

Tripartite Entanglement Transformations and Tensor Rank

Eric Chitambar,^{1,*} Runyao Duan,^{2,+} and Yaoyun Shi^{3,‡}

¹Physics Department, University of Michigan, 450 Church Street, Ann Arbor, Michigan 48109-1040, USA

²State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

³Department of Electrical Engineering and Computer Science, University of Michigan, 2260 Hayward Street, Ann Arbor, Michigan 48109-2121, USA

(Received 30 May 2008; published 2 October 2008)

A basic question regarding quantum entangled states is whether one can be probabilistically converted to another through local operations and classical communication exclusively. While the answer for bipartite systems is known, we show that for tripartite systems, this question encodes some of the most challenging open problems in mathematics and computer science. In particular, we show that there is no easy general criterion to determine the feasibility, and in fact, the problem is NP hard. In addition, we find obtaining the most efficient algorithm for matrix multiplication to be precisely equivalent to determining the maximum rate to convert the Greenberger-Horne-Zeilinger state to a triangular distribution of three EPR states. Our results are based on connections between multipartite entanglement and tensor rank (also called Schmidt rank), a key concept in algebraic complexity theory.

DOI: 10.1103/PhysRevLett.101.140502

PACS numbers: 03.67.Mn, 03.65.Ud, 89.70.Eg

One of the greatest discoveries in quantum physics [1] is that a multipartite quantum system can be in a so-called entangled state. There is an uncountable number of entangled states realizable by any quantum system, and a natural question is whether two given states can be converted to each other through local operations and classical communications (LOCC), i.e., a protocol in which no quantum information is exchanged among the subsystems.

As the notion of probability is inherent to quantum mechanics, the more natural question is with what probability p can $|\phi\rangle$ be converted into $|\psi\rangle$ under LOCC. For $p = 1$, the LOCC transformation is called deterministic, and for a general nonzero p , the protocol is called stochastic (SLOCC). Transformations of the latter form are written as $|\phi\rangle \xrightarrow{\text{SLOCC}} |\psi\rangle$. For bipartite systems, the problem is completely solved. Nielsen has provided necessary and sufficient conditions for whether two states are deterministically convertible [2]. Probabilistically, any bipartite state $|\phi\rangle$ can be transformed into $|\psi\rangle$ if and only if the matrix rank of the reduced density operator of $|\phi\rangle$ is greater than that of $|\psi\rangle$. Furthermore, Vidal [3] has derived a simple formula that gives the optimal probability for conversion.

When the number of subsystems is greater than 2, the situation becomes much more complicated. No longer can SLOCC convertibility be determined by examining the ranks of the reduced density matrices of the initial and final states. For example, a system of three qubits can be partitioned into six equivalence classes defined by SLOCC convertibility between states in the same class [4]. However, the Greenberger-Horne-Zeilinger (GHZ) and W states, $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, represent two states of distinct SLOCC classes despite having the same subsystem density matrix ranks. Likewise for four qubit systems, there exists nine

different families of equivalence classes indistinguishable by density matrix ranks alone [5].

In this Letter, we ask whether there is some relatively simple criterion for determining the convertibility of arbitrary tripartite states like there is for bipartite states. As a complete solution to the convertibility problem should be able to determine whether one state can be transformed into another with a nonzero probability, we focus our attention on the class of SLOCC protocols to judge the difficulty of the complete problem. Ultimately we find that no simple criterion exists for testing the possibility of a general tripartite entanglement transformation. In addition, through the course of investigating this problem, many other interesting results are obtained concerning specific tripartite transformation rates. The novel conversion rates are derived in part from our observation that the Schmidt measure (to be defined below) is not an additive quantity, something previously thought to be true in the quantum information community [6], but a result already acknowledged in algebraic complexity theory (see exercise 14.12 of [7]). We now summarize our main findings.

Denote by $|\Phi^3\rangle$ the unnormalized tripartite state where any two parties share an (unnormalized) EPR state $|\Phi\rangle = |00\rangle + |11\rangle$, i.e., $|\Phi^3\rangle = |\Phi\rangle_{AB}|\Phi\rangle_{AC}|\Phi\rangle_{BC} = \sum_{i,j,k=0}^1 |ij\rangle_A |ik\rangle_B |jk\rangle_C$. The following statements are true.

Theorem 1.—(a) The following problem is NP hard: Given the classical description (e.g., a binary encoding) of two tripartite states $|\phi\rangle$ and $|\psi\rangle$, decide if $|\phi\rangle \xrightarrow{\text{SLOCC}} |\psi\rangle$. (b) $|\text{GHZ}\rangle^{\otimes 3} \xrightarrow{\text{SLOCC}} |W\rangle^{\otimes 2}$. (c) $|\text{GHZ}\rangle^{\otimes 17} \xrightarrow{\text{SLOCC}} |\Phi^3\rangle^{\otimes 6}$. (d) Let $\lambda = \inf\{u: |\text{GHZ}\rangle^{\otimes \lfloor un \rfloor} \xrightarrow{\text{SLOCC}} |\Phi^3\rangle^{\otimes n}$ for sufficiently large n \}. Then λ is precisely the *exponent for matrix multiplication*, i.e., the smallest real number ω such that two N by N matrices can be multiplied with $O(N^\omega)$ number of multiplications between linear functions

on entries of the first matrix and linear functions on entries of the second matrix.

Previously, only one copy of the W state is known to be convertible from three copies of GHZ and result (b) provides an improvement to this rate. Transformation (c) is important because it reveals that the three-party EPR extraction rate from GHZ is greater than 1, a previously unknown possibility.

Our main technical tool is tensor rank, a key concept in algebraic complexity theory [7] that has also been used to measure multipartite entanglement under the synonymous names of Schmidt rank and Schmidt measure [6]. The tensor rank of a multipartite state $|\phi\rangle \in H_1 \otimes H_2 \otimes \cdots \otimes H_n$, denoted by $rk(|\phi\rangle)$, is the minimum number r such that there exists $|\phi_j\rangle_i \in H_i$, $1 \leq j \leq r$, and

$$|\phi\rangle = \sum_{j=1}^r \bigotimes_{i=1}^n |\phi_j\rangle_i.$$

The quantity $\log_2(rk(|\phi\rangle))$ is called the Schmidt measure of $|\phi\rangle$, denoted by $\text{sch}(|\phi\rangle)$. As emphasized, the proof of Theorem 1 depends on the nonadditivity of the Schmidt measure, i.e., $\text{sch}(|\phi\rangle \otimes |\psi\rangle) \neq \text{sch}(|\phi\rangle) + \text{sch}(|\psi\rangle)$.

Tensor rank has been used in algebraic complexity theory as it captures the complexity of computing a set of bilinear maps [7] and, in particular, the multiplicative complexity of multiplying two matrices. A set of bilinear maps are polynomials with respect to two distinct groups of indeterminates. The multiplicative complexity of the set is the minimum number of multiplications between the two groups required to evaluate all the polynomials. The multiplication of two $N \times N$ matrices produces a set of N^2 bilinear maps, one for each entry in the $N \times N$ product. The complexity of $N \times N$ matrix multiplication is denoted by $\mu(N, N)$, and the current best upper and lower bounds for $\mu(N, N)$ are $O(N^{2.36})$ and $\frac{5}{2}N^2 - 3N$, respectively [8,9]. The complexity of matrix multiplication is also expressed as $\mu(N, N) = O(N^\omega)$, where ω is called the exponent for matrix multiplication and defined as the smallest real number such that an algorithm exists for multiplying two $N \times N$ matrices using $O(N^\omega)$ multiplications. While ω is hypothesized to be 2, determining the validity of this conjecture is a major open problem in computational science; this implies the difficulty in determining λ of (d). For more details, a good reference is Chap. 28 of [10].

Tensor rank analysis has already shown to be valuable in quantum information as it is the distinguishing property between the $|\text{GHZ}\rangle$ and $|W\rangle$ equivalence classes of three qubits [4,11]. It has also been useful in characterizing the entanglement in graph states [12] as well as studying the distinguishability of states by separable operations [13]. An important property of the tensor rank is that it cannot increase under SLOCC.

Proposition 1.—If $|\phi\rangle \xrightarrow{\text{SLOCC}} |\psi\rangle$, then $rk(|\phi\rangle) \geq rk(|\psi\rangle)$ [14].

Through Proposition 1, the monotonic nature of the tensor rank makes studying it physically worthwhile.

Unfortunately, determining the rank of an arbitrary state is a very difficult problem [15], which is ultimately why there is no simple convertibility test applicable to all tripartite transformations. However, in some special cases it is possible to calculate the tensor rank or at least determine some useful bounds. In this Letter, we establish our main results described above by examining the ranks of certain tripartite states. The following statements are true where each is in a one-to-one correspondence with the main results stated earlier.

Lemma 1.—(a') $|\phi\rangle \in H_A \otimes H_B \otimes H_C$ can be SLOCC converted from state $\frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle_A |i\rangle_B |i\rangle_C$ if and only if $rk(|\phi\rangle) \leq N$. (b') $rk(|W\rangle^{\otimes 2}) \leq 8$. (c') $rk(|\Phi^3\rangle) = 7$. (d') $rk(|\Phi^3\rangle^{\otimes n})$ is the multiplicative complexity for multiplying two $2^n \times 2^n$ matrices.

Extending Lemma 1 to prove Theorem 1 is straightforward. It follows from item (a') that, given a tripartite tensor $|\phi\rangle$ and a number k , deciding if $rk(|\phi\rangle) \leq k$ can be reduced to the question of whether $\sum_{i=1}^k |i\rangle_A |i\rangle_B |i\rangle_C \xrightarrow{\text{SLOCC}} |\phi\rangle$. The former problem is shown to be NP hard by Håstad [15]; thus, the latter is also NP hard [item (a)].

Results (b), (c), and (d) follow directly from applying (a') to (b'), (c'), and (d'), respectively, and using the fact that $rk(|\text{GHZ}\rangle^{\otimes n}) = 2^n$. This equality holds since, as evident by taking a Schmidt decomposition with respect to any bipartition, the tensor rank is always lower bounded by the density matrix rank of any subsystem, which is 2^n for all parties in $|\text{GHZ}\rangle^{\otimes n}$. The 17 to 6 conversion ratio of (c') is important because 6 copies of $|\Phi^3\rangle$ is a total of 18 EPR pairs. Thus, the stochastic EPR distillation rate from multiple copies of $|\text{GHZ}\rangle$ is greater than 1. In fact, (d) shows that this rate can be further improved as the upper bound for ω is lowered. However, the distillation is specific in that the EPR pairs must be shared among all three parties. Indeed, if the EPR pairs are held by just two parties, $rk(|\Phi\rangle^{\otimes n}) = 2^n$ so the EPR distillation rate from n copies of $|\text{GHZ}\rangle$ equals 1. The related problem of EPR distillation from the W state has recently been studied in [16]. There, the authors show that for a single W state, the probability of extracting an EPR state via LOCC is not only higher if one does not specify which two parties share the state, but it can also be made arbitrarily close to 1.

From (d) and the lower bound on $\mu(2^n, 2^n)$, it follows that $2n$ copies of GHZ cannot be converted into n copies of $|\Phi^3\rangle$ with a nonzero probability. This result is stronger than the one derived in [17] where the authors prove strictly by entropy arguments the impossibility of $|\text{GHZ}\rangle^{\otimes 2n} \rightarrow |\Phi^3\rangle^{\otimes n}$ under deterministic LOCC. Here, we obtain the stronger conclusion except by using tools of algebraic complexity theory. It is an interesting question whether these two seemingly unrelated lines of attack are actually deeply connected.

Now we turn to prove Lemma 1. We will work with unnormalized states below since any overall factor does not affect the tensor rank. For any $|\phi\rangle \in H_A \otimes H_B \otimes H_C$, let ρ_{AB} denote Alice and Bob's subsystem obtained by

taking the partial trace $\text{Tr}_C(|\phi\rangle\langle\phi|)$. As ρ_{AB} is a positive operator, it has a spectral decomposition $\rho_{AB} = \sum_{k=1}^m p_k |\psi_k\rangle\langle\psi_k|$ where $0 < p_k \leq 1$. The vector span of $\{|\psi_k\rangle: 1 \leq k \leq m\}$ is called the support of ρ_{AB} and denoted by $\text{supp}(\rho_{AB})$. To proceed, we need the following simple equivalent characterization of a tripartite state's tensor rank.

Lemma 2.—Suppose $|\phi\rangle \in H_A \otimes H_B \otimes H_C$. The tensor rank of $|\phi\rangle$ equals the minimum number of product states in $H_A \otimes H_B$ whose linear span contains the support of $\rho_{AB} = \text{Tr}_C(|\phi\rangle\langle\phi|)$.

Proof.—Let k denote $\text{rk}(|\phi\rangle)$ and r be the minimum number of product states $\{|\alpha_j\rangle|\beta_j\rangle: 1 \leq j \leq r\}$ whose span contains $\text{supp}(\rho_{AB})$. Let $|\phi\rangle = \sum_{i=1}^m |i\rangle_{AB}|i\rangle_C$ be a Schmidt decomposition of $|\phi\rangle$. Each $|i\rangle_{AB}$ belongs to $\text{supp}(\rho_{AB})$ and so $|i\rangle_{AB} = \sum_{j=1}^r \lambda_{i,j} |\alpha_j\rangle|\beta_j\rangle$. Regrouping the $|i\rangle_C$ according to the r product states gives $r \geq k$. However, from $|\phi\rangle = \sum_{i=1}^k |a_i\rangle|b_i\rangle|c_i\rangle$ we have $\rho_{AB} = \sum_{i,j=1}^k |a_i\rangle|b_i\rangle\langle c_j|c_j\rangle\langle a_j|b_j|$ implying that $\text{supp}(\rho_{AB}) \subseteq \text{span}\{|a_i\rangle|b_i\rangle: 1 \leq i \leq k\}$. Thus $k \geq r$. \square

Using Lemma 2, the general procedure for determining tensor rank is now straightforward. Write $|\phi\rangle = \sum_{i=1}^m |i\rangle_{AB}|i\rangle_C$ where the $\{|i\rangle_C: 1 \leq i \leq m\}$ are orthonormal and then determine the minimum number of product states needed to contain the $\{|i\rangle_{AB}: 1 \leq i \leq m\}$. This question can be rephrased in another way by mapping each $|i\rangle_{AB}$ to a bilinear form f_i from the ring of indeterminates $C[\{a_j\}, \{b_j\}]$ where each a_j (b_j) is in a one-to-one correspondence with a basis vector from H_a (H_b). Product states in $H_a \otimes H_b$ correspond to a product of linear forms from $C[\{a_j\}] \times C[\{b_j\}]$, which we refer to as a *nonscalar* multiplication. Thus, we obtain the following fact.

Fact.—The minimum number of product states that contain the $\{|i\rangle_{AB}: 1 \leq i \leq m\}$, and hence the tensor rank of $|\phi\rangle$, is the same number of nonscalar multiplications $M_k = (\sum_{j=1}^{n_a} \alpha_{k,j} a_j) \times (\sum_{j=1}^{n_b} \beta_{k,j} b_j)$ needed to calculate

$$\begin{pmatrix} a_{11} & a_{10} & a_{01} & a_{00} \\ a_{10} & \cdots & a_{00} & \cdots \\ a_{01} & a_{00} & \cdots & \cdots \\ a_{00} & \cdots & \cdots & \cdots \end{pmatrix} = \begin{pmatrix} a_{10} & a_{10} & \cdots & \cdots \\ a_{10} & a_{10} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} + \begin{pmatrix} a_{01} & \cdots & a_{01} & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{01} & \cdots & a_{01} & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} + \begin{pmatrix} a_{00} & \cdots & \cdots & a_{00} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{00} & \cdots & \cdots & a_{00} \end{pmatrix} \\ + \begin{pmatrix} \cdots & \cdots & \cdots & \cdots \\ \cdots & a_{00} & a_{00} & \cdots \\ \cdots & a_{00} & a_{00} & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} + \begin{pmatrix} a_{11} - a_{10} & \cdots & \cdots & \cdots \\ -a_{01} - a_{00} & \cdots & \cdots & \cdots \\ \cdots & -a_{10} - a_{00} & \cdots & \cdots \\ \cdots & \cdots & -a_{01} - a_{00} & \cdots \\ \cdots & \cdots & \cdots & -a_{00} \end{pmatrix}. \quad (2)$$

Note that rank one matrices require only one nonscalar multiplication:

$$\begin{pmatrix} a_i & a_i \\ a_i & a_i \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_i(b_1 + b_2) \\ a_i(b_1 + b_2) \end{pmatrix},$$

while any $n \times n$ diagonal matrix requires n multiplications:

the $\{f_i: 1 \leq i \leq m\}$. We now use the technique outlined above to study the tensor rank of certain tripartite states.

Proof of Lemma 1.—(a') For $\sum_{i=1}^N |i\rangle_A |i\rangle_B |i\rangle_C$, the support of ρ_{AB} is spanned by N product states. Thus by Proposition 1 and Lemma 2, a necessary condition for the given transformation is $\text{rk}(|\phi\rangle) \leq N$. Now suppose that $|\phi\rangle = \sum_{i=1}^k |a_i\rangle|b_i\rangle|c_i\rangle$ where $k \leq N$. Since $\{|i\rangle_A: 1 \leq i \leq N\}$ is an orthonormal set, we can define the linear operator A by

$$A|i\rangle_A = \begin{cases} |a_i\rangle, & 1 \leq i \leq k \\ 0, & k < i \leq N \end{cases}.$$

Similarly, operators B and C can be constructed. As noted in [4], the existence of such operators is sufficient for an SLOCC protocol since $|\phi\rangle$ will be obtained when Alice performs the local measurement $\{A/\|A\|, \sqrt{I_A - (1/\|A\|^2)A^\dagger A}\}$ and similarly for Bob and Charlie. Note that (unnormalized) $|\text{GHZ}\rangle^{\otimes n}$ can be expressed as $\sum_{i=1}^n |i\rangle_A |i\rangle_B |i\rangle_C$. (b') One can verify by direct computation that $|W\rangle^{\otimes 2}$ expands as

$$\begin{aligned} & (|11\rangle_A |00\rangle_B + |10\rangle_A |01\rangle_B + |01\rangle_A |10\rangle_B \\ & + |00\rangle_A |11\rangle_B) |00\rangle_C + (|10\rangle_A |00\rangle_B + |00\rangle_A |10\rangle_B) |01\rangle_C \\ & + (|01\rangle_A |00\rangle_B + |00\rangle_A |01\rangle_B) |10\rangle_C + (|00\rangle_A |00\rangle_B) |11\rangle_C. \end{aligned} \quad (1)$$

The structure of $|W\rangle^{\otimes 2}$ becomes more manageable when working with its corresponding bilinears f_i since they can be succinctly expressed through the matrix multiplication

$$\begin{pmatrix} f_{00} \\ f_{01} \\ f_{10} \\ f_{11} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{10} & a_{01} & a_{00} \\ a_{10} & \cdots & a_{00} & \cdots \\ a_{01} & a_{00} & \cdots & \cdots \\ a_{00} & \cdots & \cdots & \cdots \end{pmatrix} \begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix},$$

where a “ \cdots ” means a 0 entry. We make use of the following identity [18]:

$$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \lambda_3 & \\ & & & \lambda_4 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} \lambda_1 b_1 \\ \lambda_2 b_2 \\ \lambda_3 b_3 \\ \lambda_4 b_4 \end{pmatrix}.$$

Hence, a total of eight nonscalar multiplications is sufficient to compute each f_i . These multiplications correspond

to product states that contain $\text{supp}(\text{Tr}_C(|W\rangle\langle W|^{\otimes 2}))$. By Lemma 2 then, $rk(|W\rangle^{\otimes 2}) \leq 8$. In fact, expansion (2) gives the eight product states that contain $\text{supp}(\text{Tr}_C(|W\rangle\langle W|^{\otimes 2}))$ enabling us to rewrite Alice and Bob's vector attached to $|i\rangle_C$: $i \in \{00, 01, 10, 11\}$ in (1) as a combination of these eight states. Doing so gives the unnormalized decomposition

$$\begin{aligned} |W\rangle^{\otimes 2} = & |10\rangle|0+\rangle|0+\rangle + |01\rangle|+0\rangle|+0\rangle + |00\rangle|\Phi\rangle|\Phi\rangle \\ & + |00\rangle|\Psi\rangle|\Psi\rangle - (|\Phi^-\rangle + |\Psi\rangle)|00\rangle|00\rangle \\ & - |+0\rangle|01\rangle|01\rangle - |0+\rangle|10\rangle|10\rangle - |00\rangle|11\rangle|11\rangle, \end{aligned}$$

where $|\Phi^-\rangle = |00\rangle - |11\rangle$ and $|\Psi\rangle = |01\rangle + |10\rangle$. (c') The corresponding bilinear forms of $|\Phi^3\rangle$ match the set of polynomials obtained when multiplying two 2×2 matrices:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^T \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} f_{00} & f_{01} \\ f_{10} & f_{11} \end{pmatrix}, \quad (3)$$

where T indicates the matrix transpose. An algorithm for obtaining the f_i using only seven multiplications was discovered by Strassen [19] and later proven to be optimal by Winograd [20]. These seven nonscalar multiplications correspond to a minimum number of product states containing $\text{supp}(\text{Tr}_C(|\Phi^3\rangle\langle\Phi^3|))$ and so $rk(|\Phi^3\rangle) = 7$. As an eight term expansion for $|W\rangle^{\otimes 2}$ was obtained from expansion (2), it is straightforward to find a seven term expansion of $|\Phi^3\rangle$ from Strassen's algorithm given in [19]. Since the explicit expressions are not of primary interest here, we omit the calculations. (d') By taking multiple tensor products of the matrices in (3), we see that for n copies of $|\Phi^3\rangle$, the corresponding polynomials are represented by $2^n \times 2^n$ matrix multiplication. Hence, $rk(|\Phi^3\rangle^{\otimes n})$ is the complexity of this operation. \square

In conclusion, we have found that no easy test exists for determining whether two general tripartite states are probabilistically convertible because any general solution involves tripartite tensor rank computation. As a result, one must consider tripartite transformations on a case-by-case basis. In this Letter specific tensor rank analysis has led to an improved GHZ state to W state SLOCC transformation rate as well as a demonstration of obtaining EPR pairs from GHZ states at a rate greater than one with a nonzero probability.

The connection between tensor rank and entanglement transformation opens many avenues of further research as the techniques of algebraic complexity theory might teach us more about the nature and limitations of SLOCC transformations. Conversely, SLOCC entanglement transformations may provide a unique angle to investigate algebraic complexity theory. For example, can we improve the current best matrix multiplication algorithm by constructing an efficient SLOCC transformation protocol? Another specific problem is to prove strong impossibility results on the GHZ to EPR conversion problem within a hierarchy of

SLOCC protocols (e.g., restricting the number of rounds of messages). Such results will shed light on the difficulty of matrix multiplication and may lead to a strong lower bound on ω . Finally, we note that [21] provides another connection of algebraic complexity theory to quantum information. It would be of great interest to broaden the link between these fields.

We thank Jens Eisert, Hoi-Kwong Lo, and Robert Raussendorf for valuable comments. Y.S. also thanks Wei Huang for pointing out exercise 14.12 of [7] and providing helpful discussions. This work was partially supported by the National Science Foundation of the United States under Grants No. 0347078 and No. 0622033. R.D. as partially supported by the National Natural Science Foundation of China (Grants No. 60702080, No. 60736011, and No. 60621062), the FANEDD under Grant No. 200755, and the Hi-Tech Research and Development Program of China (the 863 project) (Grant No. 2006AA01Z102).

*echitamb@umich.edu

+dry@tsinghua.edu.cn

*shiyi@eecs.umich.edu

- [1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [2] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [3] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
- [4] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [5] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).
- [6] J. Eisert and H. J. Briegel, Phys. Rev. A **64**, 022306 (2001).
- [7] P. Burgisser, M. Clausen, and M. Shokrollahi, *Algebraic Complexity Theory* (Springer-Verlag, Berlin, 1997).
- [8] D. Coppersmith and S. Winograd, J. Symb. Comput. **9**, 251 (1990).
- [9] M. Bläser, Theor. Comput. Sci. **331**, 3 (2005).
- [10] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms* (MIT, Cambridge, MA, 2001), 2nd ed.
- [11] J.-L. Brylinski, arXiv:quant-ph/0008031.
- [12] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [13] R. Duan, Y. Feng, Y. Xin, and M. Ying, arXiv:0705.0795.
- [14] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
- [15] J. Håstad, Journal of Algorithms **11**, 644 (1990).
- [16] B. Fortescue and H.-K. Lo, Phys. Rev. Lett. **98**, 260501 (2007).
- [17] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, arXiv:quant-ph/9912039.
- [18] C. M. Fiduccia, in *Complexity of Computer Computations* (Plenum Press, New York, 1972), pp. 31–40.
- [19] V. Strassen, Numer. Math. **13**, 354 (1969).
- [20] S. Winograd, Linear Algebra Appl. **4**, 381 (1971).
- [21] S. Aaronson, arXiv:quant-ph/0311039.