SCISPACE
formerly Typeset

Open access • Journal Article • DOI:10.1103/PHYSREVA.75.042310

Role of entanglement and correlations in mixed-state quantum computation — Source link

Animesh Datta, Guifre Vidal

Institutions: University of New Mexico, University of Queensland

Published on: 11 Apr 2007 - Physical Review A (American Physical Society)

Topics: Quantum algorithm, Quantum discord, Quantum capacity, Amplitude damping channel and Quantum teleportation

Related papers:

- Quantum discord: a measure of the quantumness of correlations.
- Quantum Discord and the Power of One Qubit
- Classical, quantum and total correlations
- Experimental quantum computing without entanglement.
- Entanglement and the power of one qubit

Share this paper:

View more about this paper here: https://typeset.io/papers/role-of-entanglement-and-correlations-in-mixed-state-quantum-1phzla44ej

PHYSICAL REVIEW A **75**, 042310 (2007)

Role of entanglement and correlations in mixed-state quantum computation

Animesh Datta[*]
Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156, USA

Guifre Vidal[†]
School of Physical Sciences, The University of Queensland, Queensland 4072, Australia

(Received 14 November 2006; revised manuscript received 19 March 2007; published 11 April 2007)

In a quantum computation with pure states, the generation of large amounts of entanglement is known to be necessary for a speedup with respect to classical computations. However, examples of quantum computations with mixed states are known, such as the deterministic computation with one quantum qubit (DQC1) model [Knill and Laflamme, Phys. Rev. Lett. **81**, 5672 (1998)], in which entanglement is at most marginally present, and yet a computational speedup is believed to occur. Correlations, and not entanglement, have been identified as a necessary ingredient for mixed-state quantum computation speedups. Here we show that correlations, as measured through the operator Schmidt rank, are indeed present in large amounts in the DQC1 circuit. This provides evidence for the preclusion of efficient classical simulation of DQC1 by means of a whole class of classical simulation algorithms, thereby reinforcing the conjecture that DQC1 leads to a genuine quantum computational speedup.

DOI: 10.1103/PhysRevA.75.042310 PACS number(s): 03.67.Lx

I. INTRODUCTION

Quantum computation owes its popularity to the realization, more than a decade ago, that the factorization of large numbers can be solved exponentially faster by evolving quantum systems than via any known classical algorithm [1]. Since then, progress in our understanding of what makes quantum evolutions computationally more powerful than a classical computer has been scarce. A step forward, however, was achieved by identifying entanglement as a *necessary* resource for quantum computational speedups. Indeed, a speedup is possible only if, in a quantum computation, entanglement spreads over an adequately large number of qubits [2]. In addition, the amount of entanglement, as measured by the Schmidt rank of a certain set of bipartitions of the system, needs to grow sufficiently with the size of the computation [3]. Whenever either of these two conditions is not met, the quantum evolution can be efficiently simulated on a classical computer. These conditions [which are particular examples of subsequent, stronger classical simulation results based on tree tensor networks (TTNs) [4]] are only necessary, and thus not sufficient, so that the presence of large amounts of entanglement spreading over many qubits does not guarantee a computational speedup, as exemplified by the Gottesman-Knill theorem [5].

The above results refer exclusively to quantum computations with pure states. The scenario for mixed-state quantum computation is rather different. The intriguing *deterministic quantum computation with one quantum bit* (DQC1 or "the power of one qubit") [6] involves a highly mixed state that does not contain much entanglement [7] and yet it performs a task, the computation with fixed accuracy of the normalized trace of a unitary matrix, exponentially faster than any known classical algorithm. This also provides an exponential speedup over the best known classical algorithm for simulations of some quantum processes [8]. Thus, in the case of a mixed-state quantum computation, a large amount of entanglement does not seem to be necessary to obtain a speedup with respect to classical computers.

A simple, unified explanation for the pure-state and mixed-state scenarios is possible [3] by noticing that the decisive ingredient in both cases is the presence of *correlations*. Indeed, let us consider the Schmidt decomposition of a vector $|\Psi\rangle$, given by

$$|\Psi\rangle = \sum_{i=1}^{\chi} \lambda_i |i_A\rangle \otimes |i_B\rangle, \tag{1.1}$$

where $\langle i_A | j_A\rangle = \langle i_B | j_B\rangle = \delta_{ij}$ and χ is the rank of the reduced density matrices $\rho_A \equiv \mathrm{Tr}_B[|\psi\rangle\langle\psi|]$ and $\rho_B \equiv \mathrm{Tr}_A[|\psi\rangle\langle\psi|]$; and the (operator) Schmidt decomposition of a density matrix ρ given by [9]

$$\rho = \sum_{i=1}^{\chi^\sharp} \lambda_i^\sharp O_{iA} \otimes O_{iB}, \tag{1.2}$$

where $\mathrm{Tr}(O_{iA}^\dagger O_{jA}) = \mathrm{Tr}(O_{iB}^\dagger O_{jB}) = \delta_{ij}$. The Schmidt ranks χ and $\chi^\sharp$ are a measure of correlations between parts A and B, with $\chi^\sharp = \chi^2$ if $\rho = |\Psi\rangle\langle\Psi|$. Let the density matrix ρ_t denote the evolving state of the quantum computer during a computation. Notice that ρ_t can represent both pure and mixed states. Then, as shown in Refs. [3] and [4], the quantum computation can be efficiently simulated on a classical computer using a TTN decomposition if the Schmidt rank $\chi^\sharp$ of ρ according to a certain set of bipartitions $A:B$ of the qubits scales polynomially with the size of the computation. In other words, a necessary condition for a computational speedup is that correlations, as measured by the Schmidt rank $\chi^\sharp$, grow superpolynomially in the number of qubits. In the case of pure states (where $\chi = \sqrt{\chi^\sharp}$) these correlations are

---

[*] Electronic address: animesh@unm.edu

[†] Electronic address: vidal@physics.uq.edu.au

©2007 The American Physical Society

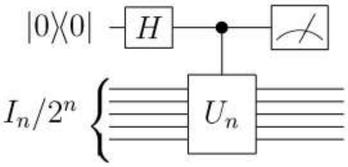
entirely due to entanglement, while for mixed states they may be quantum or classical.

Our endeavor in this paper is to study the DQC1 model of quantum computation following the above line of thought. In particular, we elucidate whether DQC1 can be efficiently simulated with any classical algorithm, such as those in [3,4] (and, implicitly, in [2]), that exploits limits on the amount of correlations, in the sense of a small $\chi^\sharp$ according to certain bipartitions of the qubits. We will argue here that the state ρ_t of a quantum computer implementing the DQC1 model displays an exponentially large $\chi^\sharp$, in spite of it containing only a small amount of entanglement [7]. We will conclude, therefore, that none of the simulation techniques mentioned above can be used to efficiently simulate the power of one qubit.

On the one hand, our result indicates that a large amount of classical correlations is behind the (suspected) computational speedup of DQC1. On the other hand, by showing the failure of a whole class of classical algorithms to efficiently simulate this mixed-state quantum computation, we reinforce the conjecture that DQC1 leads indeed to an exponential speedup. We note, however, that our result does not rule out the possibility that this circuit could be simulated efficiently using some other classical algorithm.

II. DQC1 AND TREE TENSOR NETWORKS

The DQC1 model, represented in Eq. (2.1), provides an estimate of the normalized trace $\mathrm{Tr}(U_n)/2^n$ of an n-qubit unitary matrix $U_n \in \mathbb{U}(2^n)$ with fixed accuracy efficiently [6]. For discussions on the classical complexity of evaluating the normalized trace of a unitary matrix, see [7]:



(2.1)

This quantum circuit transforms the highly mixed initial state $\rho_0 \equiv |0\rangle\langle 0| \otimes I_n/2^n$ at time $t=0$ into the final state ρ_T at time $t=T$,

$$\rho_T = \frac{1}{2^{n+1}}\begin{pmatrix} I_n & U_n^\dagger \\ U_n & I_n \end{pmatrix}, \tag{2.2}$$

through a series of intermediate states ρ_t, $t \in [0,T]$. The simulation algorithms relevant in the present discussion [2–4] require that ρ_t be efficiently represented with a TTN [4] (or a more restrictive structure, such as a product of k-qubit states for fixed k [2] or a matrix product state [3]) at all times $t \in [0,T]$. Here we will show that the final state ρ_T, henceforth denoted simply by ρ, cannot be efficiently represented with a TTN. This already implies that none of the algorithms in [2–4] can be used to efficiently simulate the DQC1 model.

Storing and manipulating a TTN requires computational space and time that grows linearly in the number of qubits n and as a small power of its rank q. The rank q of a TTN is the maximum Schmidt rank $\chi_i^\sharp$ over all bipartitions $A_i : B_i$ of the qubits according to a given tree graph whose leaves are the qubits of our system. See [4] for details. The key observation of this paper is that for a typical unitary matrix U_n, the density matrix ρ in Eq. (2.2) is such that any TTN decomposition has exponentially large rank q. By typical, here we mean a unitary matrix U_n efficiently generated through a (random) quantum circuit. That is, U_n is the product of poly(n) one-qubit and two-qubit gates. In the next section we present numerical results that unambiguously suggest that, indeed, typical U_n necessarily lead to TTNs with exponentially large rank q.

We notice that the results of the next section do not exclude the possibility that the quantum computation in the DQC1 model can be efficiently simulated with a TTN for particular choices of U_n. For instance, if U_n factorizes into single-qubit gates, then ρ can be seen to be efficiently represented with a TTN of rank 3, and we cannot rule out an efficient simulation of the power of one qubit for that case. Of course, this is to be expected, given that the trace of such U_n can be computed efficiently in the first place.

III. EXPONENTIAL GROWTH OF SCHMIDT RANKS

In this section we study the rank q of any TTN for the final state ρ of the DQC1 circuit, Eq. (2.2). We numerically determine that a lower bound to such a rank grows exponentially with the number of qubits n.

The Schmidt rank χ of a pure state $|\rho_{\phi_A\psi_B}\rangle$,

$$|\rho_{\phi_A\psi_B}\rangle \equiv \rho|\phi_A\rangle|\psi_B\rangle = \sum_{i=1}^{\chi^\sharp} \lambda_i^\sharp O_{iA}|\phi_A\rangle \otimes O_{iB}|\psi_B\rangle, \tag{3.1}$$

obtained by applying the density matrix ρ onto a product state $|\phi_A\rangle|\psi_B\rangle$, is a lower bound on the operator Schmidt rank $\chi^\sharp$ of ρ, i.e., $\chi^\sharp \geqslant \chi$. For the purpose of our numerics, we consider the pure state $U_n|0\rangle^{\otimes n}$. We build U_n as a sequence of $2n$ random two-qubit gates, applied to pairs of qubits, also chosen at random. The random two-qubit unitaries are generated using the mixing algorithm presented in [10]. Note that applying $2n$ gates means that the resulting unitary is efficiently implementable, a situation for which the DQC1 model is valid. For an even number of qubits, n, we calculate the smallest Schmidt rank χ over all $n/2 : n/2$ partitions of the qubits (similar results can be obtained for odd n). The resulting numbers are plotted in Fig. 1.

The above numerical results strongly suggest that the final state ρ in the DQC1 circuit has exponential Schmidt rank for a typical unitary U_n. We are not able to provide a formal proof of this fact. This is due to a general difficulty in describing properties of the set $\mathbb{U}_{qc}(2^n)$ of unitary matrices that can be efficiently realized through a quantum computation. Instead, the discussion is much simpler for the set $\mathbb{U}(2^n)$ of generic n-qubit unitary matrices, where it is possible to prove that ρ cannot be efficiently represented with a TTN for a Haar-generated $U_n \in \mathbb{U}(2^n)$, as discussed in the next section. Notice that Ref. [11] claims that random (but efficient) quantum circuits generate random n-qubit gates $U_n \in \mathbb{U}_{qc}(2^n)$ according to a measure that converges to the Haar measure in $\mathbb{U}(2^n)$. Combined with the theorem in the next section, this

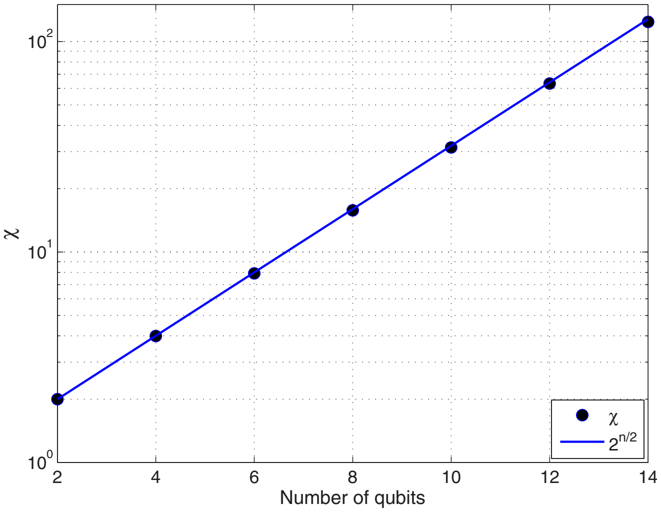


FIG. 1. (Color online) Lower bound for the operator Schmidt rank $\chi^{\sharp}$ of the DQC1 state for any equipartition $n/2:n/2$, as given by the Schmidt rank χ of the pure state in Eq. (3.1). The dots are for even numbers of qubits, and the fit is the line $2^{n/2}$. χ is calculated for a pure state obtained by applying $2n$ random two-qubit gates on the state $|0\rangle^{\otimes n}$. This is evidence that for a typical unitary U_n, the rank q of any TTN for the DQC1 state ρ in Eq. (2.2) grows exponentially with n.

would constitute a formal proof of the otherwise numerically evident exponential growth of the rank q of any TTN for the DQC1 final state ρ.

IV. A FORMAL PROOF FOR THE HAAR-DISTRIBUTED CASE

Our objective in this section is to analyze the Schmidt rank $\chi^{\sharp}$ of the density matrix ρ in Eq. (2.2) for certain bipartitions of the $n+1$ qubits, assuming that $U_n \in \mathbb{U}(2^n)$ is Haar distributed.

It is not difficult to deduce that, for any tree of the $n+1$ qubits, there exists at least one edge that splits the tree into two parts A and B, with n_A and n_B qubits, where $n_0 = \min(n_A, n_B)$ satisfies $n/5 \leqslant n_0 \leqslant 2n/5$. In other words, if a rank-q TTN exists for the ρ in Eq. (2.2), then there is a bipartition of the $n+1$ qubits with n_0 qubits on either A or B and such that the Schmidt rank $\chi^{\sharp} \leqslant q$. Theorem 1, our main technical result, shows that, if U_n is chosen randomly according to the Haar measure, then the Schmidt rank of any such bipartition satisfies $\chi^{\sharp} \geqslant O(2^{n_0})$. Therefore, for a randomly generated $U_n \in \mathbb{U}(2^n)$, a TTN for ρ has rank q (and computational cost) exponential in n, and none of the techniques of [2–4] can simulate the outcome of the DQC1 model efficiently.

Consider now any bipartition $A:B$ of the $n+1$ qubits, where A and B contain n_A and n_B qubits, with the minimum n_0 of those restricted by $n/5 \leqslant n_0 \leqslant 2n/5$. Without loss of generality we can assume that the top qubit lies in A. Actually, we can also assume that A contains the top n_A qubits. Indeed, suppose A does not have the n_A top qubits. Then we can use a permutation P_n on all the n qubits to bring the n_A qubits of A to the top n_A positions. This will certainly modify ρ, but since

$$\begin{pmatrix} P_n & 0 \\ 0 & P_n \end{pmatrix}\begin{pmatrix} I_n & U_n^{\dagger} \\ U_n & I_n \end{pmatrix}\begin{pmatrix} P_n^T & 0 \\ 0 & P_n^T \end{pmatrix} = \begin{pmatrix} I_n & V_n^{\dagger} \\ V_n & I_n \end{pmatrix}, \quad (4.1)$$

where $V_n = P_n U_n P_n^T$ is another Haar-distributed unitary, we obtain that the new density matrix is of the same form as ρ. Finally, in order to ease the notation, we will assume that $n_A = n_0$ (identical results can be derived for $n_B = n_0$). Thus $n/5 \leqslant n_A \leqslant 2n/5$.

We note that

$$\begin{pmatrix} I_n & U_n^{\dagger} \\ U_n & I_n \end{pmatrix} = \mathbb{I}_2 \otimes \mathbb{I}_n + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes U_n^{\dagger} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes U_n, \quad (4.2)$$

so that, if we multiply ρ by the product state

$$|\phi_{\vec{\alpha}}\rangle \equiv |t, i, j\rangle \equiv |t, i_A\rangle |j_B\rangle, \quad (4.3)$$

where $\vec{\alpha} \equiv (t, i, j)$, $t = 0, 1$, $i = 1, \ldots, d_A$, $j = 1, \ldots, d_B$, we obtain $|\psi_{\vec{\alpha}}\rangle \equiv \rho |\phi_{\vec{\alpha}}\rangle$ where

$$|\psi_{\vec{\alpha}}\rangle = \begin{cases} \dfrac{1}{2^{n+1}}(|0, i, j\rangle + |1\rangle \otimes U_n |i, j\rangle) & \text{if } t = 0 \\ \dfrac{1}{2^{n+1}}(|1, i, j\rangle + |0\rangle \otimes U_n^{\dagger} |i, j\rangle) & \text{if } t = 1. \end{cases} \quad (4.4)$$

This also justifies our choice of the pure state used in the numerical calculations in the previous section.

Let us consider now the reduced density matrix

$$\sigma_{\vec{\alpha}}^B \equiv \mathrm{Tr}_A[|\psi_{\vec{\alpha}}\rangle\langle\psi_{\vec{\alpha}}|] = \frac{1}{2^{n+1}}(|j\rangle\langle j| + \mathrm{Tr}_A[U_n |i, j\rangle\langle i, j| U_n^{\dagger}]) \quad (4.5)$$

for $t = 0$ (for $t = 1$, U_n and $U_n^{\dagger}$ need to be exchanged). For a unitary matrix U_n randomly chosen according to the Haar measure on $\mathrm{U}(n)$, $U_n |i, j\rangle$ is a random pure state on $A \otimes B$. Here and henceforth A is the space of the first n_A qubits without the top qubit. It follows from [13] that the operator

$$Q = \mathrm{Tr}_A[U_n |i, j\rangle\langle i, j| U_n^{\dagger}] \quad (4.6)$$

has rank d_A. Therefore the rank of $\sigma_{\vec{\alpha}}^B$ (equivalently, the Schmidt rank χ of $|\psi_{\vec{\alpha}}\rangle$) is at least 2^{n_0}. From Eq. (3.1) we conclude that the Schmidt rank of ρ satisfies $\chi^{\sharp} \geqslant 2^{n_0} \geqslant 2^{n/5}$. We can now collate these results into the following theorem.

Theorem 1. Let U_n be an n-qubit unitary transformation chosen randomly according to the Haar measure on $\mathrm{U}(2^n)$, and let $A:B$ denote a bipartition of $n+1$ qubits into n_A and n_B qubits, where $n_0 \equiv \min(n_A, n_B)$. Then $n/5 \leqslant n_0 \leqslant 2n/5$, and the Schmidt decomposition of ρ in Eq. (2.2) according to bipartition $A:B$ satisfies $\chi^{\sharp} \geqslant 2^{n/5}$.

We have seen that we cannot efficiently simulate DQC1 with an algorithm that relies on having a TTN for ρ with low rank q. However, in order to make this result robust, we need to also show that ρ cannot be well approximated by another $\tilde{\rho}$ accepting an efficient TTN. We do this in the Appendix.

V. CONCLUSIONS

The results in this paper show that the algorithms of [2–4] are unable to efficiently simulate a DQC1 circuit. The efficiency of a quantum simulation using these algorithms relies on the possibility of efficiently decomposing the state ρ of the quantum computer using a TTN. We have seen that for the final state of the DQC1 circuit no efficient TTN exists.

It is also interesting to note that the numerics and Theorems 1 and 2 in this paper can be generalized for any fixed polarization τ $(0<\tau\leqslant 1)$ of the initial state $\tau|0\rangle\langle 0|+(1-\tau)\mathbb{I}/2$ of the top qubit of the circuit in Eq. (2.1), implying that the algorithms of [2–4] are also unable to efficiently simulate the power of even the tiniest fraction of a qubit.

ACKNOWLEDGMENTS

A.D. acknowledges the U.S. Army Research Office for support via Contract No. W911NF-4-1-0242 and support from the University of Queensland, where this work was initiated. G.V. thanks the Australian Research Council for support.

APPENDIX: DISTRIBUTION OF THE SCHMIDT COEFFICIENTS

In this appendix we explore the robustness of the statement of Theorem 1. To this end, we consider the Schmidt rank $\tilde{\chi}^{\#}$ for a density matrix $\tilde{\rho}$ that approximates ρ according to a fidelity $F(O_1,O_2)$ defined in terms of the natural inner product on the space of linear operators,

$$F(O_1,O_2)\equiv \mathrm{Tr}(O_1^{\dagger}O_2)/\sqrt{\mathrm{Tr}(O_1^{\dagger}O_1)}\sqrt{\mathrm{Tr}(O_2^{\dagger}O_2)},$$

where $F=1$ if and only if $O_1=O_2$, and $F=|\langle\psi_1|\psi_2\rangle|^2$ for projectors $O_i=P_{\psi_i}$ on pure states $|\psi_i\rangle$. We will show that, if $\tilde{\rho}$ is close to ρ, then $\tilde{\chi}^{\#}$ for a bipartition as in Theorem 1 is also exponential. To prove this, we will require a few lemmas which we now present.

Lemma 1. Let $|\Psi\rangle$ be a bipartite vector with χ terms in its Schmidt decomposition,

$$|\Psi\rangle = N_{\Psi}\sum_{i=1}^{\chi}\lambda_i|i_A\rangle|i_B\rangle,\quad \lambda_i\geqslant\lambda_{i+1}\geqslant 0,\quad \sum_{i=1}^{\chi}\lambda_i^2=1,$$

where $N_{\Psi}\equiv\sqrt{\langle\Psi|\Psi\rangle}$, and let $|\Phi\rangle$ be a bipartite vector with norm N_{Φ} and Schmidt rank χ', where $\chi'\leqslant\chi$. Then,

$$\max_{|\Phi\rangle}|\langle\Psi|\Phi\rangle| = N_{\Psi}N_{\Phi}\sqrt{\sum_{i=1}^{\chi'}\lambda_i^2}. \qquad \text{(A1)}$$

Proof. Let μ_i denote the Schmidt coefficients of $|\Phi\rangle$. It follows from Lemma 1 in [12] that $\max_{|\Phi\rangle}|\langle\Psi|\Phi\rangle| =N_{\Psi}N_{\Phi}\Sigma_{i=1}^{\chi'}\lambda_i\mu_i$, and the maximization over μ_i is done next. A straightforward application of the method of Lagrange multipliers provides us with $\mu_i=c\lambda_i$, $i=1,2,\ldots,\chi'$, for some constant c. Since $\Sigma_{i=1}^{\chi'}\mu_i^2=1=c^2\,\Sigma_{i=1}^{\chi'}\lambda_i^2$, $c=1/\sqrt{\Sigma_{i=1}^{\chi'}\lambda_i^2}$. Thus,

$$\max_{|\Phi\rangle}|\langle\Psi|\Phi\rangle| = cN_{\Psi}N_{\Phi}\sum_{i=1}^{\chi'}\lambda_i^2$$

and the result follows. ■

We will also use two basic results related to majorization theory. Recall that, by definition, a decreasingly ordered probability distribution $\vec{p}=(p_1,p_2,\ldots,p_d)$, where $p_{\alpha}\geqslant p_{\alpha+1}\geqslant 0$, $\Sigma_{\alpha}p_{\alpha}=1$, is *majorized* by another such probability distribution $\vec{q}$, denoted $\vec{p}\prec\vec{q}$, if $\vec{q}$ is more ordered or concentrated than $\vec{p}$ (equivalently, $\vec{p}$ is flatter or more mixed than $\vec{q}$) in the sense that the following inequalities are satisfied:

$$\sum_{\alpha=1}^{k}p_{\alpha}\leqslant\sum_{\alpha=1}^{k}q_{\alpha}\quad\forall\ k=1,\ldots,d, \qquad \text{(A2)}$$

with equality for $k=d$. The following result can be found in Exercise II.1.15 of [14].

Lemma 2. Let $\rho_{\vec{x}}$ and $\rho_{\vec{y}}$ be density matrices with eigenvalues given by probability distributions $\vec{x}$ and $\vec{y}$. Let $\sigma(M)$ denote the decreasingly ordered eigenvalues of Hermitian operator M. Then

$$\sigma(\rho_{\vec{x}}+\rho_{\vec{y}})\prec\vec{x}+\vec{y}.$$

The next result follows by direct inspection.

Lemma 3. Let coefficients δ_i, $1\leqslant i\leqslant d$, be such that $-\delta\leqslant\delta_i\leqslant\delta$ for some positive $\delta\leqslant 1$ and $\Sigma_i\delta_i=1$, and consider the probability distribution $\vec{p}(\{\delta_i\})$,

$$\vec{p}(\{\delta_i\})\equiv\left(\frac{1}{2}+\frac{1+\delta_1}{2d},\frac{1+\delta_2}{2d},\ldots,\frac{1+\delta_d}{2d}\right).$$

Then

$$\vec{p}(\{\delta_i\})\prec\vec{p}(\{\delta_i^*\}),$$

where

$$\delta_i^*\equiv\begin{cases}\delta, & i\leqslant d/2\\ -\delta, & i>d/2,\end{cases}$$

and we assume d to be even.

Finally, we need a result from [13].

Lemma 4. With probability very close to 1,

$$\begin{aligned}\mathrm{Pr}\left((1-\delta)\frac{\Upsilon}{d_A}\leqslant Q\leqslant(1+\delta)\frac{\Upsilon}{d_A}\right)\\ \geqslant 1-\left(\frac{10d_A}{\delta}\right)^{2d_A}2^{(-d_B\delta^2/14\ \ln 2)}\\ \geqslant 1-O\left(\frac{1}{\exp[\delta^2\exp(n)]}\right),\end{aligned} \qquad \text{(A3)}$$

where $d_A=2^{n_A}=2^{n_0}$ and $d_B=2^{n_B}=2^{n-n_0+1}$, and the operator Q defined in Eq. (4.6) is within a ball of radius δ of a (unnormalized) projector Υ/d_A of rank d_A [provided d_B is a large multiple of $d_A\log d_A/\delta^2$ [13], which is satisfied for large n, given that $n/5\leqslant n_0\leqslant 2n/5$).

Our second theorem uses the fact that not only does the Schmidt decomposition of ρ have exponentially many coefficients, but these are roughly of the same size.

Theorem 2. Let ρ, U_n, and $A:B$ be defined as in Theorem

1. If $F(\rho,\tilde{\rho})\geqslant 1-\epsilon$, then with probability $p(\delta,n)=1-O(\exp[-\delta^2\exp(n)])$, the Schmidt rank for $\tilde{\rho}$ according to the bipartition $A:B$ satisfies $\tilde{\chi}^{\#}\geqslant(1-4\epsilon-\delta)2^{n/5}$.

Proof. For any product vector of Eq. (4.3) we have

$$|\langle tij|\rho\tilde{\rho}|tij\rangle| \leqslant N_{\vec{\alpha}}\tilde{N}_{\vec{\alpha}}\sqrt{\sum_{k=1}^{\tilde{\chi}^{\#}}(\lambda_k^{ij})^2} \leqslant N_{\vec{\alpha}}\tilde{N}_{\vec{\alpha}}g(\tilde{\chi}^{\#}/d_A), \tag{A4}$$

where

$$g(x)\equiv\sqrt{\frac{1+(1+\delta)x}{2}} \tag{A5}$$

and $N_{\vec{\alpha}}\equiv\sqrt{\langle tij|\rho^2|tij\rangle}$, $\tilde{N}_{\vec{\alpha}}\equiv\sqrt{\langle tij|\tilde{\rho}^2|tij\rangle}$. The first inequality in (A4) follows from Lemma 1, whereas the second one follows from the fact that the spectrum $\vec{p}$ of

$$\rho_B\equiv(N_{\vec{\alpha}})^{-2}\mathrm{Tr}_A[\rho|tij\rangle\langle tij|\rho]=\frac{1}{2}(|j\rangle\langle j|+Q),$$

where Q has all its d_A nonzero eigenvalues q_i in the interval $2^{-n_0}(1-\delta)\leqslant q_i\leqslant 2^{-n_0}(1+\delta)$, is majorized by $\vec{p}(\{\delta_i^{\#}\})$, as follows from Lemmas 2 and 3. Then,

$$1-\epsilon\leqslant\frac{\mathrm{Tr}\rho\tilde{\rho}}{\sqrt{\mathrm{Tr}\rho^2}\sqrt{\mathrm{Tr}\tilde{\rho}^2}}=\frac{\sum_{\vec{\alpha}}\langle\vec{\alpha}|\rho\tilde{\rho}|\vec{\alpha}\rangle}{\sqrt{\sum_{\vec{\alpha}}\langle\vec{\alpha}'|\rho^2|\vec{\alpha}'\rangle\sum_{\vec{\alpha}}\langle\vec{\alpha}''|\tilde{\rho}^2|\vec{\alpha}''\rangle}}$$

$$\leqslant g(\tilde{\chi}^{\#}/d_A)\frac{\sum_{\vec{\alpha}}N_{\vec{\alpha}}\tilde{N}_{\vec{\alpha}}}{\sqrt{\sum_{\vec{\alpha}}(N_{\vec{\alpha}'})^2\sum_{\vec{\alpha}''}(\tilde{N}_{\vec{\alpha}''})^2}}\leqslant g(\tilde{\chi}^{\#}/d_A),$$

where in the last step we have used the Cauchy-Schwarz inequality $|\langle x|y\rangle|\leqslant\sqrt{\langle x|x\rangle}\sqrt{\langle y|y\rangle}$. The result of the theorem follows from $g(\tilde{\chi}^{\#}/2^{n_0})\geqslant 1-\epsilon$. ■

---

[1] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, 1994*, edited by S. Goldwasser (IEEE Computer Science Press, Los Alamitos, CA, 1994), p. 124.

[2] R. Jozsa and N. Linden, Proc. R. Soc. London, Ser. A **459**, 2011 (2003).

[3] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).

[4] Y.-Y. Shi, L.-M. Duan, and G. Vidal, Phys. Rev. A **74**, 022320 (2006); M. Van den Nest, W. Dür, G. Vidal, and H. J. Briegel, *ibid.* **75**, 012337 (2006).

[5] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[6] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).

[7] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).

[8] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, Phys. Rev. Lett. **92**, 177906 (2004); J. Emerson, S. Lloyd, D. Poulin, and D. Cory, Phys. Rev. A **69**, 050305(R) (2004).

[9] M. Zwolak and G. Vidal, Phys. Rev. Lett. **93**, 207205 (2004).

[10] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).

[11] J. Emerson, E. Livine, and S. Lloyd, Phys. Rev. A **72**, 060302 (2005).

[12] G. Vidal, D. Jonathan, and M. A. Nielsen, Phys. Rev. A **62**, 012304 (2000).

[13] P. Hayden, D. W. Leung, and A. Winter, Commun. Math. Phys. **265**, 95 (2006).

[14] Rajendra Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).