Quantum Information and Computation, Vol. 11, No. 9&10 (2011) 0813–0819

DECIDING UNITARY EQUIVALENCE BETWEEN MATRIX POLYNOMIALS AND SETS OF BIPARTITE QUANTUM STATES

ERIC CHITAMBAR
Department of Physics, University of Toronto
Toronto, Ontario M5S 3G4, Canada

CARL A. MILLER
Department of Electrical Engineering and Computer Science, University of Michigan
Ann Arbor, Michigan 48109-2121, USA

YAOYUN SHI
Department of Electrical Engineering and Computer Science, University of Michigan
Ann Arbor, Michigan 48109-2121, USA

Received November 5, 2010
Revised July 12, 2011

In this brief report, we consider the equivalence between two sets of $m+1$ bipartite quantum states under local unitary transformations. For pure states, this problem corresponds to the matrix algebra question of whether two degree m matrix polynomials are unitarily equivalent; i.e. $UA_iV^\dagger = B_i$ for $0 \leq i \leq m$ where U and V are unitary and (A_i, B_i) are arbitrary pairs of rectangular matrices. We present a randomized polynomial-time algorithm that solves this problem with an arbitrarily high success probability and outputs transforming matrices U and V.

Keywords: Unitary Transformations, Matrix Polynomials, Schwartz-Zippel Lemma
Communicated by: S Braunstein & H Zbinden

1 Introduction

With entanglement being one key component in the design and operation of quantum computers, it has become natural to treat entanglement as a resource which we extract from quantum systems and put to use. Under this interpretation, much research has been devoted to quantifying the amount of entanglement present in the state of a given system [1]. However, it was soon realized that no single quantification or entanglement measure can fully capture a state's non-classical properties, and thus one must first stipulate a relative measure when asking how much entanglement some state possesses [2]. A common property of all meaningful measures is that entanglement between two subsystems cannot increase on average when manipulations are *local*, or applied to each subsystem distinctly; *global* actions are required to increase entanglement [3]. Because of the reversibility in unitary evolution, an immediate consequence of this is that for all entanglement measures, entanglement remains constant under local unitary operations (LU). As a result, studying LU equivalence is important since it identifies states that have the same amount of entanglement.

With this motivation, we investigate the question of when two sets of bipartite states are simultaneously related by a local unitary operation. While we will focus primarily on pure states, a precise statement of the general problem is the following: given two sets of states $\{\rho_0, ..., \rho_m\}$ and $\{\sigma_0, ..., \sigma_m\}$ shared between parties Alice and Bob, when is it possible for the duo to apply a fixed local unitary operation that pairwise transforms $\rho_i \stackrel{\text{LU}}{\to} \sigma_i$ for $0 \leq i \leq m$? In the specific case of just a single *pure* state pair ρ and σ, LU equivalence is decided by an equivalence in eigenvalues of the reduced density matrices [4]. This generalizes to the theory of polynomial invariants when more than two parties are considered [5, 6]. In the case of bipartite *mixed* states, equivalence between ρ and σ is determined by a set of trace invariants for certain classes of states [7, 8], but the full solution to bipartite mixed state LU equivalence still remains open. The generalization of these questions to simultaneous LU equivalence between multiple pairs of states has yet to be addressed, and such an investigation nicely complements previous work on simultaneous state transformations under global operations [9, 10, 11] and simultaneous *stochastic* local state transformations between two pairs of pure states [12].

Upon first inspection, when the two sets $\{\rho_0, ..., \rho_m\}$ and $\{\sigma_0, ..., \sigma_m\}$ consist of pure states, it seems relatively simple to decide whether there are fixed U and V such that $\rho_i \stackrel{U\otimes V}{\to} \sigma_i$ for all i. This is because if there exists at least one state $tr_A(\rho_i)$ having only one-dimensional eigenspaces (i.e. its eigenspectrum is non-degenerate), then the action of both U and V is fixed: they must map the eigenvectors to eigenvectors. However, as soon as degeneracy appears, the problem becomes highly non-trivial and there exists no previously known solution. We are motivated to study these non-generic cases because in quantum information they correspond to some of the most interesting physical scenarios, such as when the ρ_i or σ_i are maximally entangled. For instance, the task of teleportation [13], entanglement distillation/dilution [14], and quantum channel coding [15] all use states pure states with reduced density matrices having degenerate eigenvalues.

In this report, we present a randomized polynomial-time algorithm that decides whether *any* two sets of bipartite pure states can be made equivalent by a fixed local unitary operation. For sets of N-partite mixed states, the algorithm can be used to decide whether each pair is simultaneously equivalent under the same *unilocal* unitary operation. These are special operations in which just a single party applies a local unitary while the other subsystems are left unperturbed. Our algorithm applies to sets of any size and the probability of failure can be made arbitrarily small since the randomness arises from a polynomial identity testing subroutine in the algorithm. Finally, we note that our result can also decide general (not just unilocal) LU equivalence between two bipartite mixed states having distinct eigenvalues. This is because if $\rho = \sum_i c_i |\phi_i\rangle\langle\phi_i|$ with $c_i > c_{i+1}$ and $\sigma = \sum_i c'_i |\phi'_i\rangle\langle\phi'_i|$ with $c'_i > c'_{i+1}$, then ρ and σ are LU iff $c_i = c'_i$ and $|\phi_i\rangle, |\phi'_i\rangle$ are LU equivalent for all i. Hence, we see that LU equivalence between these mixed states reduces to the problem of converting one set of pure states to another by a fixed LU operation.

As explained in further detail below, our question of investigation can be phrased as a purely linear algebraic problem of deciding for $m+1$ pairs of $d_1 \times d_2$ matrices (X_i, Y_i) whether there exists unitary matrices U and V such that $UX_iV^\dagger = Y_i$ for all i. To our knowledge, this problem has not yet been studied either in the linear algebra community, although Radjavi has solved the special case of square matrices and $U = V$ [16].

The problem can be phrased in a manner better suited for deeper analysis by introducing degree m matrix polynomials $\mathcal{P}(\lambda) = \sum_{i=0}^{m} \lambda^i X_i$ and $\mathcal{Q}(\lambda) = \sum_{i=0}^{m} \lambda^i Y_i$. Two matrix polynomials are called *unitarily equivalent* if $U\mathcal{P}V^\dagger = \mathcal{Q}$, and we see that $UX_iV^\dagger = Y_i$ for all i if and only if their corresponding matrix polynomials are unitarily equivalent. There is also a more general notion of matrix polynomial equivalence in which $\mathcal{P} \sim \mathcal{Q}$ if there exists invertible constant matrices A and B such that $A\mathcal{P}B^{-1} = \mathcal{Q}$. The underlying technique of our algorithm also works to decide when two matrix polynomials are equivalent in this latter sense.

Deciding unitary equivalence of matrix polynomials is one example of a more general problem which we will consider called the **Unitary Equivalence Problem** (UEP):

> Suppose G_1 and G_2 are sub-algebras of $\mathbb{C}^{d_1\times d_1}$ and $\mathbb{C}^{d_2\times d_2}$, respectively. For two sets of matrices $\{X_i\}_{i=0,\ldots,m}$ and $\{Y_i\}_{i=0,\ldots,m}$ with $X_i, Y_i \in \mathbb{C}^{d_1\times d_2}$, decide if there exists a unitary solution U and V to the system of equations
>
> $$\chi = \{UX_iV^\dagger = Y_i | U \in G_1, V \in G_2\}. \tag{1}$$

The UEP formulation generalizes many different unitary equivalence problems. For instance, if we let $G_1 = \mathbb{C}^{d_1\times d_1}$ and $G_2 = \mathbb{C}^{d_2\times d_2}$, we recover the question of whether there exists general unitaries U and V such that $UX_iV^\dagger = Y_i$ for all pairs (X_i, Y_i). If we furthermore consider $d_1 = d_2$ with one pair of matrices both being the identity matrix (I_{d_1}, I_{d_1}), the question becomes whether $UX_iU^\dagger = Y_i$ for all i. An example of a nontrivial algebra G_1 is the set $\{M \otimes I_b : M \in \mathbb{C}^{a\times a}\}$ where $ab = d_1$.

It is easy to see the connection between UEP and the simultaneous LU equivalence between bipartite states. The states of a $d_1 \times d_2$-dimensional bipartite system can be represented as vectors $|\psi\rangle$ in the product space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, and linear operators on this space correspond to physical actions on the system. By choosing some basis $|i\rangle_1$ and $|i\rangle_2$ for spaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$ respectively, any state can be written as $|\psi\rangle = (I \otimes \psi)|\Phi\rangle$ where $|\Phi\rangle = \sum_{i=1}^{d} |i\rangle_1|i\rangle_2$. This allows for a bipartite pure state $|\psi\rangle$ to be identified with the matrix $\psi \in \mathbb{C}^{d_1\times d_2}$ so that the transformation $|\psi\rangle \to (A\otimes B)|\psi\rangle$ corresponds to $\psi \to A\psi B^T$. Consequently, simultaneous LU equivalence between states $\{|\psi_i\rangle\}_{i=0\ldots m}$ and $\{|\phi_i\rangle\}_{i=0\ldots m}$ amounts to whether $U\psi_iV^\dagger = \phi_i$ for all i. For bipartite mixed states, the UEP is encountered only in the restricted setting of unilocal equivalence. Since mixed states themselves are represented by elements in $\mathbb{C}^{d_1d_2\times d_1d_2}$, unilocal unitary equivalence between states ρ and σ is the question of whether $(U\otimes I_{d_2})\rho(U^\dagger \otimes I_{d_2}) = \sigma$, which as noted above is an UEP instance. Note that in the case of simultaneous unilocal equivalence of mixed states, the reduction to UEP applies to systems with an arbitrary number of parties.

2 The Algorithm

As we will see in greater detail, the UEP can be solved by determining whether or not a particular system of quadratic equations has a nontrivial solution. One strategy sometimes helpful for dealing with quadratic constraints is to relax the problem into a system of linear equations such that a solution to the new equations will solve the original with high probability. We demonstrate this idea on the problem of deciding whether two $d_1 \times d_2$ (assume $d_2 \geq d_1$) matrix polynomials $\mathcal{P} = \sum_{i=0}^{m} \lambda^i X_i$ and $\mathcal{Q} = \sum_{i=0}^{m} \lambda^i Y_i$ are generally equivalent,

i.e. $\mathcal{P} \sim \mathcal{Q}$. In other words, does the system of equations

$$\chi_1 = \{AX_iB^{-1} = Y_i | A \in \mathbb{C}^{d_1 \times d_1}, B \in \mathbb{C}^{d_2 \times d_2}, 0 \leq i < m\} \tag{2}$$

have a nonzero solution for invertible A and B? Clearly χ_1 has such a solution iff there are nonzero invertible solutions to

$$\chi_1' = \{AX_i = Y_iB | A \in \mathbb{C}^{d_1 \times d_1}, B \in \mathbb{C}^{d_2 \times d_2}, 0 \leq i < m\}. \tag{3}$$

There are $O(md_2^2)$ linear equations in χ_1' which can be solved thus placing constraints on the $O(d_2^2)$ free variables of A and B. A matrix solution space to χ_1' is then generated by expressing $A \oplus B$ in terms of the remaining free variables, and χ_1 has a solution iff there exists a nonsingular element in this space.

A standard randomized algorithm for deciding whether a matrix subspace has a full rank element consists of evaluating the degree $O(d_2^2)$ real polynomial $|Det(A \oplus B)|^2$ for randomly selected values of the free variables. The Schwartz-Zippel Lemma states that for some n-variate polynomial $f(x_1, \cdots, x_n)$ over a field $\mathbb{K}$ and having degree no greater than d, if f is not identically zero, then $\text{Prob}[f(x_1', \cdots, x_n') = 0] \leq \frac{d}{|X|}$ where each x_i' is independently sampled from some finite set $X \subset \mathbb{K}$ [17, 18, 19].

To use the Schwartz-Zippel Lemma for testing whether $|Det(A \oplus B)|^2$ is identically zero with success probability at least $1 - \frac{2d_2^2}{|X|}$, one evaluates it on values randomly chosen from set $X \subset \mathbb{R}$ and decides a zero identity if and only if the evaluation output is zero. As any polynomial number of linear equations can be solved in a polynomial amount of time in order to obtain the space $A \oplus B$, we thus have an efficient method for deciding whether $\mathcal{P} \sim \mathcal{Q}$ up to any probabilistic degree of certainty. We note that the Schwartz-Zippel technique can also be used in the study of bipartite entanglement distillation from a multipartite-party state [20].

To solve χ, we work analogously to χ_1 but with additional constraints enforced. Consider the system

$$\chi' = \{AX_i = Y_iB, X_iB^\dagger = A^\dagger Y_i | A, A^\dagger \in G_1, B, B^\dagger \in G_2;, 0 \leq i < m\}. \tag{4}$$

Then we have

Theorem 1: *χ has a solution iff χ' has an invertible solution A and B.*

Proof: If such a solution for χ' exists, then $A^\dagger AX_i = X_iB^\dagger B$ and $AA^\dagger Y_i = Y_iBB^\dagger$. But these equations imply $p(A^\dagger A)X_i = X_ip(B^\dagger B)$ and $p(AA^\dagger)Y_i = Y_ip(BB^\dagger)$ where p is any polynomial function. Let x_i denote the distinct eigenvalues from the combined spectrums $\lambda(A^\dagger A) \cup \lambda(B^\dagger B)$. Let X be the Vandermonde matrix of the x_i, and v the column matrix whose entries are $\sqrt{x_i}^{-1}$. Then the entries of $X^{-1}v$ provide the coefficients of a polynomial $p(t)$ such that $p(A^\dagger A) = \sqrt{A^\dagger A}^{-1}$ and $p(B^\dagger B) = \sqrt{B^\dagger B}^{-1}$ (see Appendix). Note also that $p(A^\dagger A) \in G_1$ and $p(B^\dagger B) \in G_2$. Define unitary matrices $U = A\sqrt{A^\dagger A}^{-1} \in G_1$ and $V = B\sqrt{B^\dagger B}^{-1} \in G_2$. Then $UX_i = AX_i\sqrt{B^\dagger B}^{-1} = Y_iB\sqrt{B^\dagger B}^{-1} = Y_iV$. ■

Matrix bases for G_1 and G_2 will contain no more than d_2^2 elements so that χ' represents $O(md_2^2)$ linear constraints on $O(d_2^2)$ free variables. Indeed, two additional variable matrices

M,N can be introduced to χ' giving the equations $AX_i = Y_iB$, $X_iN = MY_i$, $B^\dagger = N$, $A^\dagger = M$, $A, M \in G_1$, and $B, N \in G_2$. A solution matrix space $A \oplus B$ is generated, and like before, a polynomial identity test can be applied to decide with arbitrarily high probability whether this space contains a nonsingular element. If a nonsingular element is found, use the A and B to form unitaries U and V as in Theorem 1.

To help demonstrate how the algorithm works, we provide a very simple example. Let σ_1 and σ_3 be the Pauli matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ respectively. Consider the UEP problem of whether there exists unitaries U and V such that $U\sigma_1V^\dagger = \sigma_3$ and $U\sigma_3V^\dagger = \sigma_1$. In terms of quantum states, this problem is equivalent to deciding whether there exists $U \otimes V$ such that $(U \otimes V)|\psi_1\rangle = |\psi_3\rangle$ and $(U \otimes V)|\psi_3\rangle = |\psi_1\rangle$, where $|\psi_1\rangle = \sqrt{\frac{1}{2}}\,(|01\rangle + |10\rangle)$ and $|\psi_3\rangle = \sqrt{\frac{1}{2}}\,(|00\rangle - |11\rangle)$. By introducing complex matrices $A = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right)$, we consider the relaxed problem χ' of deciding whether there exists invertible A and B such that

$$\begin{aligned} A\sigma_1 &= \sigma_3 B, \\ \sigma_1 B^\dagger &= A^\dagger \sigma_3, \\ A\sigma_3 &= \sigma_1 B, \\ \sigma_3 B^\dagger &= A^\dagger \sigma_1. \end{aligned} \tag{5}$$

A solution to this consists of real values such that $a_1 = b_2 = -a_4 = b_3$ and $a_2 = b_1 = -b_4 = a_3$. In other words, the solution is a two-parameter matrix space given by

$$A \oplus B = \left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} b & a \\ a & -b \end{smallmatrix}\right) \tag{6}$$

for real a and b. An invertible solution to χ' exists iff $|\det A \oplus B| = (a^2 - b^2)^2$ is not identically zero. In this simple example it is easy to see this is not the case. However, for multiple matrices of greater size, this will not be immediately obvious. Fortunately, the Schwartz-Zippel Lemma assures us that by evaluating $|\det A \oplus B|$ for randomly chosen values, with arbitrarily high probability it will be zero iff it is identically zero. In the case that an invertible solution to χ' exists, a solution to χ can be constructed using the method of Theorem 1. In our example, for $a = 0$ and $b = 1$, we have $U = \sigma_1$ and $V = \sigma_3$ so that $\sigma_1\sigma_1\sigma_3 = \sigma_3$ and $\sigma_1\sigma_3\sigma_3 = \sigma_1$.

3 Conclusion

In this article we have studied the general problem of determining when a set of matrix transformations can be simultaneously achieved by a left and right unitary action. Physically, this corresponds to performing multiple transformations between bipartite pure states with the same local action and leaving the total entanglement unchanged. Our analysis also extends to the situation of simultaneous unilocal unitary transformations on N-partite mixed states. We have developed a polynomial-time randomized algorithm that decides the problem with high probability and also provides a unitary solution if it exists. In a subsequent work, Miller and Shi [21] showed that the algorithm in [16] can, in fact, be adapted to solve equations of the form $UX_iV^\dagger = Y_i$ deterministically and in polynomial time. However, their approach is different from ours, as it directly makes use of the unitary constraints, instead of solving an

invertible equivalence problem. Indeed, our technique here has broader applicability as it can be adopted to solve questions of general matrix polynomial equivalence $P \sim Q$ as described in the introduction.

Related open questions concern simultaneous general LU equivalence between sets of bipartite mixed states and of states having more than three parties. However, for this latter question, it appears the matrix polynomial and randomized techniques used above apply only to the types of LU equivalence considered in this report.

Acknowledgements

This work was supported in part by the National Basic Research Program of China under Awards 2011CBA00300 and 2011CBA00301, the NSF of the United States under Awards 0622033 and 1017335. E.C. is partially supported by CIFAR, CRC, NSERC, and QuantumWorks.

References

1. R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki (2009), *Quantum Entanglement*, Rev. Mod. Phys., 81, pp. 865-942.
2. M. Horodecki, P. Horodecki, and R. Horodecki (1998), *Mixed-State Entanglement and Distillation: Is There a Bound Entanglement in Nature?*, Phys. Rev. Lett., 80, pp. 5239-5242.
3. G. Vidal (2000), *Entanglement Monotones*, J. Mod. Opt., 47, pp. 355-376.
4. M. A. Nielsen and I. L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press.
5. N. Linden and S. Popescu (1998), *On Mult-Particle Entanglement*, Forts. der Phys., 46, pp. 567-578.
6. M. Grassl, M. Rtteler, T. Beth (1998), *Computing Local Invariants of Quantum-Bit Systems*, Phys. Rev. A, 58, pp. 1833-1839.
7. S. Albeverio, S.-M. Fei, P. Parashar, and W.-L. Yang (2003), *Nonlocal Properties and Local Invariants for Bipartite Systems*, Phys. Rev. A, 68, pp. 010303.
8. B.-Z. Sun, S.-M. Fei, X. Li-Jost, and Z.-X. Wang (2006), *A Note on Equivalence of Bipartite States Under Local Unitary Transformations*, J. Phys. A: Math. and Gen., 39, pp. L43-L47.
9. A. Chefles and S. M. Barnett (1998), *Quantum State Separation, Unambiguous Discrimination and Exact Cloning*, J. Phys. A: Math. and Gen., 31, pp. 10097-10103.
10. A. Chefles (2000), *Deterministic Quantum State Transformations*, Phys. Lett. A, 270, pp. 14-19.
11. Y. Feng, R. Duan, and Z. Ji (2005), *Condition and Capability of Quantum State Separation*, Phys. Rev. A, 72, pp. 012313.
12. Z. Ji, Y. Feng, and M. Ying (2005), *Local Cloning of Two Product States*, Phys. Rev. A, 72, pp. 032324.
13. C. H. Bennett, G. Brassard, C. Crpeau, R. Jozsa, A. Peres, and W. K. Wootters (1993), *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett., 70, pp. 1895-1899.
14. C. Bennett, H. Bernstein, S. Popescu, and B. Schumacher (1996), *Concentrating Partial Entanglement by Local Operations*, Phys. Rev. A, 53, pp. 2046-2052.
15. M.-H. Hsieh, I. Devetak, and A. Winter (2008), *Entanglement-Assisted Capacity of Quantum Multiple-Access Channels*, IEEE Trans. Inf. Theory 54, pp. 3078-3090.
16. H. Radjavi (1962), *On Unitary Equivalence of Arbitrary Matrices*, Trans. Amer. Math. Soc., 104, pp. 363-373.
17. R. DeMillo and R. Lipton (1978), *A Probabilistic Remark on Algebraic Program Testing*, Inf. Process. Lett., 7, pp. 193-195.

18. J. T. Schwartz (1980), *Fast Probabilistic Algorithms for Verification of Polynomial Identities*, J. ACM, 27, pp. 701-717.
19. R. Zippel (1979), Ph.D. thesis, MIT.
20. E. Chitambar, R. Duan, and Y. Shi (2010), *Multipartite-to-Bipartite Entanglement Transformations and Polynomial Identity Testing*, Phys. Rev. A, 81, pp. 052310.
21. C. Miller and Y. Shi (2011), Private Communication.

Appendix: Further details of Theorem 1

Observe that since $A^\dagger A \oplus B^\dagger B$ is hermitian, we can write $A^\dagger A \oplus B^\dagger B = \sum_{i=0}^{d_1-1} x_i |a_i\rangle\langle a_i| \oplus 0_{d_2\times d_2} + 0_{d_1\times d_1} \oplus \sum_{i=d_1}^{d_2-1} x_i |b_i\rangle\langle b_i|$ for real and nonzero x_i, where $0_{n\times n}$ is the $n \times n$ all-zeros matrix. Then we search for some polynomial p such that

$$\begin{aligned} p(A^\dagger A) \oplus p(B^\dagger B) &= \sum_{i=0}^{d_1+d_2-1} c_i (A^\dagger A \oplus B^\dagger B)^i \\ &= \sqrt{A^\dagger A}^{-1} \oplus \sqrt{B^\dagger B}^{-1} \\ &= \sum_{i=0}^{d_1-1} \sqrt{x_i}^{-1} |a_i\rangle\langle a_i| \oplus 0_{d_2\times d_2} \\ &\quad + 0_{d_1\times d_1} \oplus \sum_{i=d_1}^{d_2-1} \sqrt{x_i}^{-1} |b_i\rangle\langle b_i|. \end{aligned} \tag{7}$$

The action of the RHS on the eigenvectors of $A^\dagger A$ and $B^\dagger B$ respectively yield the equations $\sqrt{x_i}^{-1} = \sum_{j=0}^{d_1+d_2-1} c_j x_j^i = p(x_i)$ for $i = 0, ..., d_1 + d_2 - 1$. This is a polynomial interpolation problem for which the c_i can be found using the Vandermonde matrix technique described above.