August 30, 2016 (Tuesday)

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

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

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.

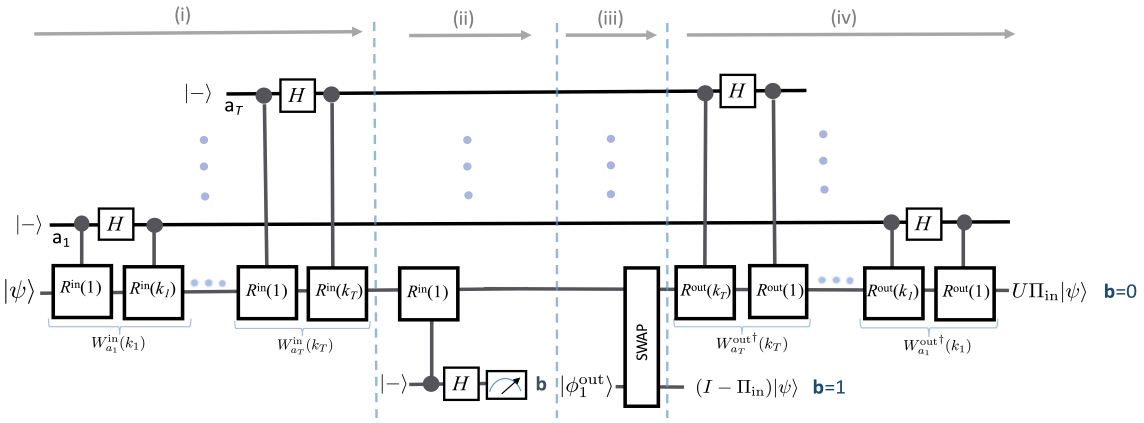

Figure 1: The quantum circuit for emulating unitary transformation U for the special case of pure input-output sample pairs. Here $k_1, \cdots, k_T$ are $T = \text{poly}(d)$ integers chosen uniformly at random from integers $1, \cdots, K$. We use the given copies of sample states in S_{in} and S_{out} 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.

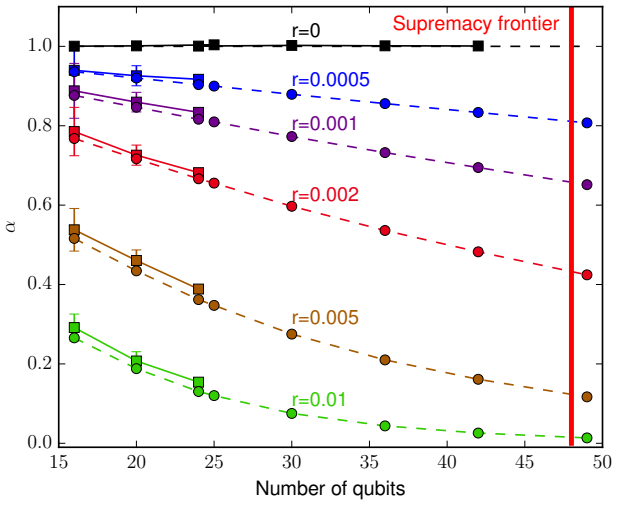

Figure 1: The circuit fidelity α as a function of the number of qubits. Different colors correspond to different Pauli error rates $r_2 = r_{\text{init}} = r_{\text{mes}} = r$ and $r_1 = r/10$. The circle markers correspond to the estimated fidelity, Eq. (14). The square markers correspond to the average 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].

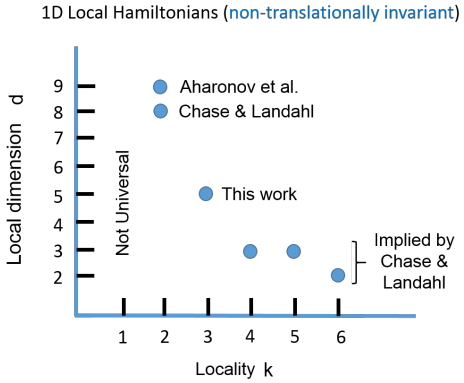

Figure 1: (color online) The status of locality k vs. local Hilbert-space dimension (level) d for universal quantum computation (BQP) in one spatial dimension.

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

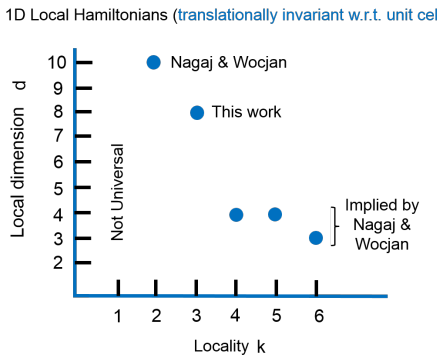

Figure 2: (color online) The translation invariant case.

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].

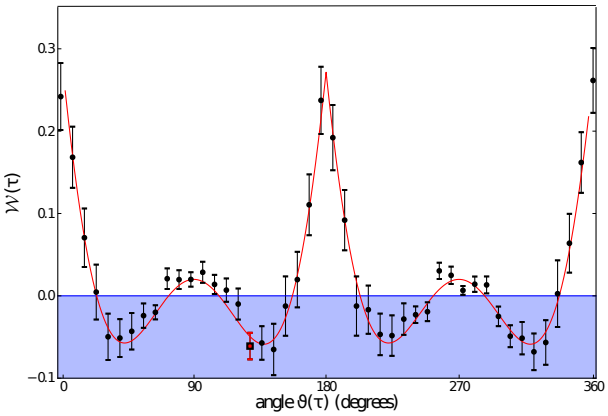

Figure 1: Experimental value of the witness $\mathcal{W}$ upon variation of a parameter θ (see [7] for more details). Non-Bell-correlated states can only achieve a value of $\mathcal{W} \geq 0$. The red dot is 3.8 standard deviations from the bound, demonstrating that the measured state can useful for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

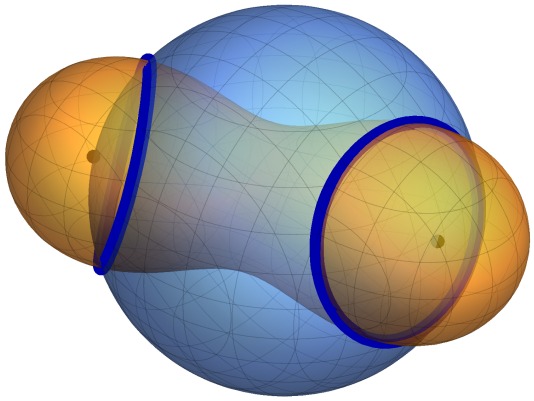

Figure 1: The curves of constant entanglement for the concurrence (or any other polynomial measure in two-root states). The curves obtained as the intersection of the surface with the Bloch sphere show all states with a given value of entanglement.

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.*