systems than bipartite ones [13]. Note that being entangled is the necessary condition of being nonlocal for quantum systems. Therefore, it has practical meaning to generate tripartite nonlocal systems from bipartite ones.

*youngpath2012@gmail.com

†Yuan.Feng@uts.edu.au

2 Summary of Contribution

We analyze in this paper a simple setting, showed in Figure 1, for generating tripartite nonlocality from bipartite resources. There are three remotely located participants Alice, Bob, and Clare. Alice and Bob each shares a copy of the resource state ρ with Clare, denoted as ρ_{AC_1} and ρ_{BC_2} respectively. Clare then applies a CNOT operation on C_1 (the control qubit) and C_2 (the target qubit), and measures the system C_2 with some projective measurement. The tripartite nonlocality of the remaining systems ABC_1 will be quantified by the maximal violation of Svetlichny inequalities.

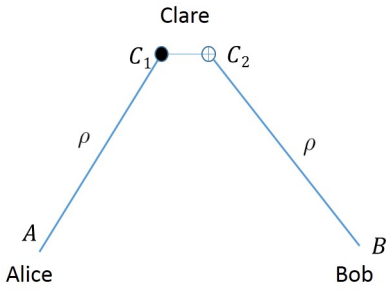


Figure 1: The setting for tripartite nonlocality generation.

Two different types of resource states are investigated in the paper: two-qubit Werner states

$$\rho_W = p|\Phi\rangle\langle\Phi| + (1-p)\frac{I}{4} \tag{1}$$

where $0 < p < 1$ and $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and arbitrarily entangled two-qubit pure states with the Schmidt decomposition

$$|\Phi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle, \quad 0 < \theta < \frac{\pi}{2}. \tag{2}$$

Our contributions are detailed as follows:

- *A simple way to evaluate the maximal violation of Svetlichny inequalities for a special class of three-qubit states.* We develop a technique to calculate the maximal violation of Svetlichny inequalities for a class of three-qubit states including both pure states and mixed states. With this technique, we are able to compute the maximal violation for generalized GHZ states $|\Psi_\theta\rangle = \cos\theta|000\rangle + \sin\theta|111\rangle$ which reads

$$S_{max}(\Psi_\theta) = \begin{cases} 4|\cos 2\theta| & \text{if } \sin^2 2\theta < \frac{1}{3} \\ 4\sqrt{2}|\sin 2\theta| & \text{if } \sin^2 2\theta \geq \frac{1}{3}. \end{cases}$$

  This result coincides with [11], but the proof is much simpler. Furthermore, the technique plays a crucial role in obtaining optimal measurements for generating tripartite nonlocality from bipartite resources considered in this paper.

- *Optimal measurement for generating tripartite nonlocality from Werner states.* Suppose a Werner state ρ_W as defined in Eq.(1) is used as the bipartite resource in Fig. 1, and Clare is only allowed to perform projective measurement in the $X-Z$ plain. Then the maximal Svetlichny inequality violation of the remaining states satisfies

$$p_0 S_{max}(\rho_0) + p_1 S_{max}(\rho_1) \leq 4p^2\sqrt{2},$$

  where ρ_0 and ρ_1 are the post-measurement states of system ABC_1 with the corresponding probabilities p_0 and p_1, respectively. The equality holds when the measurement according to the standard basis $\{|0\rangle, |1\rangle\}$ is applied. Furthermore, in this case the maximal violation $4p^2\sqrt{2}$ is achieved for both measurement outcomes, thus tripartite nonlocality will be generated *with certainty* if $p > 2^{-\frac{1}{4}} \approx 0.8409$.

- *Optimal measurement for generating tripartite nonlocality from two-qubit pure states.* Suppose $|\Phi_\theta\rangle$ as defined in Eq.(2) is used as the bipartite resource in Fig. 1, i.e. $\rho = |\Phi_\theta\rangle\langle\Phi_\theta|$ where

$$\begin{aligned} 0.4911 \approx \sqrt{\frac{1}{2} - \frac{1}{2}\sqrt{2-\sqrt{3}}} \;&\leq\; \cos\theta \\ &\leq \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{2-\sqrt{3}}} \;\approx\; 0.8711, \end{aligned}$$

  and Clare is only allowed to perform projective measurement in the $X-Z$ plain. Then the quadratic mean[1] of the maximal Svetlichny inequality violations of the remaining states satisfies

$$\sqrt{p_0 S_{max}(\Psi_0)^2 + p_1 S_{max}(\Psi_1)^2} \leq 4\sqrt{\frac{2\sin^2 2\theta}{1+\cos^2 2\theta}},$$

  where $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are the post-measurement states of system ABC_1 with the corresponding probabilities p_0 and p_1, respectively. Again, the equality holds when the measurement according to the standard basis $\{|0\rangle, |1\rangle\}$ is applied. Furthermore, in this case we have $S_{max}(\Psi_1) = 4\sqrt{2}$ and

$$S_{max}(\Psi_0) = \frac{4\sqrt{2}\sin^2 2\theta}{1+\cos^2 2\theta}. \tag{3}$$

  Thus tripartite nonlocality will be generated *with certainty* if

$$0.5412 \approx \sqrt{\frac{2-\sqrt{2}}{2}} < \cos\theta < \sqrt{\frac{\sqrt{2}}{2}} \approx 0.8409.$$

[1] For technical reasons, here we consider the quadratic mean, instead of the arithmetic mean as for the Werner states case, to quantify the tripartite nonlocality of the remaining states.

3 Acknowledgements

This research is partially supported by Chinese Scholarship Council (Grant No: 201206270069) and Australian Research Council (Grant No. DP160101652).

References

[1] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419-478, 2014.

[2] H. Buhrman, R. Cleve, S. Massar, and R. D. Wolf. Nonlocality and communication complexity. *Reviews of Modern Physics*, 82(1):665-698, 2010.

[3] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bells theorem. *Physical Review Letters*, 68(5):557-559, 1992.

[4] C. Dhara, G. Prettico, and Antonio Acn. Maximal quantum randomness in Bell tests *Physical Review A*, 88(052116), 2013.

[5] J. Barrett, L. Hardy and A. Kent No signaling and quantum key distribution. *Physical Review Letters*, 95(010503), 2005

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880-884, 1969.

[7] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a Bell-type inequality. *Physical Review D*, 35(10):3066-3069, 1987.

[8] S. Ghose, N. Sinclair, S. Debnath, P. Rungta, and R. Stock. Tripartite entanglement versus tripartite nonlocality in three-qubit GHZ states. *Physical Review Letters*, 102(250404), 2009.

[9] A. Ajoy, and P. Rungta. Svetlichny's inequality and genuine tripartite nonlocality in three-qubit pure states. *Physical Review A*, 81(052334), 2010.

[10] A. Zeilinger, M. A. Horne, H. Weinfurter, and Marek Zukowski. Three-particle entanglement from two entangled pairs. *Physical Review Letters*, 78(16):3031-3035, 1997.

Graph-Associated Entanglement Cost of Multipartite State in Exact and Finite-Block-Length Approximate Construction

Hayata Yamasaki[1] * Akihito Soeda[1] † Mio Murao[1] ‡

[1]*Department of Physics, Graduate School of Science, the University of Tokyo*
7–3–1 Hongo, Bunkyo-ku, Tokyo

Abstract. We introduce and analyze *graph-associated entanglement cost*, a generalization of the entanglement cost of bipartite quantum states to multipartite. We identify a necessary and sufficient condition for any multipartite entangled state to be constructible when quantum communication between the multiple parties is restricted to a network represented by a tree. The condition for exact construction is expressed in terms of the Schmidt ranks of the state defined with respect to edges of the tree. We also study approximate construction and provide a second-order asymptotic analysis.

Keywords: multipartite entanglement, entanglement cost, distributed construction of states

1 Introduction

Convertibility between multipartite quantum states by means of local operations and classical operation (LOCC) establishes a hierarchy on entanglement of the quantum states [1]. The convertibility results obtained in the LOCC framework also apply to more general non-LOCC settings, answering resource requirements for certain tasks. For instance, let there be two parties separated by some distance, who are connected by a quantum channel, but otherwise limited to LOCC. The optimal amount of quantum communication to asymptotically construct a shared entangled state equals the entanglement cost [2], since a noiseless qubit channel can be simulated by quantum teleportation with one Bell state besides LOCC.

This scenario generalizes to more parties connected by several quantum channels. The connectivity can be represented by a graph $G = (V, E)$, where each vertex $v \in V$ corresponds to a party and edge $e \in E$ to a channel. The total number of channels is not enough to characterize the network of channels. It amounts to the fact that the topology of the whole graph cannot be determined by the total number of edges. To represent a network connecting N parties, at least $N - 1$ edges are required. A connected graph of the least number of edges is called a *tree*.

If each channel at $e \in E$ has a limited capacity, say, of $\log_2 m_e$ qubits, the parties must suitably exploit the limited resources to construct a given state. Each noiseless quantum channel is equivalent to a maximally entangled state of m_e-level systems, which composes an initial resource state $|\Phi_{res}(G)\rangle$. The possibility of the pursued state construction is determined by a generalized notion of bipartite entanglement cost, which we name *graph-associated entanglement cost*.

We analyze the graph-associated entanglement cost of multipartite *pure* states under trees to achieve exact and approximate state construction. Our answer to the former is given in terms of the Schmidt rank [3] defined with respect to edges of the given tree. For the latter, we refine the analysis given in Ref. [4] and combine the results of Ref. [5] to provide the second-order asymptotic analysis.

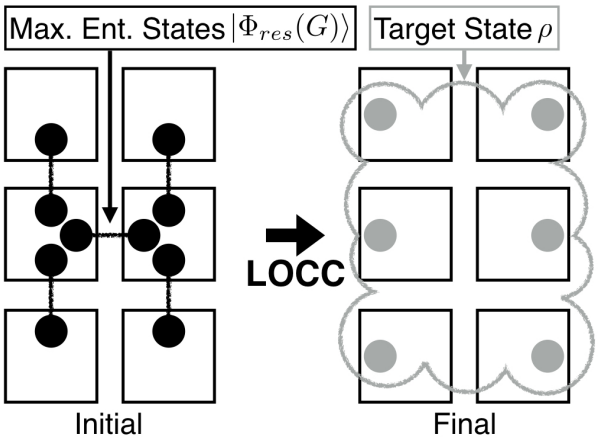


Figure 1: Construction of a multipartite entangled state ρ (gray circles) under a graph G. Parties (squares) are connected by quantum channels (lines) specified by G. Each channel is equivalent to LOCC and a maximally entangled state (a pair of black circles connected by a line), which composes a resource state $|\Phi_{res}(G)\rangle$. The construction task is to transform $|\Phi_{res}(G)\rangle$ into ρ by LOCC.

2 Multipartite State Construction and Graph-associated Entanglement Cost

We consider the tasks of *exact* and *approximate construction* of a multipartite entangled state ρ, as shown in Figure 1. In the LOCC framework, the *exact construction* under a graph G for a target state ρ is defined as a task to deterministically and exactly transform the initial resource state $|\Phi_{res}(G)\rangle$ into the target state ρ by LOCC. The (n, ϵ)-*approximate construction* under G for ρ is defined as a task to deterministically transform $|\Phi_{res}(G)\rangle$ by LOCC into an N-partite state $\tilde{\rho}_n$ which approximates

*yamasaki@eve.phys.s.u-tokyo.ac.jp
†soeda@phys.s.u-tokyo.ac.jp
‡murao@phys.s.u-tokyo.ac.jp

n copies of the target state $\rho^{\otimes n}$ up to ϵ in terms of the trace distance. Note that the system size for the initial resource state and the target state is not necessarily the same.

We define variants of graph-associated entanglement cost, namely graph-associated *total* entanglement cost and graph-associated *edge* entanglement cost. As $|\Phi_{res}(G)\rangle$ consists of bipartite maximally entangled states, we can quantify entanglement of $|\Phi_{res}(G)\rangle$ using *ebit*, which represents the entanglement entropy of a Bell state. The total amount of entanglement of $|\Phi_{res}(G)\rangle$ is the sum of the amount of bipartite entanglement at all the edges. The exact (or (n,ϵ)-approximate) graph-associated *total* entanglement cost is defined for a graph G and an N-partite state ρ as the minimum total amount of entanglement of $|\Phi_{res}(G)\rangle$ from which the exact (or (n,ϵ)-approximate) construction under G for ρ is achievable.

We define graph-associated *edge* entanglement costs to characterize distributed entanglement properties of multipartite states. There can be several optimal initial resource states minimizing the graph-associated total entanglement cost, and we assign an index i to represent different configurations of the optimal resource states. For a graph G and an N-partite state ρ, let $\left|\hat{\Phi}^i_{res}(G,\rho)\right\rangle$ denote the optimal initial resource state with configuration i for the exact construction under G for ρ. Then, *exact graph-associated edge entanglement cost* $E^G_{GC,i,e}(\rho)$ is defined as the amount of entanglement of the bipartite maximally entangled state prepared at edge $e \in E$ of $\left|\hat{\Phi}^i_{res}(G,\rho)\right\rangle$. Similarly, (n,ϵ)-*approximate graph-associated edge entanglement cost* $E^{G,n,\epsilon}_{GC,i,e}(\rho)$ is defined for the (n,ϵ)-approximate construction.

3 Graph-Associated Edge Entanglement Costs under Trees

We analyze the graph-associate entanglement costs under a special class of graphs, *trees*, which represent a network in which all the parties are connected by the smallest number of channels. We assume that target states are pure states, denoted by $|\psi\rangle$, for simplicity. When any edge $e \in E$ on a tree T is deleted, T is divided into two connected components. A reduced state ρ_e of $|\psi\rangle$ with respect to the edge e is defined as the one obtained by tracing out the systems belonging to one of the two components. We obtain the following theorems.

Theorem 1. *Exact graph-associated entanglement cost: For any tree $T=(V,E)$ and any N-partite pure state $|\psi\rangle$, the configuration i for the optimal resource state $\left|\hat{\Phi}^i_{res}(T,\psi)\right\rangle$ is uniquely determined, and, for each edge $e \in E$,*

$$E^T_{GC,i,e}(\psi) = \log_2 \operatorname{rank} \rho_e.$$

Theorem 2. (n,ϵ)*-approximate graph-associated entanglement cost: For any tree $T=(V,E)$, any N-partite pure state $|\psi\rangle$, any $\epsilon, n > 0$, and any configuration i for the optimal resource state of the (n,ϵ)-approximate construction, it holds that*

1. *upper bound: For error thresholds at respective edges denoted by $\epsilon'(e) > 0$ for each $e \in E$ satisfying $\sum_{e\in E} 2\epsilon'(e) \leqq \epsilon$,*

$$\sum_{e\in E} E^{T,n,\epsilon}_{GC,i,e}(\psi) \leqq \frac{\sum_{e\in E} \overline{H}_s^{\epsilon'(e)^2/4}(\rho_e^{\otimes n})}{n},$$

where $\overline{H}_s^{\epsilon'(e)^2/4}$ is the quantum information spectrum entropy defined in Ref. [5].

2. *lower bound: For any $\delta, \eta > 0$ and each $e \in E$,*

$$E^{T,n,\epsilon}_{GC,i,e}(\psi) \geqq \frac{\overline{H}_s^{\epsilon^2/4+\eta}(\rho_e^{\otimes n}) - \delta + \log_2 \eta}{n}.$$

To prove Theorem 1 and 2, we explicitly provide an optimal algorithm for *exact* construction, in which $|\psi\rangle$ is constructed in a distributed manner based on a recursive description of $|\psi\rangle$ under trees. *Approximate* construction of $|\psi\rangle^{\otimes n}$ can be achieved by exact construction of an approximate state $\left|\tilde{\psi}_n\right\rangle$ calculated from ϵ'. Our construction algorithms can save the maximum quantum memory space of parties.

Acknowledgment: The present work is supported by the Project for Developing Innovation Systems of MEXT, Japan, and JSPS KAKENHI (Grant No. 26330006, 15H01677 and 16H01050). We also acknowledge the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas MEXT KAKENHI (Grant No. 24106009)).

References

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009); S. Yang and H. Jeong, Phys. Rev. A **92**, 022322 (2015); K. Schwaiger, D. Sauerwein, M. Cuquet, J. I. de Vicente, and B. Kraus, Phys. Rev. Lett. **115**, 150502 (2015)

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996); P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001)

[3] B. M. Terhal and P. Horodecki, Phys. Rev. A **61**, 040301 (2000)

[4] E. F. Galvão and L. Hardy, Phys. Rev. A **62**, 012309 (2000)

[5] N. Datta and F. Leditzky, IEEE Trans. Inf. Theory **61**, 582 (2015)

Homological codes and abelian anyons

Péter Vrana[1] * **Máté Farkas**[2 3] †

[1] *Department of Geometry, Budapest University of Technology and Economics, Egry József u. 1., 1111 Budapest, Hungary*

[2] *Department of Theoretical Physics, Budapest University of Technology and Economics, Budafoki út 8., 1111 Budapest, Hungary*

[3] *Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

Abstract. We study a generalization of Kitaev's abelian toric code model defined on CW complexes. In this model qudits are attached to n dimensional cells and the interaction is given by generalized star and plaquette operators. These are defined in terms of coboundary and boundary maps in the locally finite cellular cochain complex and the cellular chain complex. We find that the set of energy-minimizing ground states and the types of charges carried by certain localized excitations depend only on the proper homotopy type of the CW complex. As an application we show that the homological product of a CSS code with the infinite toric code has excitations with abelian anyonic statistics.

1 Background

Homological quantum codes are a class of CSS codes with stabilizer generators constructed from finite dimensional chain complexes over a finite field and equipped with a distinguished basis. Algebraic topology is a rich source of such chain complexes, the main examples being the simplicial chain complex of a triangulated space and the cellular chain complex of a CW complex. From a purely coding-theoretic point of view, these are interesting because they offer the possibility to construct quantum LDPC codes from spaces with a "bounded local geometry". The first such example was the toric code introduced by Kitaev [1], which has constant stabilizer weights, $O(\sqrt{n})$ distance and constant dimension.

To every CSS code with a given set of stabilizer generators there is a canonically associated Hamiltonian. The interaction terms are -1 times the projections onto the subspaces fixed by each generator, and the ground state space coincides with the code space. Importantly, if the CSS code is constructed from a cellular chain complex, then the interaction terms are local (with respect to the underlying topology), making such codes promising candidates for a potential physical implementation. Additionally, the toric code is known to have another interesting feature, namely it exhibits topological order and has excitations resembling localized charged particles with anyonic statistics.

Ref. [2] introduced the homological product operation for CSS codes, which corresponds to the tensor product of the underlying chain complexes. This in turn is the algebraic counterpart of the cartesian product of topological spaces, but is also defined for abstract chain complexes. Important applications include ref. [3], where it was shown that the tensor product of two random chain complexes gives rise to asymptotically good codes with only $O(\sqrt{n})$ stabilizer weights, and ref. [4], where a specific family of product codes is shown to have a phase transition at a finite temperature.

The homological product construction thus seems to have interesting properties both at the level of abstract codes and for the corresponding physical systems with local Hamiltonians. In ref. [3] the following question was posed as one of the open questions: Do homological products of the toric code and some fixed code retain the property of having anyonic excitations? It is this question which served as the main motivation for our work.

2 Results

In order to rigorously formulate the question, we use the language of algebraic quantum field theory, following the similar analysis of the toric code model in refs. [5, 6]. In this framework, it is necessary to consider infinite systems, thus the torus in the toric code is replaced with a plane. It turns out that much of the analysis can be extended to more general spaces with the help of algebraic topology. For this reason, the starting point of our investigation is the following collection of data: 1) a locally finite CW complex E, 2) a finite abelian group G, and 3) a natural number n. The subsystems are described by the Hilbert space $\ell^2(G)$, and they live on the set $\mathcal{E}_n$ of n dimensional cells of E. The interaction terms (equivalently: stabilizer generators) are defined in terms of the boundaries of $n+1$-cells (for Z-type) and coboundaries of $n-1$-cells (for X-type). From these data one can construct a C*-algebra $\mathfrak{A}$ (quasilocal-algebra) together with a derivation encoding the infinitesimal time evolution.

To present the model more precisely, we introduce some notation. For any $g \in G$ we let X^g be the unitary acting on $\ell^2(G)$ as $|h\rangle \mapsto |g+h\rangle$ and for any $\chi \in \hat{G}$ we let Z^χ act as $|h\rangle \mapsto \chi(h)\,|h\rangle$. If γ is a formal linear combination of n-cells with coefficients in $\hat{G}$ (thought of as an n-chain), then Z^γ denotes the tensor product of the Z-type operators acting at the appropriate positions. Similarly, if δ is a formal linear combination of

*vranap@math.bme.hu

†mate.frks@gmail.com

n-cells with coefficients in G (a locally finite n-cochain), then X^δ denotes a product of X-type operators. For an $n-1$-cell e_α and an $n+1$-cell e_β we let

$$A_\alpha = \frac{1}{|G|}\sum_{g\in G} X^{\partial^T(ge_\alpha)} \text{ and } B_\beta = \frac{1}{|G|}\sum_{\chi\in\hat{G}} Z^{\partial(\chi e_\beta)},$$

where ∂ and ∂^T denote the boundary and coboundary operations, respectively. The Hamiltonian is the sum of $-A_\alpha$ and $-B_\beta$ over the $n\pm 1$ cells.

Since for every finite (compact) E the corresponding systems always possess frustration free ground states, it is natural to look for frustration free ground states in the infinite case as well, even though in this case there are also other ground states. We find that these ground states are in bijection with the set of *all* states on an algebra, which we call the logical algebra. The structure of this algebra is determined by the nth homology and locally finite cohomology groups with coefficients in $\hat{G}$ and G, respectively, and the canonical pairing between the two. Moreover, the bijection respects irreducibility, the factor property and quasiequivalence in both directions (the latter informs us about the possible phases of the system at zero temperature).

Having found these ground states, the next step is to look for endomorphisms which, when composed with a ground state, form states describing localized excitations. By analogy with the infinite toric code, in which case such endomorphisms can be obtained as conjugations with products of Z (X) operators along infinite paths (dual paths), the most general candidates are conjugations with arbitrary products of Z (X) operators on the n-cells. Such products can be conveniently encoded as locally finite n-chains (n-cochains). Clearly, some restrictions need to be made, otherwise the resulting states could have infinite energy, which is unphysical. The appropriate condition turns out to be that the boundary of the locally finite n-chain (coboundary of the n-cochain) has finite support. If γ_K and δ_K denote the restriction of γ and δ to a finite subset K of n-cells (i.e. removing the terms for cells outside K), the endomorphism is given by

$$\rho_{(\gamma,\delta)} : A \mapsto \lim_{K\to\mathcal{E}_n} Z^{\gamma_K} X^{\delta_K} A X^{-\delta_K} Z^{-\gamma_K}.$$

Such locally finite chains and cochains can be thought of as representatives of homology and cohomology classes at infinity, i.e. elements of $H^\infty_{n-1}(E;\hat{G})$ and $H^n_\infty(E;G)$. As usual in algebraic field theory, charged sectors are identified with certain equivalence classes of representations of the quasilocal algebra. It turns out that this equivalence class is left unchanged upon choosing a different representative of the (co-)homology classes at infinity in question.

For a partial converse, it is possible to introduce a unitary representation of $H^\infty_n(E;\hat{G})\times H^{n-1}_\infty(E;G)$ in the center of the von Neumann algebra generated by the GNS representation corresponding to these states. If these representations are inequivalent, then the equivalence classes of GNS representations are also different, i.e. these are invariants associated to the states. In many important cases these invariants are able to tell apart different charged sectors. If the GNS representation is $\pi_\omega : \mathfrak{A}\to\mathcal{B}(\mathcal{H})$, then the invariant is defined as

$$P_\omega([d]^\infty,[c]_\infty) := \lim_{K_\pm\to\mathcal{E}_{n\pm1}} \pi_\omega\left(X^{\partial^T(c-c_{K_-})} Z^{\partial(d-d_{K_+})}\right).$$

When E is essentially plane-like (e.g. the main example $E=\mathbb{R}^2\times F$ with F compact), then it is possible to introduce a canonical braiding on the category of localized endomorphisms. In this case the anyonic charged sectors correspond to elements of $H_{n-1}(F;\hat{G})$ and $H^{n-1}(F;G)$, and the braiding can be expressed via the Kronecker pairing between homology and cohomology classes. In the special case when F is a point and $n=1$, we recover the results for the toric code, where charged excitations are obtained using half-infinite paths and dual paths. In general, one can take the tensor product of an $n-1$-cycle ($n-1$-cocycle) in F with a half-infinite path (dual path), and these give rise to localized (i.e. particle-like) excitations having anyonic statistics.

References

[1] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.

[2] M. H. Freedman and M. B. Hastings, "Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs," *Quantum Information & Computation*, vol. 14, no. 1-2, pp. 144–180, 2014.

[3] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pp. 273–282, ACM, 2014.

[4] C. G. Brell, "A proposal for self-correcting stabilizer quantum memories in 3 dimensions (or slightly less)," *arXiv preprint arXiv:1411.7046*, 2014.

[5] P. Naaijkens, "Localized endomorphisms in Kitaev's toric code on the plane," *Reviews in Mathematical Physics*, vol. 23, no. 04, pp. 347–373, 2011.

[6] L. Fiedler and P. Naaijkens, "Haag duality for Kitaev's quantum double model for abelian groups," *arXiv preprint arXiv:1406.1084*, 2014.

On Thermalisation of Two-Level Quantam Systems

Sagnik Chakraborty, Prathik Cherian J, Sibasish Ghosh

Optics and Quantum Information Group, The Institute of Mathematical Sciences,
Taramani, Chennai 600113, India

Abstract

It has always been a difficult issue in Statistical Mechanics to provide a generic interaction Hamiltonian among the microscopic constituents of a macroscopic system which would give rise to equilibration of the system. One tries to evade this problem by incorporating the so-called $H-theorem$, according to which, the (macroscopic) system arrives at equilibrium when its entropy becomes maximum over all the accessible micro states. This approach has become quite useful for thermodynamic calculations using the (thermodynamic) equilibrium states of the system. Nevertheless, the original problem has still not been resolved. In the context of resolving this problem it is important to check the validity of thermodynamic concepts – known to be valid for macroscopic systems – in the microscopic world. Quantum thermodynamics is an effort in that direction. As a toy model towards this effort, we look here at the process of thermalization of a two-level quantum system under the action of a Markovian master equation corresponding to memory-less action of a huge heat bath, kept at certain temperature. A two-qubit interaction Hamiltonian (H_{th}, say) is then designed – with a single qubit mixed state as the initial state of the bath – which gives rise to thermalisation of the system qubit in the infinite time limit. We then look at the question of equilibration by taking the simplest case of a two-qubit system $A+B$, under some interaction Hamiltonian H_{int} (which is of the form of H_{th}) with the individual qubits being under the action of individual heat baths of temperatures T_1, and T_2. Different equilibrium phases of the two-qubit system are shown to appear – both the qubits or one of them get cooled down.

1 Introduction

Physical systems evolving towards an equilibrium state is a very common phenomenon. The nature of the process, taking any given initial state to a fixed final state, is non-invertible. So if one tries to give a quantum mechanical description of the process, it must be non-unitary. As we know all closed systems in quantum mechanics evolve through unitary operators, non-unitary evolution means a closed system description of equilibration is not possible. This suggests that one should take an open system approach to equilibration. Along this line Popescu et. al [3, 4] came up with the idea that although the whole system is undergoing a unitary process a part of the system can evolve towards equilibrium; the part of the system behaving as an open system. The usefulness of this process lies in the fact that although we get to study the equilibration process which is essentially non-unitary, all the nice structures of unitary dynamics are retained.

In this work [1], we take this approach and start with a known thermalization process: a qubit (system) interacting with a radiation field (bath). The corresponding master equation is called the quantum optical master equation. We device a unitary process so that the system qubit interacting with another ancilla qubit (bath) evolve in the same way as the solution of the quantum quantum optical master equation. Thus we give an joint unitary description of two qubits where one of them is thermalizing. We then go on to study a chain of qubits with nearest neighbour interaction (which we have taken to be two for simplicity) with each end connected

to a bath and the temperature of the two baths are different. We find that the system no longer behaves like its classical counter part. Rather different phases of cooling and heating of the qubits are obtained by varying the initial temperature of the baths.

2 Themalizing Hamiltonian

We start with a known thermalizing process - a qubit interacting with a bosonic bath - described by the quantum optical master equation.

$$\begin{aligned}\frac{d\rho}{dt} = \gamma_0(N+1)\left(\sigma_-\rho(t)\sigma_+ - \frac{1}{2}\sigma_+\sigma_-\rho(t) - \frac{1}{2}\rho(t)\sigma_+\sigma_-\right) \\ + \gamma_0 N\left(\sigma_+\rho(t)\sigma_- - \frac{1}{2}\sigma_-\sigma_+\rho(t) - \frac{1}{2}\rho(t)\sigma_-\sigma_+\right)\end{aligned} \tag{1}$$

Here, $N = (\exp\frac{E(\omega)}{k_B T} - 1)^{-1}$ is the Planck distribution. k_B is the Boltzmann constant, T is temperature and $E(\omega)$ is the energy at frequency ω. γ_0 is the spontaneous emission rate of the bath and $\gamma = \gamma_0(2N+1)$ is the total emission rate (including thermally induced emission and absorption processes). Here, γ gives the measure of temperature of bath

Solving this master equation gives us the evolution of the qubit. Our next step is to simulate this dynamics by appending a single qubit mixed state ancilla to the system qubit in order to find a corresponding 2-qubit unitary. By utilizing the work of G.Narang and Arvind [2], we succeed in doing this. And from this unitary we are able to extract a Hamiltonian. Since this Hamiltonian leads to thermalization of the system qubit, we call it the thermalizing Hamiltonian.

$$H_{th}(t) = f(t)\Big(|\phi^+\rangle\langle\phi^+| - |\phi^-\rangle\langle\phi^-|\Big) \tag{2}$$

where, $f(t) = \frac{\pm\gamma e^{-\gamma t/2}}{2\sqrt{1-e^{-\gamma t}}}, |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$

3 Two-qubit Interaction

Armed with the single qubit thermalizing Hamiltonian we try to extend our analysis to one-dimensional chain of qubits which has heat baths of different temperature at each end. We consider the simplest case of two qubits as shown in the figure.

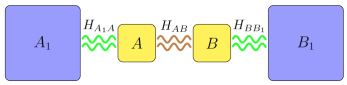


Figure 1: Two qubits A and B, which are associated with their individual baths A_1 and B_1, are interacting within themselves.

Here, A, B are the system qubits and $A1, B1$ are the corresponding ancillae representing respective heat baths. We are interested in the respective thermal behavior of the two system qubits A and B. The thermalizing hamiltonians $H_{A_1A}(t)$ and $H_{BB_1}(t)$ are given by,

$$H_{A_1A}(t) = a(t)\big(|\phi^+\rangle\langle\phi^+| - |\phi^-\rangle\langle\phi^-|\big)$$

$$H_{BB_1}(t) = b(t)\big(|\phi^+\rangle\langle\phi^+| - |\phi^-\rangle\langle\phi^-|\big)$$

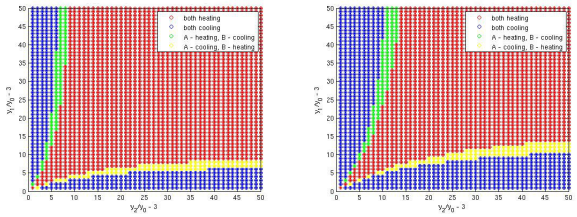
Where, $a(t) = \frac{\gamma_1 e^{-\gamma_1 t/2}}{2\sqrt{1-e^{-\gamma_1 t}}}$ and $b(t) = \frac{\gamma_2 e^{-\gamma_2 t/2}}{2\sqrt{1-e^{-\gamma_2 t}}}$

For simplicity, we take the interaction hamiltonian H_{AB} to be of the same functional form as the thermalizing Hamiltonian.

$$H_{AB}(t) = c(t)\big(|\phi^+\rangle\langle\phi^+| - |\phi^-\rangle\langle\phi^-|\big)$$

where, $c(t) = \frac{\gamma_3 e^{-\gamma_3 t/2}}{2\sqrt{1-e^{-\gamma_3 t}}}$

Now, we can calculate the total Hamiltonian and the time evolution operator. We turn to numerical calculations at this point and plot graphs that indicate whether heating/cooling has taken place for the system qubits A and B. Heating/cooling is decided by comparing the initial temperature of the qubits to their final equilibrium temperatures. Some examples for the plots are shown below (with thermal states as initial states of A, B)



The X and Y axes are the temperature measures of B_1 and A_1 respectively.Blue indicates that both qubits have cooled, red indicates that both have heated up and yellow/green indicate that one has cooled while the other has heated up.

4 Conclusions

We have here different phases of the two qubits A and B in the steady state case: (i) both of them may be cooled down to min. possible temperatures, (ii) both of them may be heated, or (iii) one of them gets cooled down and the other one gets heated. But, note that there is never any violation of the second law. Changing the form/strength of the interaction Hamiltonian H_{int} (t), we may get to see a completely different equilibrium phases No external source is acting on the two qubits (apart from their respective heat baths) In order to come up with a two-qubit refrigerator (with another qubit system being cooled down) – like in the case of [5] – we should consider a three-qubit system A + B + C (with a Hamiltonian approach)-starting from an optical master equation for a squeezed thermal bath (say).

The reference to the arxiv version of the main article is given in [1].

References

[1] S. Chakraborty, P. J. Cherian and S. Ghosh *On thermalization of two-level quantum systems* http://arxiv.org/abs/1604.04998

[2] Geetu Narang, Arvind *Simulating a single-qubut channel using a mixed state environment* Phys. Rev A **75**, 032305 (2007)

[3] S. Popescu, A. J. Short and A. Winter, *Entanglement and the foundations of statistical mechanics*, Nature Phys. **2**, 754-758 (2006).

[4] N. Linden, S. Popescu, A. J. Short and A. Winter, *Quantum mechanical evolution towards thermal equilibrium*, Phys. Rev. E **79**, 061103 (2009).

[5] N Linden, S Popescu, and P Skrzypczyk, *How Small Can Thermal Machines Be? The Smallest Possible Refrigerator*, Phys. Rev. Lett. **105**, 130401 (2010)

Optimization of Quantum Circuits with Multiple Outputs

Masato Onoda[1] * Kouhei Kushida[1] † Shigeru Yamashita[1] ‡

[1] *Graduate School of Sience and Engineering, Ritsumeikan University*

1 Introduction

In order to demonstrate the ability of quantum computing in the near future, an efficient quantum algorithm should be implemented efficiently. In general, a quantum algorithm includes a part to calculate (classical) logic functions corresponding to a problem instance. Thus, an efficient design technique for realization of a (classical) logic function should be very important even for quantum circuits, as pointed out in the literature (e.g., [1]). Therefore, the design methodology of reversible circuits has been studied very extensively in the reversible computation as well as quantum computation research communities.

There are many ways to design a reversible circuit to calculate a Boolean function; one of the most popular ways is to design an initial circuit consisting of Mixed Polarity Multiple-Control Toffoli (MPMCT) gates, and then decompose a large gate (i.e., with the large number of inputs) into elementary gates. In the latter part, there have been proposed many methods dedicated to reversible/quantum circuits.

For the first part, the important task is to find a small Exclusive-or Sum-Of-Products (ESOP) expression for a given Boolean function because we can generate a reversible circuit for a logic function by concatenating an MPMCT gate corresponding to each product term in the ESOP expression (as we will mention later). There are many ESOP-based synthesis methods; in the approaches our essential task is to find a small (with respect to the quantum cost) ESOP expression, which may be a pure classical logic synthesis problem.

Recently, the paper [2] proposed an idea to reduce quantum cost; we add MPMCT gates to change the given functionality so that the modified function has a smaller ESOP expression. However, the paper [2] only shows how to apply the idea to *a single output function*, and it is unclear how to deal with multiple-output functions. Thus, we propose a new method that can reduce quantum costs of multiple output functions by utilizing the same idea. Our method utilizes a property that we can "copy" a classical logic by using a CNOT gates. Our preliminary experimental results confirm that our new method can reduce quantum cost much more than using only previous method.

*dax@ngc.is.ritsumei.ac.jp
†is0112vk@ed.ritsumei.ac.jp
‡ger@cs.ritsumei.ac.jp

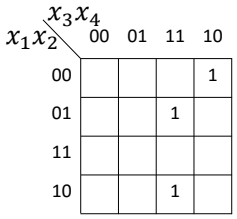


Figure 1: A Kmap for G_1.

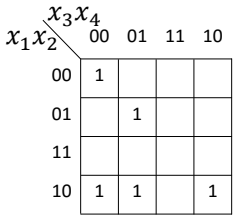


Figure 2: A Kmap for G_2.

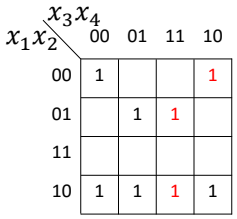


Figure 3: Kmap for $(G_1 + G_2)'$.

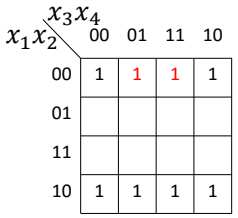


Figure 4: A Kmap after copying the function by a CNOT gate.

2 Reducing Quantum Cost by Adding MPMCT Gates

2.1 Previous Method

In the following, we refer to a blank cell or a cell having the 0 value as **0-value cell** in a Kmap. Also, a cell having the 1 value is called **1-value cell**. A **minterm** of a logic function is the combination of all the input variables (negative or positive) when the logic function becomes 1. Thus one minterm can corresponds to an MPMCT gate that has n control bits, which is called an $MPMCT_n$ gate in the following. One 1-value cell in a Kmap corresponds to one minterm in a logic function, and a rectangular consisting of 2^m 1-value cells corresponds to an $MPMCT_m$ gate.

Now let us explain the previous method in [2]. Let a circuit G have qubits, $x_1, \cdots, x_{n+1}$, and calculate a logic function with n variables $(x_1, \cdots, x_n)$ on x_{n+1}. Suppose we add an MPMCT gate whose (possibly many) control and target bits are some of $x_1, \cdots, x_n$ before and after G. Let the set of control bits of the added MPMCT gate be C and the target bit be x_t. Then, if there is a gate g in G such that the control bits of g is the same as $C + \{x_t\}$ and the polarities for the control bits of g and the added MPMCT gate are the same except for x_t, we need to change (i.e., invert) the polarity of x_t of g to keep the functionality of the circuit. This means that adding

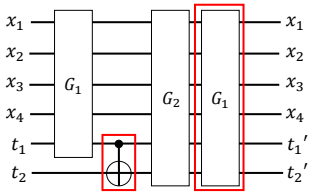


Figure 5: Copying the function of G_1 by a CNOT gate.

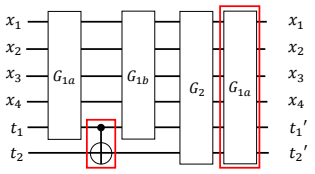


Figure 6: Copying a part of G_1 by a CNOT gate.

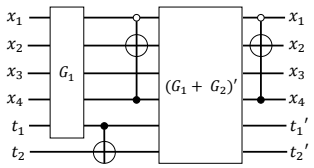


Figure 7: Applying previous method to Fig. 5.

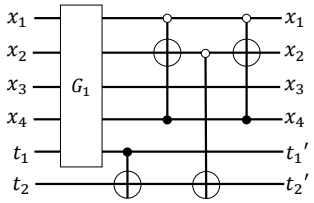


Figure 8: The final circuit.

an MPMCT can change the locations of 0-value cells and 1-value cells in a Kmap for the function realized by G. Therefore, if we add appropriate MPMCT gates, we can modify the given function so that it has a much simpler ESOP forms; the total quantum cost can be reduced. By using this modification, the previous method [2] can design a circuit for a single output function with lower quantum cost.

2.2 Our New Idea: Using CNOT Gates to Copy Classical Logic

The previous method explained in the previous section cannot deal with multiple-output functions efficiently. Here we propose an efficient method to treat multiple-output functions directly. Our idea is to use a CNOT gate to copy a classical logic between multiple outputs.

Let G_1 be a set of MPMCT gates whose target bits are all t_1. In other words, G_1 is a quantum circuit that calculates a Boolean function on t_1. Let also the Kmap for the function be as shown in Fig. 1. Further let G_2 be a set of MPMCT gates whose target bits are all t_2, and the Kmap for the function of G_2 be as shown in Fig. 2. Then let us consider to design a circuit that calculates the above two functions at the same time, i.e., two-output function. If we add a CNOT gates whose control bit is t_1 and target bit is t_2 between G_1 and G_2 as shown in Fig. 5, we can "copy" the function of G_1 at t_1 into the function of G_2 at t_2. This means that the circuit in Fig. 5 calculate the function that is exactly the same as G_2 at t_2 because any MPMCT gate-based circuit is self-inverse. In othe words, we can consider that the part of the circuit after the CNOT gate in Fig. 5 (i.e., G_1 and G_2) calculates the function whose Kmap is as shown in Fig. 3. Note that if we "copy" the 1-value cells in Fig. 1 to the Kmap as shown in Fig. 2, we get the Kmap as shown in Fig. 3. In conclusion, if the function after the above "copy" is easier to be designed than the function by only G_2, the total quantum cost of the circuit designed as Fig. 5 becomes smaller than the simple concatenation of G_1 and G_2. This is our idea in this paper.

We can copy only part of a circuit. Let G_1 be divided into two parts, G_{1a} and G_{1b}. Then, the circuit as shown in Fig. 6 can copy only the functionality of G_{1a}, and thus we need to design a circuit equivalent to G_2 and G_{1a} for the function on t_2 as shown in Fig. 6.

For the circuit as shown in Fig. 5, we can use the previous method [2] to design a circuit for the function realized by G_2 and G_1. Namely, we add two MPMCT gates before and after G_2 and G_1a. By this, the circuit becomes as shown in Fig. 7, and then our final circuit becomes as shown in Fig. 8.

3 Experimental Results and Conclusions

To evaluate our idea presented above, we performed the following experiment. We generated randomly two-output functions with four variables. We have ${}_{16}C_2 \times {}_{16}C_2 = 14{,}400$ functions even if we only consider the case when the number of minterms is two. Thus, we tried 10,000 randomly selected two-output functions with four variables having 2 to 7 minterms. For the randomly selected functions, we compared two methods; (1) we applied the previous method to each of the outputs, and combine the results, and (2) we applied our idea to add CNOT gates to copy appropriate partial function from one function to another function before applying the previous method. Then, we confirmed that our proposed method can achieve lower quantum cost for 95% cases, and it can reduce the quantum cost by approximately 12.5% compared to the previous method in average.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 24106009 and 15H01677.

References

[1] Shigeru Yamashita, Shin-ichi Minato and Miller D.Michael. DDMF:An Efficient Decision Diagram Structure for Design Verification of Quantum Circuits under a Practical Restriction. IEICE Transactions on Fundamentals of Electronics,Communications and Computer Sciences, pp. 3793–3802, 2008.

[2] Nurul Ain Binti Adnan, Kouhei Kushida, Shigeru Yamashita Pre-Optimization Technique to Generate Initial Reversible Circuits with Low Quantum Cost. Proc. IEEE International Symposium on Circuits and Systems (ISCAS), 2016, pp. 2298-2301.

Parallelization of Braiding Operations for Topological Quantum Computation

Kotaro Hoshi[1] * Shigeru Yamashita[1] †

[1] *Graduate School of Information Science and Engineering, Ritsumeikan University*

1 Introduction

Recently topological quantum computation [2] has been drawing much attention as one of the promising ways to realize fault-tolerant quantum computation. The topological quantum computation model perform computations by using braiding operations [2]. The most important issue is that any two operations can be performed parallelly when the braiding operations corresponding to the two operations are not physically overlapped [4]. For example, g_1 and g_2 in Fig. 1(a) can be performed parallelly because these are not overlapped with each other. Thus we can reduce a computational time of a circuit by parallelizing operations. Fig. 1(b) shows the parallelized circuit.

However, the number of combinations of operations to parallelize is enormous. Thus it is difficult to find a optimal way to parallelize a circuit. Therefore, we propose some heuristics to parallelize a circuit, and compare various methods. These heuristics decide sets of operations (*computational steps*) that can be performed parallelly from the beginning (left-hand side) of a give circuit. An example of a parallelized circuit is shown in Fig. 1(b) where a dotted-line box means a set of computational steps that can be performed parallelly.

In the followings, first, we describe an algorithm that is commonly used in these methods for listing candidates of computational steps that can be performed parallelly. Then, we propose three methods, a greedy method, a method based on a cost function and a probabilistic method to select good computational steps in the listed candidates. Our methods parallelize a whole given circuit by repeating the above two steps (i.e., listing candidates of computational steps and selecting one from the list.) Finally we report our experimental result which shows that the method based on a cost function and the probabilistic method produced good solutions.

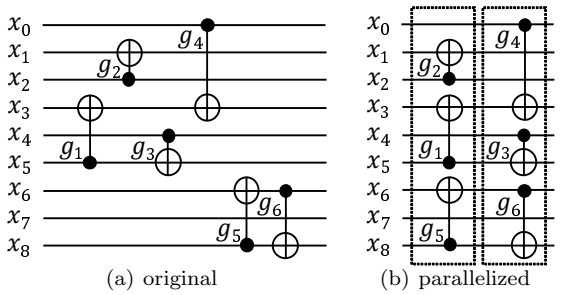


Figure 1: A quantum circuit.

*hossy@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp

2 Parallelization of a circuit

2.1 Listing candidates of computational steps

Recently, a promising implementation scheme for topological quantum computation has been proposed [2]; the implementation is divided into three parts, initialization part, a large array of only CNOT gates, and the measurement part. Thus it is very important to optimize a circuit consisting of only CNOT gates; we consider to optimize a circuit consisting of only CNOT gates. In the following, the target and the control qubits of gate g_i are denoted by $T(g_i)$ and $C(g_i)$, respectively.

First we introduce a terminology "overlapped."

Definition 1 *A pair of gates g_i and g_j are said to be* **overlapped** *if the line between $T(g_i)$ and $C(g_i)$ and the line between $T(g_j)$ and $C(g_j)$ overlap each other. If g_i and g_j are not overlapped, they are said to be* **non-overlapped** *with each other.*

For example, in the circuit as shown in Fig. 1(a), g_1 whose target and control bits are x_3 and x_5, respectively, and g_2 whose target and control bits are x_1 and x_2, respectively, are non-overlapped, whereas g_1 and g_3 whose target and control bits are x_5 and x_4, respectively, are overlapped. This is because two lines between x_3 and x_5, and between x_1 and x_2, are not overlapped, but two lines between x_3 and x_5, and between x_5 and x_4, overlap each other. If the two logical CNOT gates are non-overlapped, the braiding operations for the two CNOT gates can be performed in one logical time step in our model.

We can swap two CNOT gates, g_i and g_j , if $C(g_i) \neq T(g_j)$ and $T(g_i) \neq C(g_j)$. We refer this as **the swapping rule** in this abstract. For example, g_4 and g_5 in Fig. 1(a) can be swapped. However, g_1 and g_3 in Fig. 1(a) cannot be swapped because the control qubit of g_1 and the target qubit of g_3 are the same qubit (i.e., x_5).

To explain our method, we also need the following terminology.

Definition 2 *When g_i and g_j cannot be swapped by the swapping rule, and there is g_i before g_j, We say g_j* **depends on** *g_i.*

For example, g_3 depends on g_1 in Fig. 1(a) because $C(g_1)$ and $T(g_3)$ are the same. On the other hand, g_2 does not depend on g_1.

We explain our method to list up candidates of computational steps checking the above two relations (i.e., overlapped and dependence) of gates.

First, we create a directed acyclic graph, G_D, which represents the dependence relation between any two CNOT gates in a given circuit. A vertex in G_D correspond to a CNOT gate, and an edge between two vertices represents the dependence relation between the corresponding two CNOT gates. CNOT gates to be selected as a candidate computational step should be the source vertices in G_D.

Next, we create the undirected graph, G_S, from the source vertices in G_D. A vertex in G_S represents to a CNOT gate, and an edge between two vertices represents the non-overlapped relation between the corresponding two CNOT gates. It is obvious from our construction of the graphs that two CNOT gates whose corresponding vertices are adjacent to each other in G_S can be done at the same time. When we select some CNOT gates as a candidate computational step, there should be edges between any pair of all the vertices corresponding to the CNOT gates to be selected. This means that the vertices to be selected should compose a clique of G_S. Accordingly, we have to select a maximal clique in G_S as a candidate computational step in order to parallelize as many CNOT gates as possible. In our experiment, we utilized Bron-Kerbosch Algorithm [3] to list all maximal cliques in G_S. We consider the set of all these maximal cliques as the candidate of the computational steps to be parallelized.

2.2 Selecting computational steps

In the previous section, we described the method to list candidates of the computational steps to be parallelized. In this section, we explain how we can select one from the candidates. We can find the optimal solution by exhaustive search, which is unrealistic from the viewpoint of the computational complexity. Thus we propose three heuristics to select a possibly good computational steps from these candidates.

First, we describe a greedy method. The greedy method selects the maximum clique of the listed cliques in order to select the computational steps from the candidates. In other words, this is the method that parallelizes as many CNOT gates as possible from the beginning of a circuit.

Next, we describe the method based on a cost function. A cost function quantifies how a current situation is good statically. For our purpose, the cost function corresponds to weighting each of the listed cliques. Based on the cost function, the method selects the clique with the maximum weight. The difficulty for this method is that we still have not been able to find out a good cost function for this purpose; we consider finding a good cost function would be very difficult problem. Therefore, in our experiment we tried some cost functions and compared those. The result showed that we were able to find out a good solution when we considered the number of vertices that depend on a clique as the cost function value for the clique.

Finally, we describe the probabilistic method. As mentioned above, it is difficult to find out a good cost function. Therefore, we consider to use the method for selecting the good solution probabilistically instead of selecting based on pre-determined fixed cost function. For this purpose, we can use Monte-Carlo tree search [1] as a probabilistic method. Monte-Carlo tree search was proposed in the field of computer Go, and has been used to select the next move in any situation. In the research of computer Go, it has been known to be difficult to evaluate a situation by using a cost function similar to the case of selecting cliques. Therefore, the following idea was proposed; we play the game until the end by randomly (*playout*) from each candidate move, and select the move having the highest winning rate. However, we cannot get a good solution by simply calculating winning rates. Thus, we assign many playouts to promising moves, and make the search tree grow by expanding moves when the number of playouts exceeds a threshold. By this strategy, it has been known that we are able to efficiently select good moves with high accuracy.

Table 1: Execution results

circuit	greedy		cost function		probabilistic	
bits/gates	steps	time	steps	time	steps	time
16/100	82	0.00	68	0.00	64	0.54
16/500	190	0.01	166	0.02	157	250
49/500	116	0.02	91	0.11	88	180
100/500	81	0.15	74	0.74	66	1500
100/1000	161	0.14	128	2.50	135	12000

In the above Monte-Carlo tree search, the problem is how to define a promising move. One solution is to define that the value called "UCB1" for a promising move should be the maximum value. UCB1 is a value which is used to solve Multi-armed bandit problem [1].

We can apply Monte-Carlo tree search to our problem of selecting cliques as follows: we consider a move corresponds to selecting a clique, and a winning rate corresponds to the inverse number of the expected value of the number of the total computational steps. The reason why we consider an inverse number is that we want to minimize the number of computational steps for the problem of selecting cliques. Furthermore, we are able to normalize the value to $[0, 1]$ by inverting the number, and thus it is convenient to calculate UCB1.

2.3 Preliminary Experimental Result

We implemented the above three methods, and tried to minimize the computational steps of randomly selected circuits. The comparison results are shown in Table 1.

3 Conclusion

In this abstract, we propose three methods to parallelize a circuit for the reduction of computational steps for topological quantum computation. Our method parallelizes a circuit by repeating two steps; (1) listing the candidates of the computational steps, and (2) selecting the good computational steps from the candidates. Our method based on a cost function produces good results generally in short execution time. On the other hand, the probabilistic method needs more time but produces better results than the method based on a cost function. Thus there is a possibility that a better cost function exits, which means our future work is to find such a cost function. Also we would like to improve the execution time of the probabilistic method.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 24106009 and 15H01677.

References

[1] Guillaume Chaslot. Monte-carlo tree search. *Maastricht: Universiteit Maastricht*, 2010.

[2] Austin G Fowler, Ashley M Stephens, and Peter Groszkowski. High-threshold universal quantum computation on the surface code. *Physical Review A*, Vol. 80, No. 5, p. 052312, 2009.

[3] HC Johnston. Cliques of a graph-variations on the bron-kerbosch algorithm. *International Journal of Computer & Information Sciences*, Vol. 5, No. 3, pp. 209–238, 1976.

[4] Shigeru Yamashita. An optimization problem for topological quantum computation. In *2012 IEEE 21st Asian Test Symposium*, pp. 61–66. IEEE, 2012.

Performance of Coupled Systems as Quantum Thermodynamic Machines

George Thomas[1] * Manik Banik[1] † Sibasish Ghosh[1] ‡

[1] *Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India.*

Abstract. In this work we make a comparative study between coupled spin-1/2 systems and coupled quantum oscillators when they constitute as the working media of quantum thermodynamic machines. For this purpose, we consider anisotropic 1-D Heisenberg model of interaction between two spin-1/2 systems. Analogous interaction in the case of two oscillators is realized by considering quadratic coupling between positions and momenta of the two oscillators. Interestingly, we point out certain range of parameters for which the efficiency of the coupled oscillators outperform the efficiency obtained from coupled spin systems. With the same interaction, the coupled systems work as refrigerator for a different range of parameters and the coefficient of performance of coupled spins outperform that of the coupled oscillators.

Keywords: Otto cycle, coupled spin-1/2 system, coupled oscillators

1 Introduction

Study of thermodynamics in quantum regime can reveal fundamental features. As for example, the statement of the second law of thermodynamics in the presence of an ancilla [1, 2] or, when the system has coherence [3, 4], has been established in great details from where the classical version of the second law emerges under appropriate limits. Extension of thermodynamics to quantum regime can be approached in different directions such as information-theoretic point of view [5, 6, 7], resource-theoretic aspect [8], work extraction from quantum systems [9, 10, 11], etc. Different models of thermodynamic machines can be considered as useful tools to study in such directions. Such heat devices also help us to understand the behavior of thermodynamic quantities such as work and efficiency with non-classical feature such as entanglement, quantum superposition, squeezing, etc.

2 Results

Coupled systems as quantum heat engines are studied widely in recent past [12, 13, 14, 15, 16, 17]. It has been shown that appropriate coupling can increase the efficiency of the system compared to the uncoupled model [15]. The aim of the present work is to compare the performances of different coupled quantum systems when used as the working medium of a thermodynamic machines. For this purpose, we consider coupled spin-1/2 system and coupled quantum oscillator as working medium of quantum Otto cycle where the coupling in both the cases are taken to be of similar form (e.g. Heisenberg XX or XY interaction). Our findings are listed as follows: (i) we compare the efficiencies in the realm of increasing dimension of the system, (ii) we show that efficiency of a coupled system is bounded (both from above and below) in terms of the efficiencies of its parts (independent modes) when both the independent modes work in the engine mode, (iii) global efficiency decreases when a part of the coupled system works as refrigerator, (iv) for certain range of parameters the efficiency of the coupled oscillators outperforms the efficiency obtained from coupled spin systems, (v) with the same interaction, system work as refrigerator for a different range of parameters and the coefficient of performance of coupled spins outperform that of the coupled oscillators.

2.1 Quantum Otto cycle

Quantum Otto cycles are analogous to the classical Otto cycle, and the latter consists of two isochoric pro-

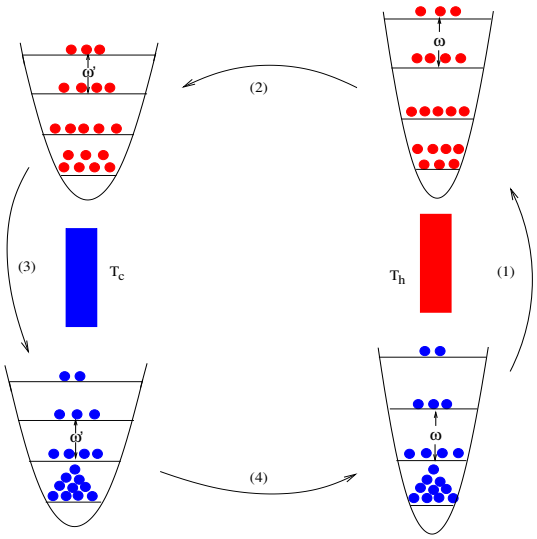


Figure 1: Pictorial representation of quantum Otto cycle. The working medium of this cycle is a harmonic oscillator. Stage 1 and Stage 3 are thermalization processes, in which the system exchanges heat with the bath. Stages 2 and 4 correspond to adiabatic processes where frequency of the oscillator changes from ω to ω' and back by doing certain amount of work.

*georget@imsc.res.in
†manik11ju@gmail.com
‡sibasish@imsc.res.in

cesses (work, $W = 0$) and two adiabatic processes (heat $Q = 0$). The system exchanges heat with the bath during the thermalization processes and the work is done when the system undergoes adiabatic process. Work and heat are calculated from the change in mean energies, where mean energy of the system represented by the state ρ and the Hamiltonian H is defined as $\mathrm{Tr}[\rho H]$.

2.2 Coupled oscillator and spin-1/2 system

Coupled oscillator: Consider two oscillators (labeled as 1 and 2) having same mass and frequency, and the Hamiltonian is given by,

$$H^{\rm os} = \frac{p_1^2}{2m} + \frac{p_2^2}{2m} + \frac{m\Omega^2}{2}x_1^2 + \frac{m\Omega^2}{2}x_2^2 + 2\left(\frac{m\Omega}{2}\lambda_x x_1 x_2 + \frac{1}{2m\Omega}\lambda_p p_1 p_2\right), \quad (1)$$

where λ_x and λ_p are the coupling strengths with same units as that of Ω. Under suitable co-ordinate transformation the Hamiltonian reads as,

$$H^{\rm os} = \frac{p_A^2}{2M_A} + \frac{M_A\Omega_A^2}{2}x_A^2 + \frac{p_B^2}{2M_B} + \frac{M_B\Omega_B^2}{2}x_B^2 \quad (2)$$

$$= \left(c_A^\dagger c_A + \frac{1}{2}\right)\Omega_A + \left(c_B^\dagger c_B + \frac{1}{2}\right)\Omega_B, \quad (3)$$

where $c_k^\dagger$ and c_k, where $k = A, B$, are the creation and annihilation operators for the independent oscillator modes A and B. Here Ω_A and Ω_B are eigenmode frequencies and M_A and M_B are the effective masses in the new co-ordinate frame. The explicit expressions are given as $M_{A/B} = \frac{m\Omega}{(\Omega\pm\lambda_p)}$,$\Omega_{A/B} = \sqrt{(\Omega\pm\lambda_p)(\Omega\pm\lambda_x)}$. While this coupled system is used as the working mideum of the above said Otto cycle, the total amount of heat absorbed by the system from hot reservoir is given by,

$$Q = \frac{\omega_A}{2}\left(\coth\left[\frac{\beta_h\omega_A}{2}\right] - \coth\left[\frac{\beta_c\omega'_A}{2}\right]\right) + \frac{\omega_B}{2}\left(\coth\left[\frac{\beta_h\omega_B}{2}\right] - \coth\left[\frac{\beta_c\omega'_B}{2}\right]\right). \quad (4)$$

The first (second) term Q_A (Q_B) denotes the heat absorbed by the system A (B). Similarly, the total work is the sum of the work done by the independent systems, $W = W_A + W_B$, which is given by,

$$W = \frac{(\omega_A - \omega'_A)}{2}\left(\coth\left[\frac{\beta_h\omega_A}{2}\right] - \coth\left[\frac{\beta_c\omega'_A}{2}\right]\right) + \frac{(\omega_B - \omega'_B)}{2}\left(\coth\left[\frac{\beta_h\omega_B}{2}\right] - \coth\left[\frac{\beta_c\omega'_B}{2}\right]\right) \quad (5)$$

The efficiency of the individual system is given as $\eta_k = 1 - \omega'_k/\omega_k$, where $k = \{A, B\}$. But the actual efficiency of the coupled system is defined as the ratio of total work over the total heat absorbed by the system. So we can write

$$\eta = \frac{W_A + W_B}{Q_A + Q_B} = \frac{\eta_A Q_A + \eta_B Q_B}{Q_A + Q_B}. \quad (6)$$

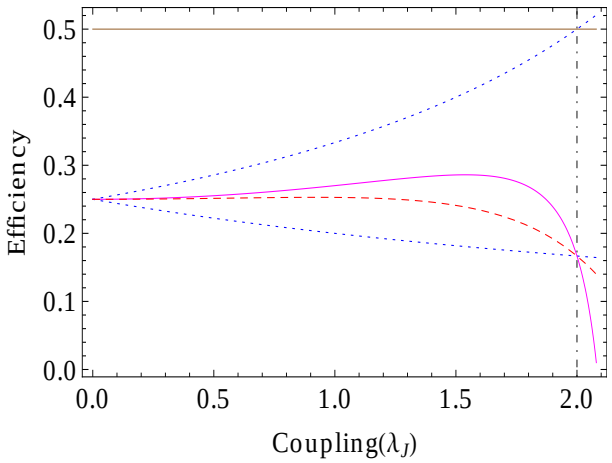


Figure 2: The two dotted curves show the upper bound (η_B) and lower bound (η_A) . The continuous curve represents the efficiency of the coupled oscillator. Efficiency of the coupled spin system is denoted by the dashed curve. Carnot value is represented by the horizontal line. When the independent systems work in engine mode, the global efficiency of the coupled system lies inside the bounds. The plot also shows that the global efficiency of the coupled oscillators is higher than that of the coupled spins for small values of λ_J. When the upper bound reaches Carnot value, $\eta_B = 1 - T_c/T_h$ for $\lambda_J = \lambda_c$ (represented by vertical dashed-dotted line), then we get $\eta^{\rm os} = \eta^{\rm sp} = \eta_A$. Here we take $T_h = 2$, $T_c = 1$, $\omega = 4$ and $\omega' = 3$.

When both the systems are working in engine mode (i.e., $Q_A > 0$ and $Q_B > 0$), we have,

$$\min\{\eta_A, \eta_B\} \leq \eta \leq \max\{\eta_A, \eta_B\}. \quad (7)$$

Coupled spin-1/2 system: Consider two spin-1/2 systems coupled via Heisenberg exchange interaction, i.e.,

$$H^{\rm sp} = B_z(S_1^z \otimes I + I \otimes S_2^z) + 2(J_x S_1^x S_2^x + J_y S_1^y S_2^y), \quad (8)$$

where J_x and J_y are the interaction constants along x and y directions. Likewise oscillator case, here also the Hamiltonian can be expessed as raising and lowering operators and under suitable coordinate transformations it can be expressed as in terms of two uncoupled spin modes. In the particular case $\lambda_x = J_x = \lambda_p = J_y = \lambda_J$(say) (in spin case, the model is known as Heisenberg XX model), the efficiencys of the coupled systems have been compared in Fig.2

3 Discussion

The coupled spins and coupled oscillators can also work as refrigerators. The refrigeration cycle is same as the cycle described for engine above provided refrigerators absorb heat from cold bath ($Q_c > 0$) and transfer it into hot bath ($Q_h < 0$). To transfer heat from the cold bath to the hot bath, work has to be done on the system and hence, we have $W = Q_h + Q_c < 0$. The coefficient of

performance (COP) is defined as $\zeta = Q_c/|W|$. Likewise efficiency, the global COP is bounded by COPs of the subsystems when both the the subsystems work as refrigerators. Interestingly we find that the global COP of the coupled spins is higher than that of the coupled oscillators for small values of λ_J.

To conclude, we compared the performance of coupled oscillators and coupled spins when they work as a heat engine. We choose suitable co-ordinate transformation to get two independent systems. The global efficiency is bounded by the efficiencies of the independent systems. We have also shown that such bounds exist when the system work as refrigerator. We also point out the range of parameters and form of interaction where the efficiency of the coupled oscillators is higher than that of the coupled spins. For two particular types of interactions, we show that the global COP is higher for coupled spins compared to coupled oscillators, whereas, with the same interaction, coupled oscillators found to be more efficient, when the system work as heat engine. Therefore coupling causes opposite effects in the figure of merits of heat engine and refrigerator.

References

[1] M. Horodecki and J. Oppenheim. Fundamental limitations for quantum and nanoscale thermodynamics. Nature Communications 4, 2059 (2013).

[2] F. Brando, M. Horodecki, N. H. Y. Ng, J. Oppenheim and S. Wehner. The second laws of quantum thermodynamics. PNAS **112**, 3275 (2015).

[3] M. Lostaglio, D. Jennings, and T. Rudolph. Description of quantum coherence in thermodynamic processes requires constraints beyond free energy. Nat Commun **6**, (2015).

[4] M. Lostaglio, K. Korzekwa, D. Jennings, and T. Rudolph. Quantum Coherence, Time-Translation Symmetry, and Thermodynamics. Phys. Rev. X **5**, 021001 (2015).

[5] R. Landauer. Irreversibility and Heat Generation in the Computing Process. IBM J. Res. Dev. **5**, 183 (1961).

[6] C. H. Bennett. The Thermodynamics of Computation- a Review. Int. J. Theor. Phys. **21**, 905 (1982).

[7] K. Maruyama, F. Nori, and V. Vedral. Colloquium: The physics of Maxwells demon and information. Rev. Mod. Phys. **81**, 1-23 (2009).

[8] F G. S. L. Brando, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens. Resource Theory of Quantum States Out of Thermal Equilibrium. Phys. Rev.Lett. **111**, 250404 (2013).

[9] P. Skrzypczyk, A. J. Short and S. Popescu. Work extraction and thermodynamics for individual quantum systems. Nat. Comm. **5**, 4185 (2014).

[10] M. Perarnau-Llobet, K. V. Hovhannisyan, M. Huber, P. Skrzypczyk, N. Brunner, and A. Acín. Extractable work from correlations. Phys. Rev. X **5**, 041011 (2015).

[11] A. Mukherjee, A. Roy, S. S. Bhattacharya, and M. Banik. Presence of quantum correlations results in a nonvanishing ergotropic gap. Phys. Rev. E **93**, 052140 (2016).

[12] R. Kosloff and T. Feldmann. Discrete four-stroke quantum heat engine exploring the origin of friction. Phys. Rev. E **65**, 055102 (2002).

[13] T. Feldmann and R. Kosloff. Quantum four-stroke heat engine: Thermodynamic observables in a model with intrinsic friction. Phys. Rev. E **68**, 016101 (2003).

[14] T. Zhang, W.-T. Liu, P.-X. Chen, and C-Z. Li. Four-level entangled quantum heat engines. Phys. Rev. A **75**, 062102 (2007).

[15] G. Thomas and R. S. Johal. Coupled quantum Otto cycle. Phys. Rev. E **83**, 031135 (2011).

[16] G. Thomas and R. S. Johal. Friction due to inhomogeneous driving of coupled spins in a quantum heat engine. Eur. Phys. J. B **87**, 166 (2014).

[17] J. Wang, Z. Ye, Y. Lai, W. Li, and J. He. Efficiency at maximum power of a quantum heat engine based on two coupled oscillators. Phys. Rev. E **91**, 062134 (2015).

Quantum Algorithm for Linear Equations with a Circulant Matrix

Souichi TAKAHIRA[1] * Asuka OHASHI[2] † Tomohiro SOGABE[3] ‡
Tsuyoshi Sasaki USUDA[1] §

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*
[2] *College of Science and Engineering, Ritsumeikan University, 1-1-1 Noji-Higashi, Kusatsu-shi, Shiga, 525-8577, Japan*
[3] *Graduate School of Engineering, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8603, Japan*

Abstract. Harrow, Hassidim, and Lloyd proposed the efficient quantum algorithm (HHL algorithm) for linear equations when the coefficient matrix is sparse and well-conditioned. The HHL algorithm can obtain a quantum state corresponding to the solution of the linear equations. Here we consider linear systems with circulant coefficient matrices and propose a quantum algorithm to obtain a quantum state of the solution. The proposed algorithm does not require Hamiltonian simulation, which is used in the HHL algorithm, because eigenvalues of circulant matrix can be obtained using quantum Fourier transform. The proposed quantum algorithm is roughly quadratically faster than the classical algorithm.

Keywords: Quantum algorithm, Linear equations, Circulant matrix

1 Introduction

Linear equations occur in science and engineering computation applications. There are many algorithms to solve linear equations, e.g., LU factorization and the conjugate gradient method. Harrow, Hassidim and Lloyd proposed a quantum algorithm (HHL algorithm) for linear equations [1]. The HHL algorithm outputs a quantum state $|x\rangle = A^{-1}|b\rangle$ with $O(\log(N))$ runtime and is exponentially faster than any classical algorithm, where A is a well-conditioned and sparse $N \times N$ matrix. Moreover, the HHL algorithm has some applications [2, 3, 4].

We wish to obtain a quantum state $|x\rangle$ for other matrix. We focus on the circulant matrix C, which appears in difference solutions of partial differential equations because the eigenvalues of C can be calculated using discrete Fourier transform.

Here, we propose a quantum algorithm to obtain $|x\rangle = C^{-1}|b\rangle$ for a specific case of the circulant matrix. The HHL algorithm obtains the quantum state $|x\rangle$ using Hamiltonian simulation [5]. In contrast, the proposed algorithm uses Amplitude Estimation (AE) [6] to obtain the quantum state $|x\rangle$. The proposed algorithm is roughly *quadratically faster* than the classical algorithm [7].

2 Known quantum algorithms

2.1 HHL algorithm

For a well-conditioned and sparse $N \times N$ matrix A, the HHL algorithm generates quantum state $|x\rangle$ that corresponds to the solution of the linear equations $A\vec{x} = \vec{b}$. The HHL algorithm assumes that we can efficiently prepare a quantum state $|b\rangle = \sum_{j=0}^{N-1} b_j|j\rangle$. The HHL algorithm first estimates the eigenvalues λ_j of A using phase estimation with Hamiltonian simulation $\mathrm{e}^{\mathbf{i}At}$, which can be implemented in $O(\log(N))$ runtime [5]. Next, the algorithm performs controlled rotation and inverse phase estimation. We obtain a quantum state $\sum_{j=0}^{N-1} \beta_j|u_j\rangle \left(\sqrt{1-\frac{\Gamma^2}{\lambda_j^2}}|0\rangle_a + \frac{\Gamma}{\lambda_j}|1\rangle_a\right)$, where $|u_j\rangle$ is the eigenvector of A, $\beta_j = \langle u_j|b\rangle$, $\Gamma = O(1/\kappa)$, and κ is the condition number of A. Finally, we measure the ancilla qubit. If we obtain 1, the quantum state becomes $\frac{1}{\sqrt{\sum_{k=0}^{N-1}|\beta_k/\lambda_k|^2}} \sum_{j=0}^{N-1} \frac{\beta_j}{\lambda_j}|u_j\rangle = |x\rangle$. If we obtain 0, the algorithm fails. Therefore, we use the Amplitude Amplification (AA) to obtain 1. Here, the total runtime is $O(\log(N)s^2\kappa^2/\epsilon)$, where s is the number of nonzero elements per row and ϵ is the allowable error.

2.2 Amplitude estimation

Let $\mathcal{A}$ be an unitary operator used to obtain quantum state $|\mu\rangle = \sum_{k=0}^{N-1} \mu_k|k\rangle$ for initial zero state $|0\rangle$, i.e., $\mathcal{A}|0\rangle = |\mu\rangle$. We can estimate $|\mu_j|$ by estimating the phase of the eigenvalues of $\mathbf{Q}_j = -\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_j$ using a technique that is similar to phase estimation, where $\mathbf{S}_j = (\mathbf{I}_N - 2\,|j\rangle\langle j|)$ and $\mathbf{I}_N$ is the $N \times N$ identity matrix. The eigenvalues of $\mathbf{Q}_j$ are given by $\mathrm{e}^{\pm\mathbf{i}2\theta_j}$, where θ_j is a real number such that $\sin(\theta_j) = |\mu_j|$.

We prepare $|\mu\rangle|0\rangle^m$ (m is the number of qubit and is relative to the estimation error) as the input state. If θ_j can be represented as $\theta_j = \pi\frac{z}{M}$ for any positive integer z, the AE can output the state $|\mu_j, g(\theta_j)\rangle = \frac{-\mathbf{i}}{\sqrt{2}}(\mathrm{e}^{\mathbf{i}\theta_j}|\mu_+^{(j)}\rangle|M\frac{\theta_j}{\pi}\rangle - \mathrm{e}^{-\mathbf{i}\theta_j}|\mu_-^{(j)}\rangle|M(1-\frac{\theta_j}{\pi})\rangle)$, where $|\mu_\pm^{(j)}\rangle$ is the eigenvector of $\mathbf{Q}_j$ and $M = 2^m$.

2.3 Parallel amplitude estimation

Let $\mathbf{Q}$ be an unitary operator $\mathbf{Q} = -(\mathbf{I}_N \otimes \mathcal{A}\mathbf{S}_0\mathcal{A}^{-1})\mathbf{S}$, where $\mathbf{S}$ is an unitary operator that changes the sign of the amplitude if and only if the first qubits equal the second qubits (i.e., $\mathbf{S}|j\rangle|j\rangle = -|j\rangle|j\rangle$ and $\mathbf{S}|j\rangle|i\rangle =$

*im151006@cis.aichi-pu.ac.jp
†a-ohashi@fc.ritsumei.ac.jp
‡sogabe@na.nuap.nagoya-u.ac.jp
§usuda@ist.aichi-pu.ac.jp

$|j\rangle|i\rangle$ for $j \neq i$). The eigenvalues and the corresponding eigenvectors are given by $|j\rangle|\mu_{\pm}^{(j)}\rangle$ and $\mathrm{e}^{\pm \mathbf{i}2\theta_j}$ for $j = 0, 1, \ldots, N-1$, respectively. For all j and any positive integer z, if the input state is $\sum_{j=0}^{N-1}|j\rangle|\mu\rangle|0\rangle^m$ and θ_j can be represented as $\theta_j = \pi\frac{z}{M}$, the parallel AE can output the state $\sum_{j=0}^{N-1}|j\rangle|\mu_j, g(\theta_j)\rangle$.

3 Circulant matrix

The circulant matrix C has the form:

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{N-1} \\ c_{N-1} & c_0 & c_1 & \cdots & c_{N-2} \\ c_{N-2} & c_{N-1} & c_0 & \cdots & c_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix}. \quad (1)$$

The eigenvalues λ_j of C are given by $\lambda_j = \sum_{k=0}^{N-1} c_k \mathrm{e}^{\mathbf{i}\frac{2\pi jk}{N}}$. We can obtain λ_j by applying quantum Fourier transform $\mathbf{F}_N$ to quantum state $|c\rangle = \sum_{k=0}^{N-1} c_k|k\rangle$. Specifically, $\mathbf{F}_N|c\rangle = \sum_{k=0}^{N-1}(\lambda_k/\sqrt{N})|k\rangle = \sum_{k=0}^{N-1}\mu_k|k\rangle =: |\mu\rangle$, where $\mu_k = \lambda_k/\sqrt{N}$.

The eigenvectors $|u_j\rangle$ corresponding to the eigenvalues λ_j are given by applying $\mathbf{F}_N$ to computational basis $|j\rangle$, i.e., $|u_j\rangle = \mathbf{F}_N|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{\mathbf{i}\frac{2\pi jk}{N}}|k\rangle$.

4 Main Algorithm

4.1 Outline

STEP 1 (state preparation):

We assume that $|b\rangle$ and $|c\rangle$ can be prepared efficiently. We prepare the quantum state $|b\rangle|c\rangle|0\rangle^m|0\rangle_a = \sum_{j=0}^{N-1}\beta_j|u_j\rangle|c\rangle|0\rangle^m|0\rangle_a$, where $|u_j\rangle$ is the eigenvector of the circulant matrix C and $\beta_j = \langle u_j|b\rangle$.

STEP 2 (parallel amplitude estimation):

We apply $\mathbf{F}_N^\dagger$ to the first quantum state and $\mathbf{F}_N$ to the second quantum state. Since $\mathbf{F}_N^\dagger|u_j\rangle = |j\rangle$ and $\mathbf{F}_N|c\rangle = |\mu\rangle$, we obtain $\sum_{j=0}^{N-1}\beta_j|j\rangle|\mu\rangle|0\rangle^m|0\rangle_a$. Next, we estimate $|\mu_j|$ for each j using parallel AE. Thus, we obtain

$$\sum_{j=0}^{N-1}\beta_j|j\rangle|\mu_j, g(\theta_j)\rangle|0\rangle_a. \quad (2)$$

STEP 3 (controlled rotation):

We perform a controlled rotation on the ancilla qubit with the third qubits as a control to obtain the following

$$\sum_{j=0}^{N-1}\beta_j|j\rangle|\mu_j, g(\theta_j)\rangle\left(\sqrt{1-\frac{\Gamma^2}{|\mu_j|^2}}|0\rangle_a + \frac{\Gamma}{|\mu_j|}|1\rangle_a\right), \quad (3)$$

where constant Γ is chosen to satisfy $|\Gamma/\sin(\pi z/M)| < 1$.

STEP 4 (inverse parallel amplitude estimation):

We undo the quantum states other than the ancilla qubit, i.e., we perform the inverse of **STEP 2** to obtain the following

$$\sum_{j=0}^{N-1}\beta_j|u_j\rangle|c\rangle|0\rangle^m\left(\sqrt{1-\frac{\Gamma^2}{|\mu_j|^2}}|0\rangle_a + \frac{\Gamma}{|\mu_j|}|1\rangle_a\right). \quad (4)$$

STEP 5 (measurement of the ancilla qubit):

We measure the ancilla qubit. If we obtain 1, then we have $\frac{1}{\sqrt{\sum_{k=0}^{N-1}|\beta_j\Gamma/\mu_j|^2}}\sum_{j=0}^{N-1}\frac{\beta_j\Gamma}{|\mu_j|}|u_j\rangle$ which equals to

$$\frac{1}{\sqrt{\sum_{k=0}^{N-1}|\beta_j/\lambda_j|^2}}\sum_{j=0}^{N-1}\frac{\beta_j}{|\lambda_j|}|u_j\rangle. \quad (5)$$

If we obtain 0, then the proposed algorithm fails. Thus, we use AA to obtain 1. If $|\lambda_j| = \lambda_j$ for all j, then obtained state (5) becomes $|x\rangle = C^{-1}|b\rangle$ corresponding to the solution.

4.2 Runtime

In parallel AE, the unitary operator $\mathbf{Q}$ that runs in $O(\log^2(N))$ is applied M times. The parallel AE requires $M = O(\sqrt{N}/\varepsilon)$ to estimate λ_j within error ε due to estimate $|\mu_j| = |\lambda_j|/\sqrt{N}$. Thus, parallel AE requires $O(\sqrt{N}\log^2(N)/\varepsilon)$ steps. The probability that we obtain 1 in **STEP 5** is $\Omega(1/\kappa^2)$, where κ is the condition number of C. Therefore, we require $O(\kappa)$ repetitions in AA. Thus, the total runtime of the proposed algorithm is as follows:

$$O(\kappa\sqrt{N}\log^2(N)/\varepsilon). \quad (6)$$

There is classical algorithm by using fast Fourier transform, which is $O(N\log(N))$ when used to solve linear equations $C\vec{x} = \vec{b}$. Therefore, the proposed algorithm is roughly quadratically faster than the classical algorithm in terms of N (i.e., the matrix size).

5 Conclusion

We have proposed a quantum algorithm to obtain quantum state $|x\rangle = C^{-1}|b\rangle$ for the circulant matrix C with which we can efficiently obtain eigenvalues using quantum Fourier transform. The proposed algorithm uses AE rather than Hamiltonian simulation to estimate eigenvalues. However, there are many constraints on the circulant matrix. Thus, in future, we plan to improve the proposed algorithm to remove such circulant matrix constraints. In addition, we plan to perform error analysis of the obtained quantum state.

Acknowledgment: This work has been supported in part by KAKENHI (Grant Nos. 24360151, 16H04367).

References

[1] A.W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett., **103**, 150502, (2009).

[2] B.D. Clader, B.C. Jacobs, and C.R. Sprouse, Phys. Rev. Lett., **110**, 250504, (2013).

[3] D.W. Berry, J. Phys. A: Theor., **47**, 105301, (2014).

[4] N. Wiebe, D. Braun, and S. Lloyd, Phys. Rev. Lett., **109**, 050505, (2012).

[5] D.W. Berry, G. Ahokas, R. Cleve, and B.C. Sanders, Commun. Math. Phys., **270**, pp.359-371, (2007).

[6] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, AMS Contemp. Math., **305**, pp.53-74, (2002).

[7] M. Chen, SIAM J. Numer. Anal., **24**, No.3, pp.668-683, (1987).

Quantum Circuit Design of Integer Division Optimizing Ancillary Qubits and T-Count

Himanshu Thapliyal[1] * T. S.S. Varun[1] Edgard Munoz-Coreas[1]

[1] *University of Kentucky, Lexington, KY, USA*

Abstract. In this paper, we present Clifford+T gates based quantum circuit design of integer division having n ancillary qubits. The proposed quantum circuit is based on restoring division algorithm. The proposed quantum circuit of integer division consists of (i) quantum circuitry of conditional addition operation, (ii) quantum circuitry of integer subtraction. To design ancillary and T-count optimized design of quantum integer division, the optimized quantum circuit design of integer conditional addition operation and integer subtraction are presented. The proposed quantum integer division circuitry has 50% improvement in terms of ancillary qubits, and 90% improvement in terms of T-count compared to the existing design of integer quantum division based on quantum fourier transform.

Keywords: Quantum Arithmetic, Quantum Circuits

1 Proposed Restoring Division Algorithm for Quantum Circuits

The proposed restoring division algorithm for quantum circuits is shown in Table 1. In Table 1, the inputs to be given are: (a) ($|Q_{[0:n-1]}\rangle$, n qubit register in which the dividend is loaded; (b) $|D_{[0:n-1]}\rangle$, n qubit register in which the divisor is loaded; (c) $|R_{[0:n-1]}\rangle$, n qubit remainder register which is initiated to 0 at the start. Therefore, for initiating $|R_{[0:n-1]}\rangle$, we require n number of ancillary qubits. The algorithm has to go through iteration processes. So, from the algorithm, we can see that at the end of n iterations, we get the quotient at ($|Q_{[0:n-1]}\rangle$ and remainder at $|R_{[0:n-1]}\rangle$. The divisor is retained at the output. The quantum circuits that are required for developing the hardware implementation of the proposed restoring division algorithm are (i) Leftshift operation circuitry, (ii) n qubit quantum subtractor and (iii)Conditional ADD operation circuitry. We observed that we can eliminate the LeftShift operation circuitry by combining $|R_{[0:n-2]}\rangle$ and ($|Q_{[n-1]}\rangle$ to form an n qubit register which is actually equal to performing an left shift operation. By combining the qubits in this way, we do not have to use a separate left shift operation circuitry.

1.1 Design of N Qubits Quantum Subtractor Module

The subtractor circuitry takes two n qubit inputs $a_{[0:n-1]}$ and $b_{[0:n-1]}$. The input a is regenerated at the output. The n-qubit output $s_{[0:n-1]}$ has the result of the subtraction of b and a, i.e., $b-a$. Fig.1 shows the circuit design of N qubit subtractor based on N qubit quantum ripple carry adder. The quantum ripple carry adder circuitry proposed in [2] or [3] can be used in developing the quantum subtractor circuitry.

1.2 Design of N qubit Quantum Conditional Adder Circuitry

The quantum Conditional ADD operation circuitry takes two n qubit inputs $a_{[0:n-1]}$ and $b_{[0:n-1]}$ and also a control qubit. The control qubit controls the operation of the whole circuitry. When the control qubit is low, both the inputs a and b are retained at the output. When the control qubit is high, while the input a is still retained without any changes, the output qubit register $s_{[0:n-1]}$ has the result of the sum of the qubits a and b. The complete working circuit of quantum conditional ADD operation circuitry is shown in Fig.2. Although, Fig.2 is just shown for 4 qubit operands, it can easily be extended to any operands sizes.

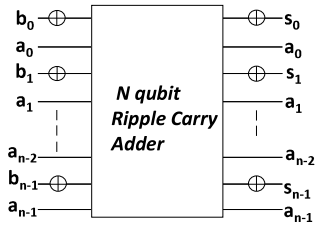


Figure 1: Circuit design of N qubits quantum subtractor based on N qubits quantum ripple carry adder

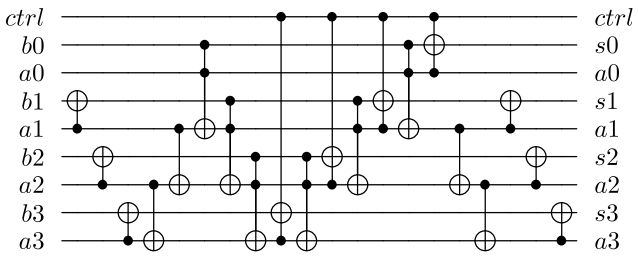


Figure 2: Circuit design of quantum conditional ADD operation circuit

*hthapliyal@uky.edu

Algorithm 1 : *Proposed Restoring division algorithm*

function *Restore* $(|Q_n\rangle, |R_n\rangle, |D_n\rangle)$
  for $i = 0$ *to* $n-1$ **do**
    $(|Q_{[1:n-1]}\rangle, |R_{[0:n-1]}\rangle) =$ Leftshift $(|Q_{[0:n-1]}\rangle, |R_{[0:n-1]}\rangle)$;
    $(|R - D_{[0:n-1]}\rangle = |R_{[0:n-1]}\rangle - |D_{[0:n-1]}\rangle$;
  if$(|R_{[0:n-1]}\rangle > 0)$ **then**
    $|Q_{[0]}\rangle = 1$
    $|R_{[0:n-1]}\rangle = |R - D_{[0:n-1]}\rangle$;
  else
    $|Q_{[0]}\rangle = 0$;
    $|R_{[0:n-1]}\rangle = |R - D_{[0:n-1]}\rangle + |D_{[0:n-1]}\rangle$;
  end if;
  end for;
//repeat for n iterations//
return R;
end function

Table 1: Proposed Restoring division algorithm for quantum circuits

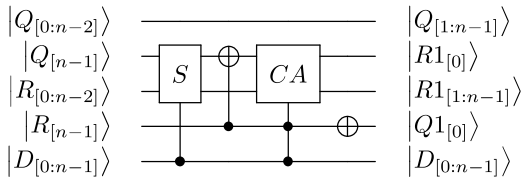


Figure 3: Quantum restoring integer divider circuitry design for a single iteration

2 Proposed Design for Quantum Restoring Integer Division circuitry

Fig.3 shows the proposed quantum circuit of restoring division. We now elaborate on how information moves through the circuit.

Step 1. The $|D_{[0:n-1]}\rangle$ holds the divisor, $|R_{[0:n-1]}\rangle$ initialised to zero, and $|Q_{[0:n-1]}\rangle$ holds the dividend.

Step 2. We consider, $|Q_{[n-1]}\rangle$ and $|R_{[0:n-2]}\rangle$, as one combined register. This allows us to not use a left shifting circuit. In Fig.3, S represents subtractor circuitry and CA represents conditional adder circuitry.

Step 3. The combined register mentioned above in Step 2, and $|D_{[0:n-1]}\rangle$ are given as inputs to the quantum subtractor circuitry. Register $|D_{[0:n-1]}\rangle$ emerges unchanged. The combined register now holds $|R - D_{[0:n-1]}\rangle$.

Step 4. Qubits $|R - D_{[n-1]}\rangle$ and $|R_{[n-1]}\rangle$ are sent to Feynman gate. $|R - D_{[n-1]}\rangle$ is the control qubit and the $|R_{[n-1]}\rangle$ is the target qubit. The target now holds the value of $|R - D_{[n-1]}\rangle$ because $|R_{[n-1]}\rangle$ is always zero throughout the computation.

Step 5. The $|R_{[n-1]}\rangle$ computed in Step 4 now becomes the control qubit to the conditional ADD circuit. $|R - D_{[0:n-1]}\rangle$ and $|D_{[0:n-1]}\rangle$ are the two n bit inputs to the conditional ADD operation circuit. The outputs of conditional ADD operation are collected. $|R_{[n-1]}\rangle$ is complemented.

Step 6. All the above operations constitute the first iteration. The outputs of first iteration will be used as inputs for the next iteration. The order of the output qubits of the first iteration is altered and arranged again as in the Fig.3. Then these altered qubits are given as inputs qubits to the second iteration.

Step 7. This process continues for n iterations. The circuit has to go through from steps 1 to 6 each time till it reaches n iterations.

Step 8. At the end of n iterations, we have Quotient in $|Qn_{[0:n-1]}\rangle$, remainder in $|Rn_{[0:n-1]}\rangle$ and the divisor is retained. The dividend is not stored in our implementation.

The resources used in the design of the proposed quantum restoring integer division circuitry is presented in Table 2. As shown in Table 2, the proposed design will require n ancillary qubits during initialization of remainder register.

Table 2: Resource count of proposed division circuitry

Designs	Ancillaries	T-count
n Subtractor	0	$n*(14n-14)$
n conditional ADDER	0	$n*(21n-14)$
Initial Ancilla qubits	n	0
Total cost	n	$35n^2-28n$

Table 3: Comparison of resource count between proposed and existing division circuitries

Designs	Ancillaries	T-count
existing design [1]	$2n$	$\approx 400n^2$
proposed design	n	$35n^2-28n$
Improvement ratio	50%	$\approx 91\%$

3 Comparison

We compared our proposed quantum restoring divider circuitry with the existing design in [1].We compare the ancillaries and T-count. T-count of the existing quantum circuitry of integer division in [1] is calculated for 3, 4 and 5 qubits and extrapolated for n qubits. The proposed quantum circuitry of integer division has an improvement ratio of 50% in terms of ancillary qubits, and 91% in terms of T-count compared to [1].

References

[1] Khosropour, A., Aghababa, H. and Forouzandeh, B., 2011, April. Quantum Division Circuit Based on Restoring Division Algorithm. In 2011 Eighth International Conference on Information Technology: New Generations.

[2] Thapliyal, H. and Ranganathan, N., 2013. Design of efficient reversible logic-based binary and BCD adder circuits. ACM Journal on Emerging Technologies in Computing Systems (JETC), 9(3), p.17.

[3] Cuccaro, S.A., Draper, T.G., Kutin, S.A. and Moulton, D.P., 2004. A new quantum ripple-carry addition circuit. arXiv preprint quant-ph/0410184.

Quantum Computation with Flying Electron Spin Qubits in Surface Acoustic Wave Systems

David Arvidsson-Shukur[1 2 *] Jacek Mosakowski[1 2] Mrittunjoy Guha-Majumdar[1 2]
Ward Haddadin[1] Crispin Barnes [1]

[1] *Cavendish Laboratory, Department of Physics, University of Cambridge, Cambridge CB3 0HE, United Kingdom*
[2] *Hitachi Cambridge Laboratory, J. J. Thomson Avenue, CB3 0HE, Cambridge, United Kingdom*

Abstract. We outline methodology for a universal set of quantum gates for surface acoustic wave (SAW) quantum computations. We use analytical methods to postulate a Hamiltonian which would implement the gates. Numerical parameter sweeps of the time-dependent Schrödinger equation finds the optimal parameters of the Hamiltonian. The two-qubit gates that we find are sqrt(SWAP) gates, either of the form of inter-channel operations or intra-channel operations. The inter-channel operations are needed for the circuit quantum computer models developed in prior SAW works. The intra-channel operations can be used for a novel type of SAW cluster state quantum computations.

1 Extended Abstract

Since the initial breakthroughs and the discovery of the potential power of a quantum computer, almost three decades have been allocated towards exploring problems that might be more efficiently solved on such a machine. [1, 2, 5, 4, 15] Whilst numerous mathematical applications have been found for quantum computers, the experimental successes in carrying out quantum computations have been limited. The difficulty in acquiring long decoherence times, short operational times, fast optimal readout and scalability has driven the field of experimental quantum computation around the entire spectrum of the subject of physics. [6, 7, 1, 8, 2, 9] In terms of quantum hardware, the quantum computation has to be tailored to the specific qubit used in the manipulations. For example, whilst the spatial quantum evolution of massless particles is essentially non-dispersive, but interactions between particles are weak; the spatial evolution of massive particles is dispersive, but interactions can be strong.

In this work we develop and investigate one of the suggested experimental protocols for realising quantum computations: quantum computations with surface acoustic wave (SAW) qubits. The ideas of a SAW quantum computational protocol is based on electron spin qubits that are carried forward by a surface acoustic wave on the surface of a semiconductor heterojunction. [7, 10] The acoustic wave begins on a 2D electron gas that is incident on 1D quantum wires. In these quantum wires the surface acoustic wave captures and carries single electrons, which become confined to the minima of the SAW. By placing a number of 1D wires parallel on the 2D surface and capturing one electron spin qubit in each wire, it is possible to realise quantum computations. We suggest magnetic gating for the implementation of single qubit rotations and non-magnetic screening gates for inter-channel sqrt(SWAP) two-qubit operations. The SAW based quantum computation model gains significant benefits over other massive qubit models in that it straightforwardly obtains the transport of the qubits, which in other technologies can be problematic. Furthermore, the SAW based systems allow the magnetic and electric gates to be stationary and static on the surface of the heterostructure device.

Presently, neither experimental data nor numerical simulations have been published for the operations needed in electron spin SAW quantum computing. Motivated by the prospect of experimentally implementing these flying qubit quantum computations, we have carried out a thorough numerical investigation of SAW flying electron spin qubit quantum gates. These simulations have allowed us to specify the physical parameters needed in order to implement the suggested two-qubit gates in real physical systems.

Before we present our findings when it comes to the implementation of the SAW two-qubit gates, we spend a few lines on describing the numerical methods used in this protocol.

In order to obtain the results of this paper, the time-dependent Schrödinger equation (TDSE) was solved based on the methods of [12]. We extended the original Staggered Leapfrog method presented in [13] to also include the spin component of the potential of the Hamiltonian and incorporate the spin-dependence in the potential. In terms of the quantum evolution in 1D quantum wires, we effectively remove two dimensions by integrating over them such that the problem reduces to a simulation of one dimension per particle but with altered Hamiltonian parameters. A more detailed overview of the numerical methods for a single particle simulation can be found in our previous work in Ref. [14].

Whilst the matrix algebra of the quantum evolution — in principle — is straightforward, the dimensionality of a two particle quantum system and the need of a large number of lattice points for a realistic simulation, leads to enormous constraints on the speed of the simulation. However, we have found that owing to the rotational nature of spin qubit quantum evolution, the use of GPU cards can significantly increase the speed of such

*drma2@cam.ac.uk

computations. By parallelising the Staggered Leapfrog method on GPUs using OpenCL, it has been possible to reduce the computational time by two orders of magnitude, which is crucial for realising parameter scans in realistic computational times. We also deem the numerical GPU adapted methods of this work to be highly valuable for simulations of any similar system and we strongly advocate the use of GPU boosted code in tailoring few-particle quantum Hamiltonians on classical computers.

Inter-Channel Gates: The simulations of the proposed inter-channel sqrt(SWAP) operations were successfully implemented. We simulated Hamiltonians created by carefully tuned screening gates on the top of the heterostructure. The electric gates are such that they can bring two separated harmonic potential minima to a mutual minimum and then separate them again. Crucially, the massive wavepacket dispersion is eliminated due to the Gaussian wavepacket nature of the qubits in these potentials. These simulations are crucial in order to get a hint of what the real experimental parameters will have to be.

One way of realising quantum computations in these systems is by allowing a circuit model to be implemented on the set of input qubits that are initialised in the array of 1D quantum wires of the system. However, owing to the 2D nature of the device structure qubits can only directly interact with qubits in neighbouring wires. The limit of the two-qubit interactions to nearest neighbour inter-channel gates significantly limits the speed of the quantum computation. Hence, we suggest the alternative implementation of SAW quantum computing; namely flying qubit cluster state one-way quantum computing. In order to efficiently create cluster states for fault tolerant quantum computing, the SAW system will have to include multiple qubits travelling on successive minima of the SAW in the same wire. This creates a 2D array of qubits. Crucially, the system then requires means of intra-channel two-qubit gates.

Intra-Channel Gates: These gates are implemented on two-qubits trapped in successive minima travelling down the same 1D quantum wire. We find that by implementing a stripe Schottky gate, perpendicular to the direction of travel of the qubits, one can alter the Hamiltonian, such that the ground state is perturbed for a short period of time, allowing some tunnelling between the two quantum dot minima that contain the qubits. By carefully tuning the parameters of the confining potential and the stripe gate, it is possible to utilise the spin-dependent difference in the interaction potential of the electron qubits in order to implement a sqrt(SWAP) operation. We calculate the time-dependent Hamiltonian analytically based on a semi-classical model and numerically obtain its form by using density functional theory to self-consistently solve the Poisson equation. In terms of realising the intra-channel sqrt(SWAP) operation, the two potentials are equivalent.

The intra-channel and inter-channel two-qubit gates can then be used to create a cluster state of the $M-1$ first channels in the semiconductor heterostructure junction. The M^{th} channel is used as the input channel. This channel would remain latent during the first half of the SAW computation (the half during which the cluster state is created) but become live and manipulated in the second half (the half during which the one-way computation takes place).

Experimentally attainable SAWs have typical speeds of around 3000 ms^{-1} and coherence times of about 100 ns. Hence, with gate sizes of about a micron, several hundreds of qubit operations can be carried out within the lifetime of the qubits.

Conclusively, this work presents a toolkit for the implementation of SAW quantum computing with flying electron spin qubits. We show how two types of two-qubit gates can be implemented. The realisations of these gates are simulated by solving the time-evolution of the Schrödinger equation for a Hamiltonian with credible stripe Schottky gate and screening gate potentials found either analytically or by density functional theory. We also suggest how the combination of these two particle gates together with single particle gates can be used in order to realise one-way cluster state computations using the SAW systems.

References

[1] R. P. Feynman. Simulating physics with computers International Journal of Theoretical Physics. 21, 467 (1982).

[2] D. P. DiVincenzo. Quantum Computation Science. 270, 255 (1995).

[3] R. Horodecki. Quantum entanglement Rev. Mod. Phys. 81, 865 (2009).

[4] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of the 28th ACM STOC*, pages 212–219, 1996.

[5] R. Horodecki. Quantum entanglement Rev. Mod. Phys. 81, 865 (2009).

[6] J. I. Cirac. A scalable quantum computer with ions in an array of microtraps Nature 404, 579 (2000).

[7] C. H. W. Barnes. A scalable quantum computer with ions in an array of microtraps Phys. Rev. B 62, 8410 (2000).

[8] E. Knill. A scheme for efficient quantum computation with linear optics Nature 409, 46 (2001).

[9] D. Loss. Quantum computation with quantum dots Phys. Rev. A 57, 120 (1998).

[10] G. Giavaras. Quantum entanglement generation with surface acoustic waves Phys. Rev. B 74, 195341 (2006).

[11] J. J. V. Maestri. Two-particle Schrodinger equation animations of wave packetwave packet scattering American Journal of Physics 68, 1113 (2000).

[12] J. J. V. Maestri. Two-particle Schrodinger equation animations of wave packetwave packet scattering American Journal of Physics 68, 1113 (2000).

[13] A. Askar. Explicit integration method for the timedependent Schrodinger equation for collision problems The Journal of Chemical Physics 68 (1978).

[14] D. R. M. Arvidsson-Shukur. A local non-iterative method for the implementation of Procrustean entanglement distillation ArXiv (2016).

[15] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Comp.*, 26(5):1484–1509, 1997.

Quantum input-output algorithms for quantum systems with limited controllability

Ryosuke Sakai[1] * Akihito Soeda[1] † Mio Murao[1] ‡

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, Japan*

Abstract. We present two algorithms that apply an arbitrary quantum operation on a qubit, which may be continuously evolving according to its own Hamiltonian. The qubit couples to a quantum computer through a fixed interaction Hamiltonian, which can only be switched on and off. The algorithms achieve an input and output operation, i.e., transfer of the qubit state between the qubit and quantum computer. All the steps of the algorithms are described by a closed formula of the input parameters of the algorithm and the interacting unitary between the qubit and quantum computer.

Keywords: quantum control, quantum algorithm, input-output approach

1 Introduction

Quantum algorithms assume that quantum systems can be controlled, or more precisely, that the necessary operations can be applied on the systems at will, but such high controllability is scarce in actual quantum systems. In contrast, a quantum computer is a quantum system, on which arbitrary quantum operations are possible. One of the main goals of quantum control theory [1–4] is to identify the means to increase the controllability of a quantum system by coupling it to a quantum computer. Typically, the poorly controllable systems are assumed to evolve continuously according to its self-Hamiltonian.

Occasionally referred to as local control [5–12], certain parts of a physical system are assumed to be highly controllable or the system can be coupled with a quantum computer. Protocols such as [10–12] show that we can transfer the state of the physical system to the quantum computer (output) and return it to the physical systems (input), *in principle* by local control. Thus, physical systems become fully controllable by this input-output approach because of high controllability of quantum computers. The advantage of this approach is independence on the desired operation to be implemented on the physical system. Hence, once we find methods to realize the input-output operations under limited controllability, we can perform any quantum operations for the physical system.

In this paper, we study means to control a physical system by the input-output approach, for a system coupled with a part of a quantum computer by a single fixed interaction Hamiltonian, for which we can arrange the duration of the coupling. It is generally difficult to construct exact input-output operations on our restrictions as pointed out in [10,11]. Thus, we will present two algorithms for a given coupling which implement *approximate* input-output operations. The first algorithm is similar to a procedure introduced by [10, 11] and requires a larger quantum memory for the quantum computer to perform approximate input-output operations with higher accuracy. The second algorithm requires only a fixed amount of quantum memory with respect to the required accuracy. Finally, we will evaluate the upper bound of the accuracy of the implemented operations of our algorithms in the diamond norm.

2 Setting

We consider a qubit S, which evolves according to a fixed time-independent self-Hamiltonian H_S. We assume that the quantum computer in contrast to S is able to perform arbitrary quantum operations (CPTP maps and quantum instruments).

We model the coupling between S and the quantum computer by two subsystems, a register system R and an interface system I of the quantum computer. R is the main processing part of the quantum computer consisting of N qubits. The interface system I is one qubit system, which directly couples to S by a single *fixed* interaction Hamiltonian $H_{\rm int}$. We assume that we are only allowed to choose between on and off of $H_{\rm int}$, and that I behaves as a part of the quantum computer, i.e., any unitary operations can be performed on IR when $H_{\rm int}$ is off. The set of unitary operators $\mathbb{LU}^N_{H_S,H_{\rm int}}$ describes all the possible operations on the total system.

3 Algorithms

Our two algorithms implement an approximate output operation $T^{\rm out}_M(\xi)$, which satisfies for any state $|\psi_S\rangle_S = a_S|0\rangle_S + b_S|1\rangle_S$ on S

$$\begin{aligned} &T^{\rm out}_M(\xi)\,|\psi_S\rangle_S\,|0\rangle_I\,|0\rangle_R^{\otimes M} \\ &= |0\rangle_S \otimes \left(a_S|0\rangle_I + b_S\sqrt{1-\xi^2}\,|1\rangle_I\right) \otimes |0\rangle_R^{\otimes M} \\ &\qquad + b_S\xi\,|1\rangle_S\,|g_{\rm out}\rangle \end{aligned} \tag{1}$$

with a certain fixed basis on SIR, $|g_{\rm out}\rangle$ is a state on IR, and M is the number of qubits on R. We see that $T^{\rm out}_M(0)$ is the exact output operation when the initial state of IR is $|0\rangle_I\,|0\rangle_R^{\otimes M}$. Our algorithms consist of the unitary operator $U_{\rm int}$ on SI which is generated by $H_{\rm int}$ and H_S such as $U_{\rm int} := e^{-iH_{\rm on}\tau}$ for some fixed duration time τ, where we defined $H_{\rm on} := H_S \otimes I_S + H_{\rm int}$. Then, the algorithms have the following properties:

*sakai@eve.phys.s.u-tokyo.ac.jp
†soeda@phys.s.u-tokyo.ac.jp
‡murao@phys.s.u-tokyo.ac.jp

- Algorithm 1 [10, 11]: Alg. 1 requires sufficiently large N-qubit register system for the approximate output operation, i.e., ξ of Eq. (1) is exponentially close to zero with N.

- Algorithm 2: Alg. 2 requires only one qubit register system for the approximate output operation. The quantum circuit representation of Alg. 2 is in Fig. 1.

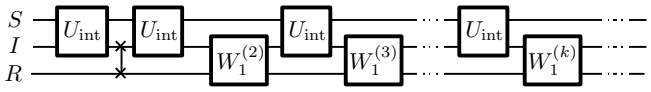


Figure 1: A quantum circuit representation of the Alg. 2. The first three steps are the same as Alg. 1. Then $W_1^{(k)}$ and $U_{\rm int}$ are iterated, where $W_1^{(k)}$ $(k = 1, 2, \dots)$ are unitary operators on IR and depend on $U_{\rm int}$. Thus, the total operations are in $\mathbb{LU}^N_{H_S,H_{\rm int}}$. By Alg. 2, ξ of Eq. (1) is exponentially close to zero with increasing the number of iterations of $W_1^{(k)}$ and $U_{\rm int}$.

By performing the inverse of our algorithms $(T^{\rm out}_M(\xi))^\dagger$ for $U^\dagger_{\rm int}$ instead of $U_{\rm int}$, we can construct the approximate input operation in $\mathbb{LU}^N_{H_S,H_{\rm int}}$. (One can check that when the initial state of S is $|0\rangle_S$, $(T^{\rm out}_M(0))^\dagger$ is the exact input operation by applying $(T^{\rm out}_M(\xi))^\dagger$ on Eq. (1).) Therefore, we obtain the concrete procedures of the realizations of approximate input-output operations in $\mathbb{LU}^N_{H_S,H_{\rm int}}$.

Note that our algorithms do not succeed for all $U_{\rm int}$, and we obtain the set of unitary operators on SI which make the algorithms work. We will refer these unitary operators as *exploitable unitary* operators.

4 Accuracy of control by approximate input-output operations

We divide operations on the total system SIR into three steps. First, we implement the output operation $T^{\rm out}_M(\xi_{\rm out})$ to transfer the state on S to I. At the second step, we perform a desired operation on I, say $\mathcal{M}$, which is always possible by definition. Finally, we perform the input operation $T^{\rm in}_M(\xi_{\rm in}) := (T^{\rm out}_M(\xi_{\rm in}))^\dagger$ to transfer back the state in I to S. We define map $\Phi^{\xi_{\rm out},\xi_{\rm in}}_{\mathcal{M}}$ formed by the above procedure, then we show the following lemma to compare with $\mathcal{M}$. The diamond norm is denoted by $\| \bullet \|_\diamond$.

Lemma 1 *For any CPTP map $\mathcal{M}$ on S, and $0 \le \xi_{\rm out}, \xi_{\rm in} \le 1$, $\|\Phi^{\xi_{\rm out},\xi_{\rm in}}_{\mathcal{M}} - \mathcal{M}\|_\diamond \le 2\sqrt{1-\Xi^2}$ if $\Xi \ge 0$, otherwise if $\Xi < 0$, then $\|\Phi^{\xi_{\rm out},\xi_{\rm in}}_{\mathcal{M}} - \mathcal{M}\|_\diamond \le 2$, where $\Xi := -1 + \sqrt{1-\xi^2_{\rm out}} + \sqrt{1-\xi^2_{\rm in}} - \xi_{\rm out}\xi_{\rm in}$.*

The lemma shows that when $\xi_{\rm out}, \xi_{\rm in}$ are close to 0, $\Xi^2 \approx 1 - (\xi_{\rm out} + \xi_{\rm in})^2$, hence $\|\Phi^{\xi_{\rm out},\xi_{\rm in}}_{\mathcal{M}} - \mathcal{M}\|_\diamond \le 2(\xi_{\rm out} + \xi_{\rm in}) \approx 0$. Therefore, Lem. 1 implies that $T^{\rm out}_M(\xi_{\rm out})$ and $T^{\rm in}_M(\xi_{\rm in})$ behave as input and output operations, respectively, even when $\xi_{\rm in}, \xi_{\rm out}$ are not strictly 0.

5 Conclusion

We have considered controlling a physical system by coupling to a quantum computer, and the coupling is described by time-independent Hamiltonian $H_{\rm int}$. In these situations, we presented two algorithms for approximate input-output operations under given unitary operator $U_{\rm int}$ on SI, where $U_{\rm int}$ needs to be an exploitable unitary. Although we have assumed that $U_{\rm int}$ is generated by time-evolution, we can prepare a unitary operator on SI such as $U^{(n)}_{\rm eff} = e^{-iH_{\rm on}t_n}(\prod_{j=1}^{n-1}(I_S \otimes u^{(j)}_I)e^{-iH_{\rm on}t_j})$ for any positive integer n, unitary operators $u^{(j)}_I$ on I, positive real numbers t_j. Then our algorithms apply with $U^{(n)}_{\rm eff} \in \mathbb{LU}^N_{H_S,H_{\rm int}}$ instead of $U_{\rm int}$. In fact, this technique is sometimes useful to construct an exploitable unitary operator. For example, we suppose that $H_{\rm int} := \alpha X_S \otimes X_I$ and $H_S := gZ_S$, where X, Z are Pauli X and Z operators, respectively, and $\alpha, g \in \mathbb{R}$, then we can show that $e^{-iH_{\rm on}\tau}$ is not exploitable unitary for any τ, but becomes $U^{(2)}_{\rm eff}$ by the technique.

Acknowledgment

This work is supported by ALPS, the Project for Developing Innovation Systems of MEXT, Japan, and JSPS KAKENHI (Grant No.26330006, No.15H01677 and No.16H01050). We also acknowledge the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas MEXT KAKENHI (Grant No.24106009)).

References

[1] S. Lloyd, *Phys. Rev. A* **62**, 022108 (2000).

[2] D. D'Alessandro, *Introduction to Quantum Control and Dynamics*. Taylor and Francis, Boca Raton, 2008.

[3] D. Dong *et al.*, *IET Control Theory Appl.* **4**, 2651 (2010).

[4] C. Altafini *et al.*, *IEEE Transactions on Automatic Control* **57**(8), 1898 (2012).

[5] M. Owari *et al.*, *Phys. Rev. A* **91**, 012343 (2015).

[6] S. Lloyd *et al.*, *Phys. Rev. A* **69**, 012305 (2004).

[7] D. Burgarth *et al.*, *Phys. Rev. A* **79**, 060305(R) (2009).

[8] R. Heule *et al.*, *Phys. Rev. A* **82**, 052333 (2010).

[9] R. Heule *et al.*, *Eur. Phys. J. D* **63**, 41 (2011).

[10] D. Burgarth *et al.*, *Phys. Rev. Lett.* **99**, 100501 (2007).

[11] D. Burgarth *et al.*, *arXiv*:0710.0302 (2008).

[12] D. Burgarth *et al.*, *Phys. Rev. A* **81**, 040303(R) (2010).

Quantum Media Conversion Between SAW Driven Flying Electron-Spin Qubits and Flying Photon-Polarization Qubits.

H. V. Lepage[1] * C. H. W. Barnes[1]

[1] *Cavendish Laboratory, Department of Physics, University of Cambridge, Cambridge, CB3 0HE, UK*

Abstract. Different physical implementations of qubits offer advantages in different tasks required by a quantum computer. In hybrid quantum systems, the need arises for an interface between different types of qubtis. This research investigates quantum media conversion between electron-spin qubits and photon-polarization qubits through accurate GPU accelerated simulations.

Keywords: QMC, SAW, Single Photon Source, Quantum Computer, Qubit

1 Introduction

Quantum computing and quantum cryptography are the two main areas of interest for the applications of quantum information systems. Currently, there exist no perfect physical qubit implementation which could be used efficiently for all operations involved in quantum-information technologies.[1] Different types of qubits can be used at each step of the quantum computation or quantum communication to optimise the success of each task. For example, electron-spin qubits in a semiconductor material offer straightforward initialization and manipulation of the qubit state since the interactions between particles and an external magnetic field are strong. Strong particle-particle interactions also favour stable and scalable computation as they allow straightforward implementation of two qubit logic gates.[2] Conversely, photon-polarization qubits are advantageous for readout operations and for fast long-distance communication.[3, 4] Qubit coherence over long distances makes photons absolutely necessary for quantum key distribution schemes.

2 Quantum Media Conversion

Due to the hybrid nature of these quantum systems, we investigated methods for interfacing different qubit types and an efficient implementation of quantum media conversion (QMC) between electron-spin qubits and photon-polarization qubits. Certain protocols only require QMC between definite states – mapping a spin-½ system onto a circular polarization state. In this case, the Hilbert space for each qubit has dimension 2 and the mapping of states can be expressed in terms of spin selection rules.[5] This has been the main focus of our research. For truly generalizable QMC hardware, the entire Bloch Sphere must be mapped onto the Poincare Sphere. For the transmission of quantum states over arbitrary distances, several interfaces could be laid out in series leading to a set of quantum repeaters.

A promising approach to the problem of single electron transport are travelling surface acoustic waves (SAWs). In piezoelectric materials such as gallium arsenide, an oscillating stress and strain wave is accompanied by an electric potential modulation of similar waveform. Carefully tuned travelling SAWs can be used to carry single electrons acting as qubits across a GaAs device.[6, 7]

In this research, a model is built in which an electron is taken from a 2D electron gas and carried by a SAW along a 1D channel, where its spin is initialized by an external magnetic field. It is then carried across a lateral p-n junction and is ultimately introduced to a 2D hole gas

*hl407@cam.ac.uk

where it recombines with a hole and produces a single photon. By engineering the band structure in the region of recombination to lift any degeneracies in the valence band, the hole gas becomes populated with $|m_J| = \frac{3}{2}$ holes only. Spin selection rules then dictate the photon circular polarization state from the electron spin state and provide insight on the relationship between the electron spin state and the angle at which the photon was emitted.

3 GPU Accelerated Simulations

We model SAW-driven electron transport across our device by solving the time dependent Schrodinger Equation whilst the effective potential of the n-p junction itself it obtained via the density functional theory (DFT) modelling method. The quest for meaningful and stable resutls leads to a very large number of operations to be carried out by a computer. A two dimensional simulation with N_x by N_y lattice points will require a vector of size $(N_x N_y)$, which then scales exponentially with the number of particles simulated.

For simple operations, when each calculation is independent of others, such calculations can be performed in parallel. Modern CPU architectures make use of parallel computing where multi-threaded processors can perform 4 to 32 tasks simultaneaously. However, graphics processing units (GPUs) have been optimised to operate at a very high level of parallelism. As of when this paper is being written, modern GPUs contain several thousands of processor cores and can operate on the order of ten billion floating-point operations per second (10 GFLOP/s). We found GPU accelerated computation to be especially useful when simulating electron transport in a 2D or 3D heterostructure.

4 Conclusions

SAW-driven single electron transport is simulated by solving the time dependent Schrodinger Equation. Band structure engineering and appropriate selection rules dictate how quantum information is converted from electron-spin qubits to photon-polarization qubits. Accurate simulations are obtained using fast algorithms and GPU acceleration.

For more information, please refer to `http://www.sp.phy.cam.ac.uk/research/surface-acoustic-waves-saws`

References

[1] H. Kosaka *et al.* Coherent transfer of light polarization to electron spins in a semiconductor. In *Physical review letters*, 100.9 (2008): 096602.

[2] F. H. L. Koppens, *et al.* Driven coherent oscillations of a single electron spin in a quantum dot. *Nature*. 442.7104 (2006): 766-771.

[3] C. H. Bennett, G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (1984): 175-179.

[4] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. In *Physical Review Letters* 68.21 (1992): 3121.

[5] V. Rutger, and E. Yablonovitch. A spin-coherent semiconductor photo-detector for quantum communication. In *Physica E: Low-dimensional Systems and Nanostructures* 10.4 (2001): 569-575.

[6] J. M. Shilton, *et al.* High-frequency single-electron transport in a quasi-one-dimensional GaAs channel induced by surface acoustic waves. In *Journal of Physics: Condensed Matter* 8.38 (1996): L531.

[7] C. H. W. Barnes, *et al.* Quantum computation using electrons trapped by surface acoustic waves. In *Physical Review B* 62.12 (2000): 8410.

Quantum Multiclass Support Vector Machine with Quantum One Against All Approach for Big Data Classification

Arit Kumar Bishwas[1] * Ashish Mani[2] † Vasile Palade[3] ‡

[1] *Department of Information Technology, Amity University Uttar Pradesh, Noida, India*
[2] *Department of EEE, Amity University Uttar Pradesh, Noida, India*
[3] *Faculty of Engineering and Computing, Coventry University, Coventry, UK*

Abstract. In this paper, it has been shown that multiclass support vector machine for big data classification can be implemented in logarithm time complexity on a quantum computer. Quantum version of one-against-all approach has been developed to address the quantum SVM multiclass problem statement. With quantum one-against-all approach, there will be k quantum binary support vector machine (SVM) classifiers. The strategy involves training a single quantum binary classifier per class, with the samples of that class as positive samples and all other samples as negatives. Once all the k quantum binary classifiers get trained, all quantum classifiers are applied to an unseen quantum query state to predict the class for which the corresponding classifier reports the highest confidence score. The quantum multiclass SVM with proposed approach exhibits an exponential speed up over its classical counterpart.

Keywords: Quantum Algorithm, Multiclass Classification, SVM

1 Introduction

Support vector machine (SVM) is a very popular binary classifier, however,in recent years the need for multiclass support vector machine has been growing with increase in big data applications. Multiclass SVM classifies vectors into multiple sets with the help of trained oracles[1]. Many approaches have been proposed for constructing multiclass support vector machine with the help of binary SVM and one of the most popular one is one-against-all[2]. Recently,Rebentrost,Mohseni and Lloyd[3],proposed an elegant quantum version of binary support vector machine for big data which works in logarithm time for both training and classification stages, so it has an exponential time complexity improvement overits classical counter part.However, the algorithm in [3] does not support multiclass classification. In our proposed work, we have investigated and developed the multiclass quantum SVM algorithmfor big data with one-against-all approach. For the purpose we adopted the technique mentioned in [3] to construct the binary quantum SVM as a base and then lead our investigation for multiclass quantum SVM. We have used quantum version of one-against-all approach. The run time complexity of our proposed multiclass quantum SVM with quantum one-against-all approach has been analyzed. It was found that the algorithm works exponentially faster than the classical version.

2 Multiclass quantum SVM Classification for big data with Quantum One-Against-All Approach

With quantum one-against-all approach, there is one quantum binary support vector machine for each class to separate members of that class from rest of the class members, this results inkquantum binary classifiers. At first, we have formulated k quantum binary least square SVM classifiers.Then we apply all the quantum binary classifiers to an unseen quantum query state to predict the class for which the corresponding classifier reports the highest confidence score.The mentioned quantum version of one-against-all approach uses Grover's search algorithm [4]and finds the highest confidence score with quadratic speed up $O(\sqrt{k})$ in comparison to the classical version of one-against-all approach, which is O (k). The total runtime of the proposed quantum multiclass SVM has been analyzed as

$$O(k(logMN)) + O(\sqrt{k}) \tag{1}$$

where M is the training vectors associated with k quantum binary classifiers and N is the dimension of feature space.

While estimating the total run time of the algorithm, the following error analysis has been carried out. We begin the analysis for single classifier, later we scale to k classifiers. The kernel matrix preparation causes O (log M N) costs. The number of time steps in phase estimation T requires $O(t_0^2\epsilon^{-1})$.

Where (t_0^2) is the total evolution time which is determining the phase estimation error and ϵ is the maximally error. Combining, we get the run time $O(t_0^2\epsilon^{-1}O(logMN))$. Lets define a constant ϵ_{Kr} such that $\epsilon_{Kr} \leq |\lambda_l| \leq 1$, also lets define an effective condition number $\kappa_{eff} = \epsilon_{Kr}^{-1}$. Where λ_l are eigen values and κ_{eff} is used to employ the filtering procedure in phase estimation, referring [5]. By considering the error analysis, and iterating the algorithm for $O(\kappa_{eff})$ times for achieving a constant success probability of the post selection step, the total run time is $O(\kappa_{eff}^3\epsilon^{-3}(logMN))$ including the error factor of $O(\kappa_{eff}^3\epsilon^{-3})$. Which can be scaled as O (log M N). Nowtherefore, for k classifiers with quantum one-against-all approach it will be considered $O(k(logMN)) + O(\sqrt{k})$.

*aritkumar.official@gmail.com
†amaini@amity.edu
‡vasile.palade@coventry.ac.uk

3 Conclusion

It has been shown that the multiclass support vector machine can be quantum mechanically implemented in logarithm time complexity as compared to the classical counterpart multiclass support vector machine for big data classification, which runs in polynomial time complexity, thus resulting in an exponential speed up. We have analyzed and addressed the quantum multiclass SVM problem with quantum mechanically implemented one-against-all approach, which shows quadratic speed gain as compared to the classical one-against-all approach. In quantum one-against-all approach, we first construct k quantum binary classifiers. Then we construct a quantum query state, which is to be classified. Next, is to classify the quantum query state with all the k quantum binary classifiers. The class, for which the corresponding quantum binary classifier's probability confidence score is highest, will be considered as predicted class.

References

[1] J.A.K. Suykens and J. Vandewalle, Multiclass least squares support vector machines. In *Proc. of International Joint Conference on Neural Networks, 1999.(Volume:2), 900-903 (1999)*

[2] Chih-Wei Hsu, Chih-Jen Lin A comparison of methods for multiclass support vector machines IEEE Transactions on Neural Networks (Volume:13 , Issue: 2), 415-425 (2002)

[3] P. Rebentrost, M. Mohseni and S. Lloyd The capacity of quantum channel with general signal states. arXiv:1307.0471v3

[4] Grover. Lov K A fast quantum mechanical algorithm for database search and discrete logarithms on a quantum computer. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (1996).

[5] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett.103, 150502 (2009).

Reducing Loops for Topological Cluster State Quantum Computation

Kentaro Haneda[1] * Shigeru Yamashita[1] † Simon Devitt[2] ‡ Kae Nemoto[3] §

[1] *Graduate School of Science and Engineering, Ritsumeikan University*
[2] *Center for Emergent Matter Sciences, Riken*
[3] *National Institute of Informatics*

1 Introduction

The TQC (Topological Quantum Computing) model has been receiving a lot of attention because it has proven to be one of the most promising fault-tolerant quantum computation models. In the TQC model, we arrange qubits in a two-dimensional space, and we encode logical qubits by using a surface code for error correction. By adding the time axis, we consider the three-dimensional space to represent calculation steps for the TQC model. In a three-dimensional space, a region of physical qubits measured in a specific basis is called a *defect*. We prepare a pair of *defects* to encode one logical qubit. Then, in a TQC model, we can perform a desired calculation by *moving* defects in the space [1]. This computation model is called topological cluster state computation (TCSC), and computation steps can be represented by defect patterns in the three-dimensional space.

In TCSC, if the two defect patterns are *topologically* equivalent, the represented two quantum computations by the defect patterns are proven to be the same. We can optimize the space for TCSC by using this property. There have been found various transformations which do not keep the topological equivalence, but still keep computational equivalence [3].

Theoretically, we can optimize the necessary space (or, volume) size for TCSC by applying transformation rules. However, it is not fully automated to find a good order of applying the rules up to today, and it is desirable to have an automated software to do so [2].

The functionality of TCSC does not change when we change the shape of each defect in anyway if we keep the topology, e.g., we can bent and/or stretch it in anyway without changing the functionality. Thus, if we consider the exact shape of defects, we may need to consider infinite possibilities of transformations. Thus, in this paper, we propose an efficient way to represent a computation for TCSC; we consider a loop for each defect, and we maintain only the relationship between loops to represent a computation. We formulate the known transformations as changing the relationship of loops by using simple set operations. Accordingly, we can have an automated optimization method based on our formulation.

*hub@ngc.is.ritsumei.ac.jp
†ger@cs.ritsumei.ac.jp
‡simon.devitt@riken.jp
§nemoto@nii.ac.jp

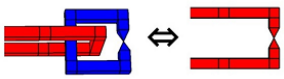


Figure 1: Rule 3.

Figure 2: Rule 4.

In the following, we explain our formulation and our optimization method with some preliminary experimental results.

2 Space Optimization for the TCSC

2.1 Transformation Rules

Here, we denote some useful transformation rules which can be used to reduce the space for TCSC. In our formulation, each defect pattern is represented by a (open or closed) loop. Each *braid* between two defect patterns is represented by a crossing between the corresponding two loops.

Rule 1. In TCSC, topologically equivalent defect patterns perform the same computation. Therefore we can bent and/or stretch the shape of any loop.

Rule 2. If there are two braids between two defects, they cancel each other. Thus, we can remove even number of crossings between two loops.

Rule 3. If one loop, l_i, crosses only one loop, l_j, we can remove l_i. If l_i has injection points and/or input/outputs, they move to l_j. This rule is called teleporting. An example is shown in Fig. 1.

Rule 4. If one loop, l_i, which does not have either any injection point nor any input/output, crosses three loops, we can remove l_i. Also we can remove one of the three loops if it does not have either any injection point nor any input/output. This rule can be described as in Fig. 2.

Rule 5. This is similar to Rule 4. If one loop, l_i, that does not have either any injection point nor any input/output crosses two loops, we can remove l_i. Also

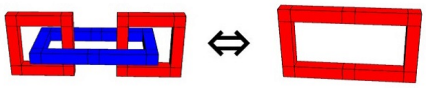
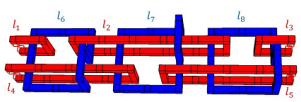
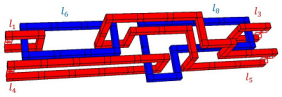


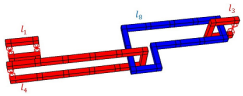
Figure 3: Rule 5



(a) SWAP Circuit



(b) Removing l_7 and l_2 by Rule 4.



(c) Removing l_5 and l_6 by Rule 5.

(d) Removing l_8 and l_3 by Rule 5.

Figure 4: Optimizing SWAP circuit by our method.

we can remove one of the two loops if it does not have either any injection point nor any input/output. This rule can be described as in Fig. 3.

2.2 Optimization Method

As we mentioned before, topologically equivalent defect patterns perform the equivalent computation. Therefore, there are infinite equivalent defect patterns. Accordingly, our method represents TCSC as a set of loops; we can treat topological equivalent defect patterns as the same set of loops.

We do not need to consider Rule 1 because we consider the whole circuit as a set of loops, and thus we do not need to care the geometry information of each defect, such as size and position.

Our method is stated as follows:

- We find a loop, l_i, that does not have either any injection point nor any input/output.
  - If l_i crosses only one loop, we apply Rule 3 to delete l_i.
  - If l_i crosses only two loop, we apply Rule 5 to delete loops.
  - If l_i crosses only three loop, we apply Rule 4 to delete loops.

We show an example in the following.

Fig. 4 (a) shows the defect patterns of TCSC for realizing SWAP operation. First, we remove l_7 and l_2 by Rule 4 to get Fig. 4 (b). Then, we remove l_6 and l_5 by Rule 5 to get Fig. 4 (c). Finally, we use Rule 5 again to remove l_8 and l_3; Our optimized circuit is represented by Fig. 4 (d). The circuit indeed swaps the inputs.

3 Preliminary Experimental Results and Conclusion

We implemented the proposed method and performed a preliminary experiment as follows. We first randomly generated 10,000 circuits for each specific case (i.e., the number of qubits, gates, and external inputs/outputs, and injectors). Then, we derived defect patterns from the circuits, and reduced the number of loops by our method. Table 1 shows the numbers of loops of the initial circuit in the fifth column from the left, and the average (over 10,000 circuits) number of loops after our optimization method in the sixth column. The specification of circuits (i.e., the number of qubits, gates, and external inputs/outputs, and injectors) of our randomly generate circuits are given in the first to the fourth columns, in this order. The last column show the average reduction ratios.

Table 1: Comparison between before and after our optimization.

Quantum circuits				♯ loops		
qubits	gates	ex	in	Before	After	(%)
10	10	1	0	30	1.00	96.7
10	10	1	10	30	8.84	70.5
10	10	10	0	30	6.38	78.7
10	10	5	5	30	4.55	84.8
10	10	10	10	30	17.82	40.6
100	100	1	0	300	1.00	99.7
100	100	1	100	300	92.94	69.0
100	100	100	0	300	51.84	82.7
100	100	50	50	300	36.49	87.8
100	100	100	100	300	221.45	26.2

From the experimental results, we can observe that the number of loops after our optimization method would be related to the number of primary inputs/outputs and injectors. In our experiment, we confirmed that the order of applying our rules does not affect the final results. In our future work, we would like to study this feature (i.e., the order of applying the rules) further. Also, our future work would be to seek how to reduce the volume of TCSC after reducing the number of loops by our method.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 24106009 and 15H01677.

References

[1] Austin G Fowler and Kovid Goyal. Topological cluster state quantum computing. *arXiv*, 2008.

[2] Ilia Polian and Austin G Fowler. Design automation challenges for scalable quantum architectures. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, pages 1–6. IEEE, 2015.

[3] Robert Raussendorf, Jim Harrington, and Kovid Goyal. Topological fault-tolerance in cluster state quantum computation. *New Journal of Physics*, 9(6):199, 2007.

Reduction of computation complexity of classical optimal decoding by adiabatic quantum computation

Yuta NISHINO[1] * Souichi TAKAHIRA[1] Akihito KADOYA[1] Asuka OHASHI[2] †
Tsuyoshi Sasaki USUDA[1] ‡

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute-shi, Aichi, 480-1198, Japan*
[2] *College of Science and Engineering, Ritsumeikan University, 1-1-1 Noji-Higashi, Kusatsu-shi, Shiga, 525-8577, Japan*

Abstract. Adiabatic quantum computation (AQC)[1, 2] was proposed by Farhi *et al.* to quickly solve combinational optimization problems. However, there are only a few applications of AQC and we aim to find more applications. In this study, we demonstrate the implementation of a method of classical optimal decoding in digital communication using AQC. In particular, we consider classical optimal decoding of single parity check codes. Moreover, we reduce the computational complexity and demonstrate the simulation results.

Keywords: quantum algorithm, adiabatic quantum computation, classical optimal decoding

1 Introduction

Adiabatic quantum computation (AQC) using quantum annealing theory[3] was proposed by Farhi *et al.* in 2002[1]. It was pointed out that AQC can solve combinational optimization problems faster than classical computation. However, only a few problems are quickly solved by AQC.

In this study, we consider implementing classical optimal decoding of binary linear codes in digital communication by AQC. The computational complexity of classical optimal decoding increases exponentially as the codeword length increases. An efficient calculation algorithm for classical optimal decoding was presented[4]; however, the algorithm could efficiently decode only some codes. In the research of quantum ciphers called Keyed Communication in Quantum noise (KCQ)[5], classical optimal decoding was used to evaluate the performance of KCQ protocols using binary linear codes[6]; however, owing to the high computational complexity of classical optimal decoding, the performance of KCQ protocols could not be evaluated. To solve these problems, we first demonstrate how to implement classical optimal decoding by AQC. In particular, we consider classical optimal decoding of single parity check (SPC) codes that are used in KCQ research[6]. Second, we reduce the computational complexity by devising a step function and demonstrate the numerical results.

2 Adiabatic quantum computation (AQC)

In this section, we introduce AQC based on the references[1, 2]. AQC uses quantum annealing theory[3] and solves combinational optimization problems. In AQC, the Hamiltonian is

$$H(t) = \big(1 - q(t)\big)H_0 + q(t)H_1, \tag{1}$$

where H_0 is an initial Hamiltonian whose ground state is trivial, H_1 is a final Hamiltonian whose ground state corresponds to the solution, and $q(t)$ is monotone increasing function that satisfies $q(0) = 0$ and $q(1) = 1$. We control the Hamiltonian $H(t)$ by varying the function $q(t) = 0$ to $q(t) = 1$. AQC works by maintaining the quantum state close to the instantaneous ground state of Eq.(1). Finally, we obtain the solution by finding the ground state of H_1; however, if there is a level crossing, quantum systems cannot keep the quantum state close to the ground state.

3 Classical optimal decoding of binary linear codes

In this study, we use binary phase shift keying (BPSK) signals coded by binary linear codes, and we assume that channel noise is an additive white Gaussian noise (AWGN). AWGN is the most common model used in the evaluation of KCQ protocols. To implement classical optimal decoding, we have to find the codeword that has the maximum conditional probability as follows:

$$P(\boldsymbol{y}|\boldsymbol{w}_i) = \prod_{j=1}^{n} \frac{1}{2\pi\sigma^2} \mathrm{e}^{-|y_j - w_{i,j}|^2/2\sigma^2}, \tag{2}$$

where $\boldsymbol{y}(y_1, y_2, \ldots, y_n), y_j \in \mathbb{C}$ is the output, n is the codeword length, $w_{i,j} \in \{-A, A\}$ is the amplitude of the BPSK signal, and σ^2 is the variance of noise.

4 Classical optimal decoding by AQC

To implement classical optimal decoding by AQC, we have to construct the Hamiltonian of Eq.(1) in accordance with the problem. First, the H_0 is constructed as follows:

$$H_0 = I_{2^n} - |\psi(0)\rangle\langle\psi(0)|\,, \tag{3}$$

where

$$|\psi(0)\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=1}^{2^k} |\boldsymbol{w}_i\rangle\,, \quad |\boldsymbol{w}_i\rangle = \bigotimes_{j=1}^{n} |w_{i,j}\rangle\,, \tag{4}$$

$|w_{i,j} = A\rangle = (1, 0)^{\mathrm{T}}$, $|w_{i,j} = -A\rangle = (0, 1)^{\mathrm{T}}$, and I_M is the $M \times M$ identity matrix. Second, the H_1 is constructed

*im161008@cis.aichi-pu.ac.jp
†a-ohashi@fc.ritsumei.ac.jp
‡usuda@ist.aichi-pu.ac.jp

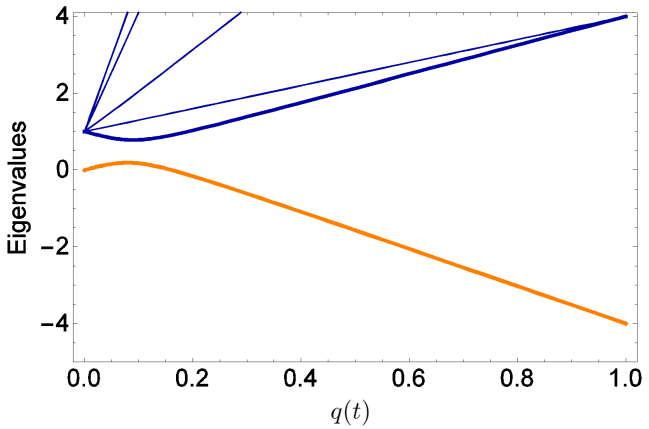


Figure 1: Behavior of the eigenvalues of Hamiltonian when the codeword length $n = 4$.

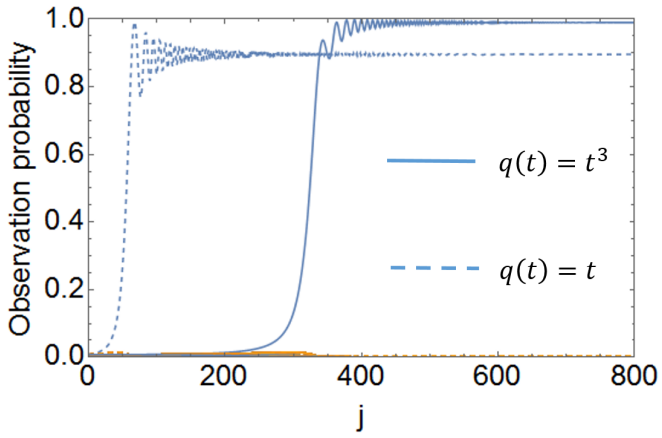


Figure 2: Observation probability when the number of steps $J = 800$.

so that its eigenvalues express the cost function of the problem. The cost function is Eq.(2) in classical optimal decoding. On finding the codeword $\boldsymbol{w}_i$ that maximizes Eq.(2), we can transform Eq.(2) as follows:

$$P'(\boldsymbol{y}|\boldsymbol{w}_i) = \sum_{j=1}^{n}(-2\mathrm{Re}[y_j]w_{i,j} + w_{i,j}^2). \quad (5)$$

The final Hamiltonian H_1 is constructed based on Eq.(5) and the property of SPC codes that states that no codewords can have an odd number of 1.

$$H_1 = \sum_{j=1}^{n}\lambda_j - c(n)\bigotimes_{j=1}^{n}\left(\sigma_{i,j}^z - I_2\right), \quad (6)$$

where $c(n)$ is a penalty function that is determined for the problem, $\sigma_{i,j}^z$ is the Pauli matrix, and λ_j is

$$\lambda_j = I_2 \otimes I_2 \otimes \cdots \otimes \underbrace{(-2Ay_j\sigma_{i,j}^z + A^2\sigma_{i,j}^{z2})}_{j\text{th}} \otimes \cdots \otimes I_2. \quad (7)$$

5 Simulation

We examined the behavior of the eigenvalues of the $H(t)$ and simulated the behavior of observation probabilities.

5.1 Problem setting

In simulating AQC, for simplicity we set the amplitude $A = 1$, the output $\boldsymbol{y} = (1, 1, \ldots, 1)$ and the variance of noise $\sigma^2 = 1/2$. We set the penalty function $c(n) = nA^n$ to increase as the codeword length increased and the amplitude grew. We prepared the step parameter $t = j/J, (0 \leq j \leq J)$ for simulation, where J is the number of steps and corresponds to the computational complexity. In this study, we compare the step functions $q(t) = t$ and $q(t) = t^3$.

5.2 Behavior of the eigenvalues of the $H(t)$

Fig.1 shows that the behavior of the eigenvalues of Hamiltonian when the codeword length $n = 4$. As observed from the lower two lines, these do not cross between $q(t) = 0$ and $q(t) = 1$ and therefore, we can appropriately implement classical optimal decoding.

5.3 Simulation results

Fig.2 is the simulation result for AQC with each step function $q(t)$ when the number of steps $J = 800$ and $n = 8$. Each of the blue lines represents a solution state. When $J = 800$, we can obtain the $|11111111\rangle$ state with an observation probability of 99.02% with the step function $q(t) = t^3$. On the other hand in AQC with the step function $q(t) = t$, we obtain the state with an observation probability of 89.58%. To achieve an observation probability of 99% with the step function $q(t) = t$, we need to implement AQC with $J \approx 1700$. From these results, it can be observed that we can obtain a solution with higher probability and reduce the computational complexity for classical optimal decoding by using our proposed step function $q(t) = t^3$.

6 Conclusion

We considered implementing classical optimal decoding of SPC codes by AQC. First, we demonstrated that classical optimal decoding is apparently implemented by using Hamiltonian proposed in this study. Second, we can obtain the solution state vector with higher probability and lower number of steps than the conventional step function $q(t) = t$ by using the cubic step function. In the future, we aim to consider the implementation of classical optimal decoding with other codes by AQC.

Acknowledgment: This work has been supported in part by KAKENHI (Grant Nos. 24360151, 16H04367).

References

[1] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, quant-ph/0001106, (2000).

[2] E. Farhi, *et al.*, Science, **292**, pp.472-474, (2001).

[3] T. Kadowaki and H. Nishimori, Phys. Rev., **E58**, pp.5355-5363, (1998).

[4] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, (2003).

[5] H.P. Yuen, quant-ph/0311061v6, (2004).

[6] A. Kadoya, Y. Umemura, S. Asano, N. Iwata, and T.S. Usuda, Proc. of AQIS2015, pp.161-162, (2015).

Reduction of Quantum Cost by Changing the Functionality

Nurul Ain Binti Adnan[1] * Kouhei Kushida[1] † Shigeru Yamashita[1] ‡

[1] *Ritsumeikan University, Graduate School of Information Science and Engineering, 1-1-1 Noji Higashi, Kusatsu, Shiga 525-8577, Japan TEL: 077-561-4947 FAX: 077-561-4947*

1 Introduction

In order to demonstrate the ability of quantum computing in the near future, an efficient quantum algorithm should be implemented. Since most of known quantum algorithms include Boolean components, an efficient design technique for realization of a Boolean function is very crucial even for quantum circuits.

There are many ways to design a reversible circuit to realize a Boolean function; one of most popular ways is to generate an initial circuit consisting of Mixed Polarity Multiple-Control Toffoli (MPMCT) gates [1], [2] based on a small Exclusive-or Sum-Of-Products (ESOP) expression [3] and then decompose a large gate (i.e., with the large number of inputs) into elementary gates. Once an initial circuit is obtained, further post-optimization techniques such as library-based, transformation-based and template-based optimization method can be applied [5].

This paper describes a technique to reduce the quantum cost by changing the functionality of a Boolean function, represented as ESOP. This technique is of particular interest since it is one of few in the literature (i.e., [4]), that presents a way in which ESOP expressions can be manipulated to reduce the quantum cost of the corresponding circuit. The idea presented in [4] cannot be simply applied to large practical functions. Thus, in this paper, we propose a heuristic technique to utilize the idea. Our proposed method find a small ESOP expressions for the given function. Then, it will find a good pair of product terms in the ESOP expression so that we can reduce the quantum cost by applying the idea of [4] to the two terms.

We expect that our approach may produce a better quantum cost reduction than existing method, and indeed our experimentary results confirm this expectation.

2 Preliminaries

2.1 Quantum cost

For evaluating the performance of the quantum circuit synthesis, the most basic thing to do is to calculate the quantum cost. The quantum cost of a reversible circuit is the number of premitive quantum gates needed to implement the circuit. Primitive quantum gates are elementary gates that are consist of two bits or less, such as CNOT gates, NOT gates and control-V gates. Each elementary gates are considered to have a unit cost.

2.2 Realizing Boolean function with MPMCT Gates

A **minterm** of a Boolean function is the combination of all the input variables (negative or positive) when the Boolean function becomes one. In the following, an $MPMCT_n$ gate means an MPMCT gate that has n control bits.

*nu_ain@ngc.is.ritsumi.ac.jp
†is0112vk@ed.ritsumei.ac.jp
‡ger@cs.ritsumei.ac.jp

Table 1: A Truth Table for a 4-input Boolean Function with 4 Minterms

x_1	x_2	x_3	x_4	$f(x)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

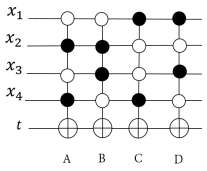


Figure 1: The quantum circuit for Table 1

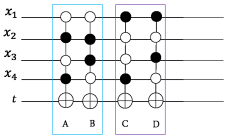


Figure 2: Grouping of gates

To realize an n-input Boolean function with k minterms by a reversible circuit, one possible way is to put k $MPMCT_n$ gates such that (1) each $MPMCT_n$ gate corresponds to each minterm of the function, and (2) the polarity of each control bit for an MPMCT gate corresponds to each variable's polarity in the corresponding minterm. In other words, if x_i or $\overline{x_i}$ appears in a minterm, the corresponding control bit is positive or negative, respectively. In this construction, the target bit of all the $MPMCT_n$ gates is the same as the qubit where we want to realize the function.

For instance, Table 1 shows a 4-input Boolean function with 4 minterms, and the circuit in Fig. 1 realizes the function: $x_2 \cdot x_4 \cdot \overline{x_1} \cdot \overline{x_3} \oplus x_2 \cdot x_3 \cdot \overline{x_1} \cdot \overline{x_4} \oplus x_1 \cdot x_4 \cdot \overline{x_2} \cdot \overline{x_3} \oplus x_1 \cdot x_3 \cdot \overline{x_2} \cdot \overline{x_4}$. For example, the left most gate in Fig. 1 corresponds to $x_2 \cdot x_4 \cdot \overline{x_1} \cdot \overline{x_3}$; the control bits for x_2 and x_4 are in the positive polarities denoted by black circles, and x_1 and x_3 are in the negative polarities denoted by white circles.

3 Better ESOP-based Implementation

3.1 Previous work

It has been shown in [4] that we can modify a given specification in order to obtain a better ESOP-based implementation, and then modifies the result to get back to the originally desired specification/function. This justified us a way/approach in which ESOP expressions can be manipulated to reduce the quantum cost of the corresponding circuit. However, the method in [4] cannot deal with a large function. Motivated by this, this paper proposes an iterative heuristic approach to reduce the quantum cost of a large function.

3.2 Proposed Method

The idea behind our method that we first generate a smaller versions of ESOP to the whole functions. We group the product terms in the obtained ESOP by two,

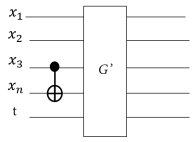


Figure 3: The insertion of a CNOT gate

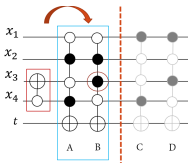


Figure 4: The insertion of a CNOT gate (Group 1)

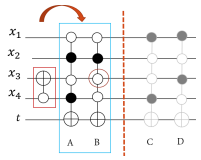


Figure 5: After the insertion of a CNOT gate (Group 1)

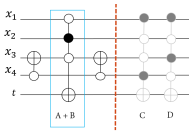


Figure 6: Final circuit (Group 1)

and then apply the concept to each group of two product terms. This involves adding MPMCT gates to the initial quantum circuit as shown in Fig. 3

Let us take the example of circuit shown in Fig. 1 and group the gates into two groups as shown in Fig. 2. For the first group (two gates from the left, gate A and B), if we insert an MPMCT gate whose negative control bit is x_4 and the target bit is x_3 (i.e., a CNOT gate) before G' as shown in Fig. 4, the inserted CNOT gate (the control bit is x_4 and the target bit x_3) inverts the value of x_3 when $x_4 = 0$. See Fig. 5. This means that the gate changes the input state $(0110) = \overline{x_1}, x_2, x_3, \overline{x_4}$ to $\overline{x_1}, x_2, \overline{x_3}, \overline{x_4}$. Thus the two MPMCT gates (A and B) can be merged into one new MPMCT gate as shown in Fig. 6.

Similarly, for the second group (two gates from right, gate C and D), if we insert an MPMCT gate whose positive control bit is x_4 and the target bit is x_3 (i.e., CNOT gate) before G', the inserted CNOT gate (the control bit is x_4 and the target bit x_3) inverts the value of x_3 when $x_4 = 1$. See Fig. 7. and Fig. 8. Thus the gate changes the input state $(1001) = x_1, \overline{x_2}, \overline{x_3}, x_4$ to $x_1, \overline{x_2}, x_3, x_4$. Therefore the two MPMCT gates (C and D) can be merged into one new MPMCT gate as shown in Fig. 9.

Further, we would like to note that after applying the CNOT gate in Fig. 3, the resulting states of the qubits after the circuit are not exactly the same as the ones of the desired circuit because we changed the functionality of x_3 by inserting the MPMCT gate. Therefore, we insert the same MPMCT gate after G' at the end of the circuit as shown in Fig. 10.

Finally gates A, B, C and D in the circuit as shown in Fig. 1 can be merged into two gates as shown in Fig. 10. After applying the same MPMCT gate at the end of circuit in Fig. 10, the functionality of the resulting circuit is exactly the same as the original circuit in Fig. 1. The original quantum cost for Fig. 1 is 112 but now is reduced to 30.

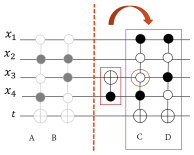


Figure 7: The insertion of a CNOT gate (Group 2)

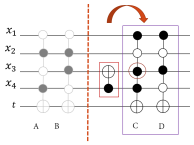


Figure 8: After the insertion of a CNOT gate (Group 2)

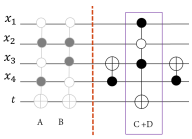


Figure 9: Final circuit (Group 2)

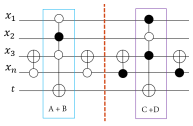


Figure 10: Optimized Circuit

Table 2: Experimental Results

Function	Original Cost	This Work (Proposed)
z4ml	573	513
9symml	3,429	1,563
alu2	13,011	10,248
alu4	496,980	38,3312
cordic	27,580,332	20,283,129

4 Experimental Results and Conclusions

To evaluate an ESOP-based synthesis method, we use the program called as ABC. We can minimize ESOP forms by ABC, and so we used the program as a base method; we calculate the original quantum cost based on the minimized ESOP forms by ABC. We applied our algorithm to various benchmark circuits and compared our results with the original cost. The outcome of the comparison (see Table 2) clearly shows that the proposed method can reduce quantum cost.

From the results, we can observe that our proposed method not only has the ability to produce a smaller ESOP expression for the modified specification but also can reach the result with much lower quantum cost. Obviously our future work is to improve the resulting quantum cost of other circuits.

5 Acknowledgement

This work was supported by JSPS KAKENHI Grant Number 24106009 and 15H01677.

References

[1] Mona Arabzadeh, Mehdi Saeedi, and Morteza Saheb Zamani. Rule-based optimization of reversible circuits. In Design Automation Conference (ASP-DAC), 2010 15th Asia and South Pacific, pp. 849-854. IEEE 2010.

[2] Kamalika Datta, Gaurav Rathi, Indranil Sengupta, and Hafizur Rahaman. An improved reversible circuit synthesis approach using clustering of esop cubes. J.Emerg. Technol. Comput. Syst., Vol. 11, No. 2, Article No. 15, November 2014.

[3] K Fazel, M Thornton, and JE Rice. Esop-based Toffoli gate cascade generation. In IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 206-209, citeseer, 2007.

[4] Nurul Ain Binti Adnan, Kouhei Kushida, and Shigeru Yamashita. A pre-Optimization Technique to Generate Initial Reversible Circuits to Reduce the Low Quantum Cost. In IEEE International Symposium on Circuits and Systems, May 2016.

[5] Mehdi Saeedi and a Igor L. Markov. Synthesis and Optimization of Reversible Circuits&Mdash;a Survey ACM Comput. Surv., Vol. 45, No. 2, Article 21, March 2013

Regularized Boltzmann entropy determines possibility of macroscopic adiabatic transformation

Hiroyasu Tajima[1] * Eyuri Wakakuwa[2] †

[1] *Center for Emergent Matter Science (CEMS), RIKEN, Wako, Saitama 351-0198 Japan*
[2] *Graduate School of Information Systems, The University of Electro-Communications, Chofu, Japan*

Abstract. Whether the Boltzman entropy is equal to the thermodynamic entropy has been one of the central issue since the beginning of statistical mechanics. Today, it is believed that the thermodynamic entropy S_{TD} is equal to a function $\tilde{S}_{TD}$ that is defined by regularizing the Boltzman entropy in order to ensure extensivity. However, it is not known whether $\tilde{S}_{TD}$ completely determines the possibility of the macroscopic adiabatic transformation in the same way as S_{TD} does. In this paper, by formulating possibility of the macroscopic adiabatic transformations in terms of "coarse-graining" of quantum operations, we prove that $\tilde{S}_{TD}$ provides a necessary and sufficient condition for possibility of a macroscopic adiabatic transformation.

Keywords: Quantum thermodynamics, Second law, macroscopic state transition

1 Introduction

How the thermodynamic entropy S_{TD} is related to the Boltzmann entropy S_B has been one of the central issue since the beginning of statistical mechanics. Today, it is believed that the thermodynamic entropy is equal to the following regularzied Boltzmann entropy $\tilde{S}_{TD}$, which is defined in terms of the Boltzmann entropy S_B and is extensive by definition [1];

$$\tilde{S}_{TD}[U,V,N] := \lim_{X\to\infty} \frac{S_B[UX,VX,NX]}{X}, \qquad (1)$$

where U, V and N, denoting the internal energy, the volume and the number of particles, respectively. However, it is not known whether $\tilde{S}_{TD}$ completely determines possibility and impossibility of a macroscopic adiabatic transformation in the same way as S_{TD}. As stated by the second law of thermodynamics, the thermodynamic entropy S_{TD} satisfies the following statement [2];

$$(U,V,N) \prec_{aq} (U',V',N) \Leftrightarrow S_{TD}[U,V,N] \leq S_{TD}[U',V',N']. \qquad (2)$$

where $(U,V,N) \prec_{aq} (U',V',N)$ means "an adiabatic transformation from (U,V,N) to (U',V',N) is possible".

In statistical mechanics field, many researches [3–5] have demonstrated the "only if" part of (2) for $\tilde{S}_{TD}[U,V,N]$ by adopting certain formulations of "adiabatic operations", while leaving the "if" part unproven. On the other hand, recent approaches from quantum information theory [6–15] have succeeded in deriving detailed thermodynamic relations, which characterize possibility and impossibility of quantum state transformations by a set of restricted operations. In their approaches, however, conditions for possibility of state transformations are represented by not only the macroscopic parameters, but also the microscopic parameters such as the fluctuation in microcanonical state. This is in contrast to (2), which is represented only by macroscopic parameters.

In this paper, we propose a coarse-graining approach to try the "if" part in (2), and show that $\tilde{S}_{TD}$ provides a necessary and sufficient condition for possibility of a macroscopic adiabatic transformation, i.e., a macroscopic state transformation by adiabatic operations. First, we pdefine the possibility of macroscopic adiabatic transformations, based on a "coarse-graining" of possibility of quantum state transformations by unital operations. Second, we prove that the magnitude relation of $\tilde{S}_{TD}$ provides a necessary and sufficient condition for possibility of a macroscopic adiabatic transformation.

2 Preliminaries

In this section, we clarify basic concepts of thermodynamics and statistical mechanics. See e.g. [1, 2] for details.

In thermodynamics, an equilibrium state is represented by values of a set of macroscopic physical quantities such as (U,V,N). In this abstract, we consider cases where all these physical quantities are extensive, and where the quantities include the internal energy, i.e., we represent the equilibrium state as $\vec{a} := (U, a_1, ..., a_L)$.

As the second law of thermodynamics, the thermodynamic entropy S_{TD} completely determines possibility and impossibility of a macroscopic adiabatic transformation; $\vec{a} \prec_{aq} \vec{a}' \Leftrightarrow S_{TD}[\vec{a}] \leq S_{TD}[\vec{a}']$, where $\vec{a} \prec_{aq} \vec{a}'$ to represent the statement that "an adiabatic transformation from $\vec{a}$ to $\vec{a}$ is possible".

Let us introduce the statistical mechanical counterpart for the thermodynamic equilibrium $\vec{a}$. Since we are concerning a macroscopic limit, we describe a physical system by a Hilbert space $\mathcal{H}^{(X)}$ depending on a scaling parameter X. The macroscopic limit is defined as the limit of $X \to \infty$. We assume that X takes values in a set $\mathcal{X} = \mathbb{N}$ or $\mathcal{X} = \mathbb{R}^+$. For each $X \in \mathcal{X}$ and $l = 0, \cdots, L$, we denote the set of the Hermite operators on $\mathcal{H}^{(X)}$ as $\vec{A}^{(X)} := (H^{(X)}, A^{(X),[1]}, ..., A^{(X),[L]})$. Then, the micro-

*hiroyasu.tajima@riken.jp
†e.wakakuwa@gmail.com

canonical state corresponding to an equilibrium state $\vec{a}$ is defined by $\hat{\pi}^{(X)}_{\vec{a},\delta_X} := \hat{\Pi}^{(X)}_{\vec{a},\delta_X}/D^{(X)}_{\vec{a},\delta_X}$, where $\hat{\Pi}^{(X)}_{\vec{a},\delta_X}$ and $D^{(X)}_{\vec{a},\delta_X}$ are the projection and the dimension of the following $\mathcal{H}^{(X)}_{\vec{a},\delta_X}$, which is a subspace of of $\mathcal{H}^{(X)}$;

$$\mathcal{H}^{(X)}_{\vec{a},\delta_X} := \mathrm{span}\left\{|\psi\rangle \in \mathcal{H}^{(X)} \;\middle|\; \exists \lambda^{[l]} \in [X(a^{[l]}-\delta_X), X(a^{[l]}+\delta_X)) \text{ s.t. } A^{(X)[l]}|\psi\rangle = \lambda^{[l]}|\psi\rangle \text{ for } 0 \le l \le L\right\}. \tag{3}$$

The parameter δ_X is a positive function of X, which represents the negligible fluctuation of macroscopic quantities. Since we are normalizing macroscopic observables as (5), it is natural to assume that $\lim_{X\to\infty}\delta_X = 0$.

Next, we introduce the regularized Boltzmann entropy. When the limit $\tilde{S}_{TD}$ exists, we call it the regularized Boltzmann entropy;

$$\tilde{S}_{TD}[\vec{a}] := \lim_{X\to\infty}\frac{1}{X}\log D^{(X)\downarrow}_{\vec{a}} \tag{4}$$

Here, $D^{(X)\downarrow}_{\vec{a}}$ is the dimension of the following $\mathcal{H}^{(X)\downarrow}_{\vec{a}}$;

$$\mathcal{H}^{(X)}_{\vec{a}} := \mathrm{span}\left\{|\psi\rangle \in \mathcal{H}^{(X)} \;\middle|\; \exists \lambda^{[l]} \le X a^{[l]}, \text{ s.t. } A^{(X)[l]}|\psi\rangle = \lambda^{[l]}|\psi\rangle \text{ for } 0 \le l \le L\right\}, \tag{5}$$

With concrete calculations, it has been shown that there exists the limit $\tilde{S}_{TD}$ in many physical systems, e.g., gases of particles with natural potentials including the van der Waars potential [1].

3 Formulation of Possibility of Macroscopic Adiabatic Transformations

We propose a definition of the possibility of a macroscopic state transformation, by "coarse-graining" the possibility of the quantum state transformation which can be considered as a quantum mechanical counterpart of the adiabatic transformation. We employ the unital CPTP map $\mathcal{E}(\hat{1}) = \hat{1}$ as the quantum state transformation, because a unital map does not decrease the von Neumann entropy of an arbitrary quantum state [16], i.e., $S(\mathcal{E}(\rho)) \ge S(\rho)$ for all $\rho \in \mathcal{S}(\mathcal{H})$. Because this feature is similar to the adiabatic transformation in thermodynamics, many researches have treat the unital operation as a quantum counterpart of the adiabatic transformation in thermodynamics [5, 12, 13].

Now, we give of the possibility of a macroscopic adiabatic transformation. The basic idea is as follows;

Basic Idea 1 *Suppose a microcanonical state $\pi^{(X)}_{\vec{a},\delta_X}$ is transformed by a quantum operation $\mathcal{E}_X$ to another microcanonical state $\pi^{(X)}_{\vec{a}',\delta'_X}$. From a macroscopic point of view, we observe that an equilibrium state $\vec{a}$ is transformed to another equilibrium state $\vec{a}'$, for any δ_X and δ'_X within the range of "macroscopically negligible fluctuations". Therefore, we could say that an equilibrium state $\vec{a}$ can be transformed to another equilibrium state $\vec{a}'$ if, for any macroscopically negligible δ_X and a δ'_X, a state $\pi^{(X)}_{\vec{a},\delta_X}$ can be transformed to $\pi^{(X)}_{\vec{a}',\delta'_X}$.*

We translate the above idea into a strict definition;

Definition 1 *We define $\vec{a} \prec_{\tilde{a}q} \vec{a}'$ as follows; For any $\{\delta_X\}_{X\in\mathcal{X}} \in \Delta$, there exists $\{\delta'_X\}_{X\in\mathcal{X}} \in \Delta$ and a set $\{\mathcal{E}_X\}_{X\in\mathcal{X}}$ such that*

$$\lim_{n\to\infty}\left\|\mathcal{E}_X(\hat{\pi}^{(X)}_{\vec{a},\delta_X}) - \hat{\pi}^{(X)}_{\vec{a}',\vec{\delta}'_X}\right\| = 0, \tag{6}$$

and $\mathcal{E}_X$ is a unital CPTP map on $\mathcal{S}(\mathcal{H}^X)$ for all $X \in \mathcal{X}$. Here, $\|\rho-\sigma\|$ is the trace distance.

4 Main Results

Theorem 2 *When the regularized Boltzmann entropy $\tilde{S}_{TD}$ exists, the following holds for arbitrary $\vec{a}$ and $\vec{a}'$:*

$$\tilde{S}_{TD}[\vec{a}] \le \tilde{S}_{TD}[\vec{a}'] \Leftrightarrow \vec{a} \prec_{\tilde{a}q} \vec{a}'. \tag{7}$$

Theorem 2 states that $\tilde{S}_{TD}$ provides a necessary and sufficient condition for possibility of a macroscopic adiabatic transformation in the same way as S_{TD} does.

Our results shows that the regularized Boltzmann entropy $\tilde{S}_{TD}$ gives a total ordered structure of macroscopic adiabatic transforamtion, just as thermodynamic entropy S_{TD}. We emphasize that our results do not depend on any microscopic parameters, including δ_X that we have introduced to define the generalized microcanonical state $\hat{\pi}_{\vec{a},\delta_X}$. This is in contrast to Ref. [14], and other previous approaches from quantum information theory [6–13, 15], in which convertibility of states are characterized by functions that depends on microscopic parameters.

[1] H. Tasaki, *Statistical mechanics 1,2*, ISBN-13: 978-4563024376 and ISBN-13: 978-4563024383 (Baihukan, 2008 (in Japanese)).

[2] E. H. Lieb and J. Yngvason Phys. Rep. **310**, 1, (1996).

[3] C. Jarzynski, Phys. Rev. Lett. **78**, 2690, (1997).

[4] J. Kurchan, arXiv:cond-mat/0007360(2000).

[5] H. Tasaki, arXiv:1511.01999 (2015).

[6] M. Horodecki and J. Oppenheim, Nat. Commun. **4**, 2059 (2013).

[7] O. C. O. Dahlsten, R. Renner, E. Rieper, and V. Vedral, New. J. Phys.**13**, 053015, (2011).

[8] J. Aberg, Nat. Commun. **4**, 1925 (2013).

[9] D. Egloff, O. C. O. Dahlsten, R. Renner and V. Vedral, arXiv:1207.0434, (2012).

[10] F. G. S. L. Brandao, M. Horodeck, N. H. Y. Ng, J. Oppenheim, and S. Wehner, PNAS, 112,3215(2015).

[11] S. Popescu, arXiv:1009.2536.(2010).

[12] P. Skrzypczyk, A. J. Short and S. Popescu, Nature Communications **5**, 4185, (2014).

[13] H. Tajima and M. Hayashi arXiv:1405.6457 (2014).

[14] M. Weilenmann, L. Krämer, P. Faist, and R. Renner, arXiv:1501.06920(2015).

[15] G. Gour, M. P. Muller, V. Narasimhachar, R. W. Spekkens, N. Y. Halpern, arXiv:1309.6586 (2013).

[16] H. P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, USA, 2007).

[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

States evolution of a quantum-feedback-enhanced single photon source

C. Y. Chang[1 3 *] D. S. Citrin[2 3 †] L. Lanco[4] P. Senellart[4]

[1] *School of Physics, Georgia Institute of Technology, Atlanta, Georgia 30332-0250 USA*
[2] *School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia 30332-2050 USA*
[3] *UMI 2958 Georgia Tech-CNRS, Georgia Tech Lorraine, 2 Rue Marconi F-57070, Metz, France*
[4] *Laboratoire de Photonique et Nanostructures, LPN/CNRS, Route de Nozay, 91460 Marcoussis, France*

Abstract. We present a theory of quantum optical feedback from a single-photon quantum-dot (QD) emitter embedded in a microcavity in the strong-coupling limit [1] with optical feedback from a distant mirror (external cavity) [2].

Keywords: Single photon emitter, Quantum coherence feedback

1 Introduction

The basic phenomenon for quantum information processing network relies on preserving the coherence exchange between atomic excitations and photonic state. Nowadays, the network technologies for optical quantum device relied on the pure interaction at the single particle level and it requires photon source that can reproduce highly indistinguishable single photons. Recently, the advances in designing semiconductor devices allows fabricating such devices that meet the requirement. A single quantum dot (QD) embedded in a microcavities create high-purity single photon with high brightness with the enhancement of the cavity. Additionally, by adding quantum feedback of this system can be driven to a target state via external control of the target state by a modification of the repumping strength. The single photon emitter has been shown to stabilize the exchange between the quantum states and improve qubit control based on the repeated action of a sensor-controller-actuator loop.

Here, We discuss a theory of quantum optical feedback from a single-photon quantum-dot (QD) emitter embedded in a microcavity in the strong-coupling limit [1] with optical feedback from a distant mirror (external cavity) [2]. Furthermore, we expand our study for single excitation state to two-excitation state within the external cavity system, we study the photon statistics of the device and compare it to a single photon emitter without feedback. Our proposed quantum feedback control scheme shows a potential route to improve the purity of the single photon source.

2 Model

The system consists of a microcavity with a QD coupled to a single-cavity mode (see Fig. 1). An external mirror is placed in front of the single photon emitter at distance, $L = \frac{c\tau}{2}$, to introduce coherent feedback into the microcavity. The Hamiltonian within the rotating-wave and dipole approximations is given in [3]:

$$\frac{\hat{H}}{\hbar} = -\gamma(\sigma^- a^\dagger + \sigma^\dagger a^-) - \int_0^\infty [G(k,t)a^\dagger d_k + G^*(k,t)d_k^\dagger a]\mathrm{d}k$$

*cychang@gatech.edu
†david.citrin@ece.gatech.edu

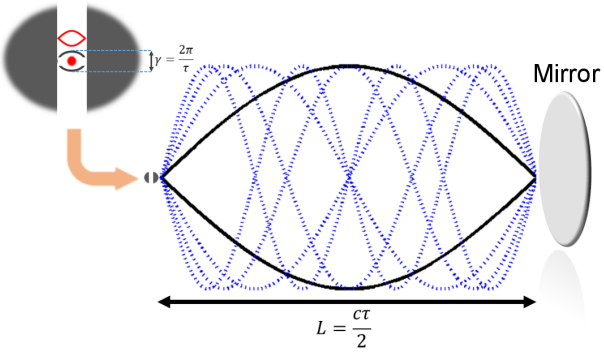


Figure 1: Experimental scheme.

Thus, the system can be describe with superposition of three orthogonal basis for single excitation:

$$|\Psi\rangle = c_e\,|e,0,0\rangle + c_g\,|g,1,0\rangle + \int c_{gk}\,|g,0,k\rangle\,\mathrm{d}k \quad (1)$$

Projecting the time-dependent Schrödinger equation ($i\hbar\frac{\partial}{\partial t}|\Psi\rangle = \hat{H}\,|\Psi\rangle$), the three rate equations for single excitation are written:

$$\frac{\partial c_e}{\partial t} = i\gamma c_g \quad (2)$$

$$\frac{\partial c_g}{\partial t} = i\gamma c_e + i\int c_{g,k}G(k,t)\mathrm{d}k \quad (3)$$

$$\frac{\partial c_{g,k}}{\partial t} = ic_g G^*(k,t) \quad (4)$$

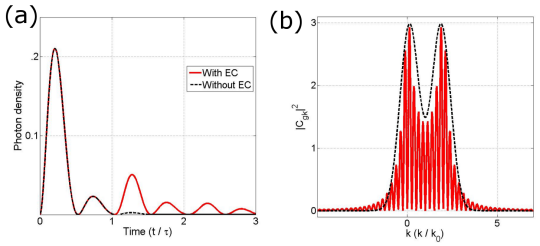


Figure 2: (a) The photon density inside the cavity $|c_g(t)|^2$ with feedback (red) and without quantum feedback (black).(b) The spectrum of the output photon $|c_{gk}(t)|^2$ with external feedback (red) and without quantum feedback (black).

Next, We study the two-excitation states in our system. A general time-dependent wavefunction for two-excitation state is thus represent by superposition of each state parameter:

$$|\Psi\rangle = c_{ec}\,|e,1,0\rangle + \int c_{ek}\,|e,0,k\rangle\,\mathrm{d}k + c_{cc}\,|g,2,0\rangle + \int c_{ck}\,|g,1,k\rangle\,\mathrm{d}k + \int\int c_{kk'}\,|g,0,\{k,k'\}\rangle\,\mathrm{d}k\mathrm{d}k'$$

Following the similar process for single excitation case, we obtain five equations of motion for the various amplitudes:

$$\frac{\partial c_{ec}}{\partial t} = i\gamma c_{cc} + i\int c_{ek}G(k,t)\mathrm{d}k \tag{5}$$

$$\frac{\partial c_{ek}}{\partial t} = i\gamma c_{ck} + ic_{ec}G^*(k,t) \tag{6}$$

$$\frac{\partial c_{cc}}{\partial t} = i\gamma c_{ec} + i\int c_{ck}G(k,t)\mathrm{d}k \tag{7}$$

$$\frac{\partial c_{ck}}{\partial t} = i\gamma c_{ek} + i\int c_{kk'}G(k',t)\mathrm{d}k' + ic_{cc}G^*(k,t) \tag{8}$$

$$\frac{\partial c_{kk'}}{\partial t} = ic_{ck'}G^*(k,t) \tag{9}$$

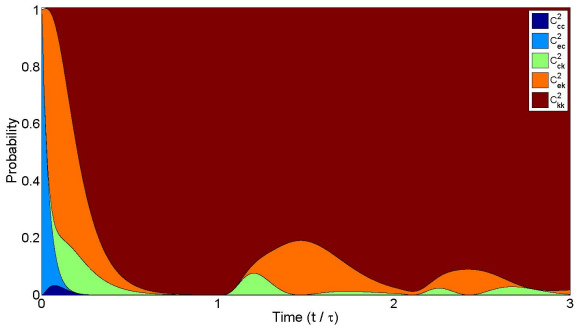


Figure 3: Time evolution of the probabilities of five states

3 Result and Conclusion

While Fig. 3 shows the dynamics of each state it is more interesting to study the photon statistics due to their coherent nature. Assuming that the probability of emission of photons is proportional to the square of the state coefficient and independent from the different mode in the external cavity(green and orange), we can see such setup may emit single photon between 0 and τ which are from only one photon in the external cavity, for a photon from these states, $g^{(2)}(t,0) = 0$ for a single photon source.

$$g^{(2)}(t,\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle\,\langle I(t+\tau)\rangle}.$$

The dynamic of the photon statistics can also be characterized by an experimental observable quantity, $g^{(2)}(t,\tau)$, the second-order coherence of the excitation light source in a typical HBT setup (inset of Fig. 4(a)). The correlation function at times detector 1 and 2 can be used to characterize the photon statistics,

The value of $g^{(2)}(t,0)$ can be used to categorize the quantum nature of the light: thermal if $g^{(2)}(t,0) = 2$, coherent if $g^{(2)}(t,0) = 1$, or squeezed if $g^{(2)}(t,0) = 0.2$. In the following, we consider g(2)(t,0) as is measured in the HBT experiment. We define $g^{(2)}_{\mu}(t,\tau)$ as that associated with photons in the microcavity $g^{(2)}_{EC}(t,\tau)$ as that associated with photons in the external cavity [3],

$$g^{(2)}_{\mu}(t,0) = \frac{\langle a^\dagger a^\dagger aa\rangle}{\langle a^\dagger a\rangle^2} = \frac{|c_{cc}(t)|^2}{\left||c_{ec}(t)|^2 + |c_{ec}(t)|^2 + |c_{ec}(t)|^2\right|},$$

$$g^{(2)}_{EC}(t,0) = \frac{\left\langle d_k^\dagger d_k^\dagger d_k d_k\right\rangle}{\left\langle d_k^\dagger d_k\right\rangle^2} = \frac{|c_{kk'}(t)|^2}{\left||c_{ek}(t)|^2 + |c_{ck}(t)|^2 + |c_{kk'}(t)|^2\right|}.$$

Here, we use our previous result in Fig. 3 to compute $g^{(2)}(t,\tau)$ shown in Fig.4(b) and compare with a continuous single photon source in Fig. 4(a).

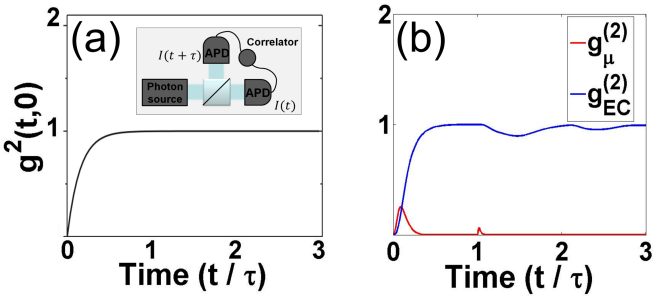


Figure 4: (a) The second order coherence function, $g^{(2)}(t,0)$, for continuous single photon source and (b) $g^{(2)}(t,0)$ for micro cavity photon (red) and an external cavity photon (blue).

In conclusion, we performed a cQED simulation of a single-photon emitter in a microcavity with time-delayed optical feedback. The model extends the exact analytical solutions of the single excitation case [2] to the two-excitation. Our results establish a future framework for the theoretical description of feedback control in the quantum limit of a quantum dot/micropillar coherent feedback system. Such a scheme shows enhanced oscillation. Our result also shows generating highly purity and indistinguishable single photons that are desirable for quantum network and large scale photonic quantum computers.

References

[1] S. M. Hein, F. Schulze, A. Carmele, and A. Knorr, "Optical feedback-enhanced photon entanglement from a biexciton cascade," *Phys. Rev. Lett.*, vol. 113, p. 027401, 2014.

[2] J. Kabuss, D. O. Krimer, S. Rotter, K. Stannigel, A. Knorr, and A. Carmele, "Analytical study of quantum feedback enhanced rabi oscillations," *Phys. Rev. A*, vol. 92, p. 053801, 2015.

[3] A. Carmele, "Theory for strongly coupled quantum dot cavity quantum electrodynamics," 2011.

Steering fraction and its application to the superactivation of Einstein-Podolsky-Rosen steering

Chung-Yun Hsieh[1] * Yeong-Cherng Liang[2] † Ray-Kuang Lee[1 3] ‡

[1] *Department of Physics, National Tsing Hua University, Hsinchu 300, Taiwan*
[2] *Department of Physics, National Cheng Kung University, Tainan 701, Taiwan*
[3] *Physics Division, National Center for Theoretical Science, Hsinchu 300, Taiwan*

Abstract. Einstein-Podolsky-Rosen (EPR) steering is a quantum phenomenon associated with the ability of spatially separated observers to *steer* — by means of local measurements — the assemblage, i.e., the set of conditional quantum states accessible by a distant party. Inspired by the studies of Bell-nonlocality, we introduce the concept of steering fraction, which quantifies the extent to which a given assemblage violates a steering inequality. We then use this to establish (1) a sufficient condition for the superactivation of steering and (2) an upper bound on the maximal quantum violation of steering inequality achievable by arbitrary finite-dimensional maximally entangled state.

Keywords: Einstein-Podolsky-Rosen steering, superactivation, quantum nonlocality

From the famous Einstein-Podolsky-Rosen (EPR) paradox [1] to Bell's seminal discovery [2], quantum theory has never failed to surprise us with its plethora of intriguing phenomena and mind-boggling applications [3, 4]. Among those who made the bizarre nature of quantum theory evident was Schrödinger, who not only coined the term "entanglement", but also pointed out that quantum theory allows for *steering* [5]: through the act of local measurements on one-half of an entangled state, a party can *remotely* steer the set of (conditional) quantum states accessible by the other party.

Taking a quantum information perspective, the demonstration of steering can be viewed as the verification of entanglement involving an untrusted party [6]. Imagine that two parties Alice and Bob share some quantum states and Alice's wants to convince Bob that the shared state is entangled, but Bob doesn't trust her. If Alice can convince Bob the shared state indeed exhibits EPR steering, then Bob would believe that they share entanglement, as the latter is a prerequisite for steering. Note, however, shared entanglement is generally insufficient to guarantee steerability. Interestingly, steerability is actually a necessary but generally insufficient condition for the demonstration of Bell-nonlocality. Hence, steering represents a form of quantum inseparability that is intermediate between entanglement and Bell-nonlocality.

Apart from entanglement verification in a partially-trusted scenario, steering has also found applications in the distribution of secret keys in partially trusted scenario [7]. From a resource perspective, the steerability of a quantum state ρ, i.e, the extent to which a quantum state can exhibit steering turns out to provide also an indication for the usefulness of ρ in other quantum information processing tasks. For instance, steerability as quantified by steering robustness [8] is monotonously related to the probability of success in the problem of subchannel discrimination when one is restricted to local measurements aided by one-way communications. The quantification of steerability is thus of relevance also in quantum information.

In this work, inspired by the *nonlocality fraction* introduced by Cavalcanti *et al.* [9], we introduce a quantifier for steerability dubbed *steering fraction*, which is particularly suited for the studies of steerability in relation to an arbitrary but *fixed* steering inequality [10, 11] or steering functional. To this end, consider an *assemblage* of (unnormalized) conditional quantum states

$$\sigma = \{\sigma_x^a\} = \{\mathrm{tr}_A(\rho(E_{a|x} \otimes \mathbb{I}))\} \tag{1}$$

and a steering functional $F = \{F_x^a\}$ [11], where $\mathbb{E} = \{E_{a|x}\}$ is the set of positive-operator-valued measure (POVM) elements implemented by Alice on the shared state ρ, $\mathbb{I}$ is the identity operating acting on Bob's Hilbert space, and tr_A is the partial trace over Alice's Hilbert space. We define the corresponding *steering fraction* as:

$$\Gamma_s(\sigma, F) = \frac{1}{B_C(F)} \sum_{x,a} \mathrm{tr}(F_x^a \sigma_x^a), \tag{2}$$

where $B_C(F) = \sup_{\sigma \in \mathcal{L}_s} \sum_{x,a} \mathrm{tr}(F_x^a \sigma_x^a)$ is the supremum of the steering functional F over the set $\mathcal{L}_s$ of all assemblages describable by *local hidden-state model* [6, 11]. In this form, the steerability of an assemblage σ (and hence of the underlying state ρ giving rise to this assemblage) for the given steering functional F is evident: the assemblage σ violates the steering inequality corresponding to F if and only if $\Gamma_s(\sigma, F) > 1$. From here, let us also define—for any given state ρ and and steering functional F—the largest steering violation corresponding to F as

$$LV_\rho(F) = \sup_{\mathbb{E}} \Gamma_s(\sigma(\rho, \mathbb{E}), F), \tag{3}$$

where $\sigma(\rho, \mathbb{E})$ is understood as the assemblage induced by the state ρ and the set of POVMs $\mathbb{E}$. Essentially, this is just the largest steering fraction attainable by ρ with respect to the steering inequality F. This can be computed by maximizing Eq. (2) over Alice's POVMs, and hence the corresponding assemblages via Eq. (1).

*andrew79106@yahoo.com.tw
†ycliang@mail.ncku.edu.tw
‡rklee@ee.nthu.edu.tw

As any quantum experiments necessarily involves repeated measurements over many copies of the quantum state ρ, a natural question that arises in this context is the steerability of ρ compared with multiple copies of ρ, i.e., $\rho^{\otimes k}$ with $k > 1$. In particular, an interesting question that one may ask is whether there exists ρ which is non-steerable (and hence does not violate any steering inequality), but which becomes steerable if we allow joint measurements on sufficiently many copies of the same state. Following the terminology introduced by Palazuelos [12] in the context of Bell-nonlocality, we say that a quantum state ρ can be *superactivated* if it has the aforementioned property, namely, that ρ is non-steerable (and hence describable by a local-hidden-state model), but $\rho^{\otimes k}$ is steerable for some $k > 1$. The superactivation of ρ for EPR-steering can be rephrased as:

$$LV_\rho(F) \leq 1 \quad \forall\, F, \tag{4a}$$

$$\Gamma_s(\sigma(\rho^{\otimes k}, \mathbb{E}), F') > 1 \quad \text{for some } k, \mathbb{E} \text{ and } F'. \tag{4b}$$

That superactivation is possible for Bell-nonlocality was first demonstrated by Palazuelos [12] using the isotropic state in $\mathbb{C}^8 \otimes \mathbb{C}^8$ in conjunction with the so-called *Khot-Vishnoi* (KV) game [13, 14] G_{KV}. Their result was soon generalized by Calvacanti *et al.* [9] to show that all entangled isotropic states that are Bell-local can be superactivated. Since there exist entangled isotropic states that are non-steerable, and as mentioned above, a quantum state that is Bell-nonlocal must also exhibit steering, we know that there must also be entangled isotropic states whose steerability can be superactivated. Indeed, our calculations show that for any state ρ acting on $\mathbb{C}^d \otimes \mathbb{C}^d$, one can find a collection of POVM $\tilde{\mathbb{E}}^{(k)} = \{\tilde{E}^{(k)}_{a|x}\}$ acting on $\mathbb{C}^{d^k}$ (Alice's side) and a steering functional $\tilde{F}_{\text{KV}}$ induced by G_{KV} such that:

$$\Gamma_s(\sigma(\rho^{\otimes k}, \tilde{\mathbb{E}}^{(k)}), \tilde{F}_{\text{KV}}) \geq C \frac{[F_{\max}(\rho) d]^k}{(\log d^k)^2}, \tag{5}$$

where $F_{\max}(\rho)$ is the fully entangled fraction [15, 16] of the state ρ. This implies that for any state that is non-steerable but with $F_{\max}(\rho) > \frac{1}{d}$ (such as those entangled but non-steerable isotropic states) must exhibit superactivation of EPR steering via the steering functional F_{KV}. More generally, we establish the following result:

Theorem 1 *Given a state ρ acting on $\mathbb{C}^d \otimes \mathbb{C}^d$ and a steering functional $F = \{F^a_x \geq 0\}$. A sufficient condition for ρ to be k-copy $\tilde{F}$-steerable (from Alice to Bob) is*

$$F_{\max}(\rho) > \left[\frac{1}{LV_{\text{MES}}(F)}\right]^{\frac{1}{k}} \tag{6}$$

Here $\tilde{F}$ is a steering functional induced by F through the operation of twirling and $LV_{MES}(F)$ is the largest violation (Eq. (3)) of maximally entangled pure states in $\mathbb{C}^d \otimes \mathbb{C}^d$, such as $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$, with respect to F.

Notice that in the sufficient condition given above, the right-hand-side is phrased in terms of the property of a d-dimensional maximally entangled state, such as $|\Phi_d\rangle$, which illustrates once again the importance of the maximally entangled state as a benchmark for quantum information task. Apart from its own interest, Theorem 1 together with a simple physical argument imply the following estimate for $LV^{\pi}_{\text{MES}}(F)$, where π indicates only projective POVMs are considered: ($H_d = \sum_{i=1}^{d} \frac{1}{i}$)

Corollary 2 *For a steering functional $F = \{F^a_x \geq 0\}$:*

$$LV^{\pi}_{\text{MES}}(F) \leq \frac{d^2}{H_d + H_d d - d}. \tag{7}$$

Note that the upper bound is less than $\frac{d}{\log d}$, which is the current finest upper bound for the largest Bell violation of maximally entangled states under projective measurements [17]. Let us stress the generality of the above corollary: it holds for arbitrary dimension d and arbitrary steering functional that involves only positive semidefinite operators. This upper bound is better than Proposition 2.17 derived recently in [11] by a factor $\frac{1}{\log d}$.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] J. S. Bell, Physics **1**, 195 (1964).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[4] N. Brunner *et al.* Rev. Mod. Phys. **86**, 419 (2014).

[5] E. Schrodinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935); **32**, 446 (1936).

[6] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007); Phys. Rev. A **76**, 052116 (2007).

[7] C. Branciard *et al.*, Phys. Rev. A **85**, 010301(R) (2012).

[8] M. Piani and J. Watrous, Phys. Rev. Lett. **114**, 060404 (2015).

[9] D. Cavalcanti *et al.*, Phys. Rev. A **87**, 042104 (2013).

[10] E. G. Cavalcanti *et al.*, *ibid.* **80**, 032112 (2009).

[11] Z. Yin, M. Marciniak, and M. Horodecki, J. Phys. A: Math. Theor. **48**, 135303 (2015).

[12] C. Palazuelos, Phys. Rev. Lett. **109**, 190401 (2012).

[13] S. A. Khot and N. K. Vishnoi, in Proceedings 46th FOCS, Pittsburgh, pp. 53-62 (2005).

[14] H. Buhrman *et al.*, Theor. Comp. **8**, 623 (2012).

[15] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[16] S. Albeverio, S-M. Fei, and W-L. Yang, Phys. Rev. A **66**, 012301 (2002).

[17] C. Palazuelos, J. Funct. Anal. 267, 1959 (2014)

Visualizing the sets of 3-local and 3-quantum correlations

Rui-Yang You[1] * Denis Rosset[1 2] † Yeong-Cherng Liang[1] ‡

[1] *Department of Physics, National Cheng Kung University, Taiwan*
[2] *Group of Applied Physics, University of Geneva, Switzerland*

Abstract. According to Bell's theorem, quantum systems exhibit stronger correlations than classical systems described by local hidden variables. In standard Bell scenarios, the local hidden variable is shared between all observers; consequently, the set of local correlations is convex. Convexity also holds for the quantum set when sharing a multipartite state between all observers. In quantum networks however, resources have a distribution restricted according to a specific topology; the resulting local and quantum sets are particularly difficult to characterize. Considering the simplest cyclic quantum network, the triangle, we devise a method to sample a three-dimensional slice of local and quantum sets.

Keywords: Quantum nonlocality, causal structures, n-locality, quantum networks, nonlinear Bell-like inequalities

Bell's theorem characterizes the scenarios where all observers have access to the same resource. Consider, for example, an experiment with three observers, who we name Alice, Bob and Charlie. The measurement settings corresponding to these observers are written x, y and z, while the measurement outcomes are written a, b and c. We write the joint probability distribution $P(abc|xyz)$ of observing outcomes (a, b, c) for the choice (x, y, z) of measurement settings, where outcomes and settings are taken from finite sets. Correlations are local if they can be written:

$$P(abc|xyz) = \int_\Lambda \mathrm{d}\lambda \rho_\lambda(\lambda) P_\mathrm{A}(a|x\lambda) P_\mathrm{B}(b|y\lambda) P_\mathrm{C}(c|z\lambda), \tag{1}$$

for suitable local response probabilities P_A, P_B, P_C and a local hidden variable λ taken from the set Λ with distribution ρ_λ. With a suitable enumeration of coefficients, the distribution $P(abc|xyz)$ can be written as a vector $\vec{P} \in \mathbb{R}^n$ where n is the product of the number of outcomes and settings.

Let $\mathcal{L} \subset \mathbb{R}^n$ the set of all $\vec{P}$ obeying (1). It is known that $\mathcal{L}$ is convex; specifically, $\mathcal{L}$ is a polytope formed by the convex hull of a finite number of vertices [1, 2]; alternatively, the polytope can be converted to be represented as the intersection of half-spaces, defining the Bell inequalities [3] revelant to the scenario.

On the other hand, correlations are quantum if they can be written:

$$P(abc|xyz) = \mathrm{tr}\left[\left(M^\mathrm{A}_{a|x} \otimes M^\mathrm{B}_{b|y} \otimes M^\mathrm{C}_{c|z}\right) \rho_\mathrm{ABC}\right], \tag{2}$$

for suitable POVMs $\left\{M^\mathrm{A}_{a|x}\right\}, \left\{M^\mathrm{B}_{b|y}\right\}, \left\{M^\mathrm{C}_{c|z}\right\}$ and a density matrix ρ_ABC. The quantum set is convex as well and can be approximated by semidefinite relaxations using the NPA hierarchy [4]; we write $\mathcal{Q} \subset \mathbb{R}^n$ the set of all $\vec{P}$ obeying (2).

Many algorithms exist to describe the boundary of the local set, and, for visualization purposes, the NPA hierarchy converges sufficiently well. However, when restricting the distribution of local hidden variables and states according to the topology of a network, the problem is much harder.

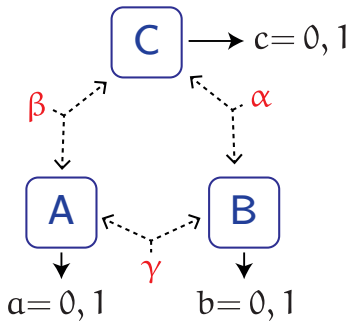


Figure 1: Three observers sharing bipartite resources α, β, γ.

1 Sets of 3-local/3-quantum correlations

Let us now consider a network formed by three sources and three observers, as in Figure 1. To simplify the problem, we assume the observers always

*l26041155@ncku.edu.tw
†denis.rosset@unige.ch
‡ycliang@mail.ncku.edu.tw

perform the same measurement, whose outcomes are binary $a, b, c = 0, 1$.

When the sources are represented by local hidden variables, the resulting set of correlations is given by:

$$P(abc) = \int_{\Lambda_\alpha} \mathrm{d}\alpha \int_{\Lambda_\beta} \mathrm{d}\beta \int_{\Lambda_\gamma} \mathrm{d}\gamma \rho_\alpha(\alpha)\rho_\beta(\beta)\rho_\gamma(\gamma) \cdot P_\mathrm{A}(a|\beta\gamma)P_\mathrm{B}(b|\gamma\alpha)P_\mathrm{C}(c|\alpha\beta). \quad (3)$$

This set, which we write $\mathcal{L}_3$, is known not to be convex [5, 6], and the characterization of its boundary is not known apart from some entropic inequalites [6, 7].

To help in characterizing the set of those correlations, we will consider the subspace of symmetric correlations $\mathcal{S} = \{\vec{P}|P(abc) = P(acb) = P(bca)\} \subset \mathbb{R}^8$.

The subspace $\mathcal{S}$ can be represented in a three-dimensional plot, as normalization shows that:

$$P(000) + 3P(001) + 3P(011) + P(111) = 1. \quad (4)$$

The symmetric correlations P_single, $P_=$, $P_\neq$ are already studied [8]:

	$P(000)$	$P(001)$	$P(011)$	$P(111)$	3-local
P_single	0	1/3	0	0	?
$P_=$	1/2	0	0	1/2	no
$P_\neq$	0	1/6	1/6	0	yes

(5)

Sampling the 3-local correlations. — We plot some of the established inequalities in that scenario [8, 9], along with point cloud samples taken at random in $\mathcal{S} \cap \mathcal{L}_3$ using the following method. We draw the cardinality m of the sets Λ at random between 2 and 15. We then take $\Lambda_\alpha = \Lambda_\beta = \Lambda_\gamma = \{1, \ldots, m\}$, and draw a random discrete distribution $P_\alpha(\alpha)$. We also draw a random response function $P_\mathrm{A}(a|\beta\gamma)$. We reuse the distribution P_α for P_β, P_γ as well, and the response function P_A for P_B and P_C. This guarantees that the resulting correlations are symmetric:

$$P(abc) = \sum_{\alpha,\beta,\gamma=1}^{m} P_\alpha(\alpha)P_\beta(\beta)P_\gamma(\gamma) \cdot P_\mathrm{A}(a|\beta\gamma)P_\mathrm{B}(b|\gamma\alpha)P_\mathrm{C}(c|\alpha\beta). \quad (6)$$

We then repeat the process a sufficient number of times to populate $\mathcal{S} \cap \mathcal{L}_3$.

Sampling the 3-quantum correlations. — We follow the same reasoning for 3-quantum correlations, where no state is shared by the three observers, only bipartite states $\rho_\mathrm{A'B}$, $\rho_\mathrm{B'C}$, $\rho_\mathrm{C'A}$. To start with, we draw a random qubit state $\rho_\mathrm{A'B}$, along with a random POVM element $M_0^\mathrm{AA'}$ corresponding to the outcome $a = 0$. The same state is reused for $\rho_\mathrm{B'C}$, $\rho_\mathrm{C'A}$, and the same POVM element for $M_0^\mathrm{BB'}$, $M_0^\mathrm{CC'}$. The resulting correlations are written:

$$P(abc) = \mathrm{tr}\Big[(\rho_\mathrm{A'B} \otimes \rho_\mathrm{B'C} \otimes \rho_\mathrm{C'A}) \cdot \Big(M_a^\mathrm{AA'} \otimes M_b^\mathrm{BB'} \otimes M_c^\mathrm{CC'} \Big) \Big], \quad (7)$$

where the tensor product ordering is specified by the indices.

References

[1] I. Pitowsky. *Quantum Probability – Quantum Logic* Springer, Berlin, 1989.

[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478, 2014.

[3] K. Fukuda and A. Prodon. Double description method revisited. In *Combinatorics and Computer Science*, number 1120 in Lecture Notes in Computer Science, pages 91–111. Springer Berlin Heidelberg, 1996.

[4] M. Navascués, S. Pironio and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):73013, 2008.

[5] C. Branciard, D. Rosset, N. Gisin and S. Pironio. Bilocal versus nonbilocal correlations in entanglement-swapping experiments. *Physical Review A*, 85(3):32119, 2012.

[6] T. Fritz. Beyond Bell's theorem: correlation scenarios. *New Journal of Physics*, 14(10):103001, 2012.

[7] J. Henson, R. Lal and M. F. Pusey. Theory-independent limits on correlations from generalized Bayesian networks. *New Journal of Physics*, 16(11):113043, 2014.

[8] R. Chaves. Talk at the *Quantum networks workshop*, ICFO, 2016.

[9] E. Wolfe, R.W. Spekkens and T.Fritz Talk at the *Quantum networks workshop*, ICFO, 2016 and work in preparation.