PHYSICAL REVIEW A **68**, 052311 (2003)

Lower bounds on the complexity of simulating quantum gates

Andrew M. Childs,[1,*] Henry L. Haselgrove,[2,3,†] and Michael A. Nielsen[2,4,5,‡]

[1]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

[2]*School of Physical Sciences, The University of Queensland, Brisbane QLD 4072, Australia*

[3]*Information Sciences Laboratory, Defence Science and Technology Organisation, Edinburgh 5111, Australia*

[4]*School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane QLD 4072, Australia*

[5]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA*

(Received 4 August 2003; published 18 November 2003)

We give a simple proof of a formula for the minimal time required to simulate a two-qubit unitary operation using a fixed two-qubit Hamiltonian together with fast local unitaries. We also note that a related lower bound holds for arbitrary n-qubit gates.

DOI: 10.1103/PhysRevA.68.052311

PACS number(s): 03.67.−a

I. INTRODUCTION

Understanding quantum dynamics is at the heart of quantum physics. Recent ideas from quantum computation have stimulated interest in studying the physical resources needed to implement quantum operations. In addition to a qualitative understanding of what resources are necessary, we would like to quantify the resource requirements for universal quantum computation and other information processing tasks. Ultimately, we would like to understand the minimal resources that are necessary and sufficient to implement particular quantum dynamics.

As a first step towards answering these questions, it has been shown that there is a sense in which all entangling dynamics are qualitatively equivalent. In particular, it has been shown that any n-qudit two-body Hamiltonian capable of creating entanglement between any pair of qudits is, in principle, universal for quantum computation, when assisted by arbitrary single-qudit unitaries [1–8]. Thus, any particular entangling two-qudit Hamiltonian can be used to simulate any other, provided local unitaries are available. This suggests that such dynamics are a fungible physical resource.

Having established the qualitative equivalence of all entangling dynamics, we would like to quantify their information processing power. In particular, it is interesting to consider the minimal time required to implement a unitary operation U on a two-qubit system, using a fixed Hamiltonian H and the ability to intersperse fast local unitary operations on the two qubits. This problem was studied by Khaneja, Brockett, and Glaser [9], who found a solution using the theory of Lie groups. Their results, although giving a solution in principle, are neither explicit about the form of the minimal time, nor do they explain how to construct all elements of the time-optimal simulation. Further work by Vidal, Hammerer, and Cirac [10], from a different point of view, resulted in an explicit formula for the minimal time, and gave a constructive procedure for minimizing that time (see also Ref. [11], where an alternate proof is given by the same authors).

The purpose of the present paper is to give a simplified proof that the formula of Vidal, Hammerer, and Cirac is, in fact, a lower bound on the simulation time. Note that the difficult part of Refs. [10], [11] was proving the lower bound; finding a protocol to meet the lower bound was comparatively easy.

The main advantages of our proof are its simplicity and conceptual clarity, as compared to the ingenious, but rather complex, arguments in Refs. [9–11]. This simplicity is achieved by making use of a powerful result from linear algebra, Thompson's theorem. We expect that Thompson's theorem might be useful for many other problems in quantum information theory. A second advantage of using Thompson's theorem is that it does not rely on special properties of two-qubit unitary operators. Therefore, essentially the same arguments give a lower bound on the time required to implement an n-qubit unitary operation using a fixed n-qubit interaction Hamiltonian, and fast local unitary operations.

Our approach to the proof of the lower bound has its roots in the framework of dynamic strength measures for quantum operations [12]. The dynamic strength framework is an attempt to develop a quantitative theory of the power of dynamical operations for information processing. The idea is to associate with a quantum dynamical operation, such as a unitary operation U, a quantitative measure of its "strength." In Ref. [12] it was shown that such strength measures can be used to analyze the minimal time required for the implementation of a quantum operation. The present paper takes a similar approach, but instead of using a single real number to quantify dynamic strength, we use a vector-valued measure. This can also be compared to the analysis of optimal simulation of Hamiltonian dynamics using a set of several strength measures [13].

Our paper is structured as follows. Section II reviews some background material on majorization, Thompson's theorem, and the structure of the two-qubit unitary matrices. The main result, the lower bound on optimal simulation, is proved in Sec. III. We conclude in Sec. IV by presenting our generalization of the lower bound to n qubits and suggesting some directions for future work. In addition, an appendix

[*] Electronic address: amchilds@mit.edu

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

[‡] Electronic address: nielsen@physics.uq.edu.au; www.qinfo.org/people/nielsen

gives a procedure for calculating a canonical decomposition of two-qubit unitary gates.

II. BACKGROUND

This section reviews the relevant background needed for our proof. Section II A reviews the basic notions of majorization, introduces Thompson's theorem, and explains how to use Thompson's theorem and majorization to relate properties of a product of unitary operators to properties of the individual unitaries. Section II B introduces the canonical decomposition, a useful representation theorem for two-qubit unitary operators, and Section II C presents an analogous decomposition for Hamiltonians.

A. Majorization and Thompson's theorem

Our analysis uses the theory of majorization together with Thompson's theorem. More detailed introductions to majorization may be found in Ref. [14], Chaps. 2 and 3 of Ref. [15], and in Refs. [16], [17].

Suppose $x=(x_1,\ldots,x_D)$ and $y=(y_1,\ldots,y_D)$ are two D-dimensional real vectors. The relation x is majorized by y, written $x\prec y$, is intended to capture the intuitive notion that x is less ordered (i.e., more disordered) than y. To make the formal definition we introduce the notation ↓ to denote the components of a vector rearranged into nonincreasing order, so $x^{\downarrow}=(x_1^{\downarrow},\ldots,x_D^{\downarrow})$, where $x_1^{\downarrow}\geqslant x_2^{\downarrow}\geqslant\cdots\geqslant x_D^{\downarrow}$. Then x is majorized by y, that is, $x\prec y$, if

$$\sum_{j=1}^{k} x_j^{\downarrow}\leqslant\sum_{j=1}^{k} y_j^{\downarrow} \tag{1}$$

for $k=1,...,D-1$, and the inequality holds with equality when $k=D$.

To connect majorization to Hamiltonian simulation, we use a result of Thompson relating a product of two unitary operators to the individual unitary operators. Recall that an arbitrary pair of unitary operators can be written in the form e^{iH} and e^{iK}, for some Hermitian H and K. Thompson's theorem provides a representation for the product $e^{iH}e^{iK}$ in terms of H and K.

Theorem 1 (Thompson [18]). Let H, K be Hermitian matrices. Then there exist unitary matrices U, V such that

$$e^{iH}e^{iK}=e^{i(UHU^{\dagger}+VKV^{\dagger})}. \tag{2}$$

The proof of Thompson's theorem in Ref. [18] depends on a result conjectured earlier by Horn [19]. A proof of this conjecture had been announced and outlined by Lidskii [20] at the time of Thompson's paper. However, remarks in Ref. [18] suggest that Ref. [20] did not contain enough detail to be considered a fully rigorous proof. Fortunately, a proof of Horn's conjecture has recently been fully completed and published. See, for example, Refs. [21], [22] for reviews and references.

Thompson's theorem may be related to majorization using the following theorem of Ky Fan.

Theorem 2 (Ky Fan [15,23]). Let H, K be Hermitian matrices. Then $\lambda(H+K)\prec\lambda(H)+\lambda(K)$, where $\lambda(A)$ denotes the vector whose entries are the eigenvalues of the Hermitian matrix A, arranged into nonincreasing order.

Combining the results of Ky Fan and Thompson, we have the following.

Corollary 3. Let H, K be Hermitian matrices. Then there exists a Hermitian matrix L such that

$$e^{iH}e^{iK}=e^{iL};\quad \lambda(L)\prec\lambda(H)+\lambda(K). \tag{3}$$

We will not apply this corollary directly, but we have included it here because it captures the spirit of our later argument, combining the Thompson and Ky Fan theorems to relate the properties of a product of unitaries to the individual unitaries themselves. Corollary 3 can be regarded as a vector-valued analog of the chaining property for dynamic strength measures used in Ref. [12] to establish lower bounds on computational complexity.

B. The canonical decomposition of a two-qubit gate

The *canonical decomposition* is a useful representation theorem characterizing the nonlocal properties of a two-qubit unitary operator. It was proved by Khaneja, Brockett, and Glaser [9] using ideas from Lie theory. Kraus and Cirac [24] have given a constructive proof using elementary notions, while Zhang *et al.* [25] have discussed the decomposition in detail from the point of view of Lie theory. The decomposition states that any two-qubit unitary U may be written in the form

$$U=(A_1\otimes B_1)e^{i(\theta_x X\otimes X+\theta_y Y\otimes Y+\theta_z Z\otimes Z)}(A_2\otimes B_2), \tag{4}$$

where A_1, A_2, B_1, B_2 are single-qubit unitaries, and the three parameters θ_x, θ_y, and θ_z characterize the nonlocal properties of U.[1] Without loss of generality, we may choose the local unitaries to ensure that

$$\frac{\pi}{4}\geqslant\theta_x\geqslant\theta_y\geqslant|\theta_z|, \tag{5}$$

and we refer to the set of parameters chosen in this way as the *canonical parameters* for U. We will see below that these parameters are unique. We define the *canonical form* of U to be

$$U_c:=(A_1^{\dagger}\otimes B_1^{\dagger})U(A_2^{\dagger}\otimes B_2^{\dagger}), \tag{6}$$

up to local unitaries, U_c is equivalent to U. It will be convenient to assume through the remainder of this section that U has unit determinant. This is equivalent to requiring that A_1, A_2, B_1, B_2 can all be chosen to have unit determinant.

The canonical parameters turn out to be crucial to results about simulation of two-qubit gates. If

$$U_c=e^{i(\theta_x X\otimes X+\theta_y Y\otimes Y+\theta_z Z\otimes Z)} \tag{7}$$

[1] Prior to Ref. [9], Makhlin [26] gave a proof that the nonlocal properties of U are completely characterized by θ_x, θ_y, and θ_z, but did not write down the canonical decomposition explicitly.

is the canonical form of U, then we define the *nonlocal content* $\phi(U)$ of U by $\phi(U) := \lambda(H_U)$, where

$$H_U := \theta_x X\otimes X + \theta_y Y\otimes Y + \theta_z Z\otimes Z. \tag{8}$$

Explicitly, the components of $\phi(U)$ are

$$\phi_1 = \theta_x + \theta_y - \theta_z, \tag{9}$$

$$\phi_2 = \theta_x - \theta_y + \theta_z, \tag{10}$$

$$\phi_3 = -\theta_x + \theta_y + \theta_z, \tag{11}$$

$$\phi_4 = -\theta_x - \theta_y - \theta_z. \tag{12}$$

We now outline a simple procedure to determine the canonical parameters of a two-qubit unitary operator. Our explanation initially follows Refs. [11] and [27]. However, as explained below, there is an ambiguity in the procedure described in those papers, related to the fact that the logarithm function has many branches. Our procedure resolves this ambiguity.

To explain the procedure, we need to introduce a piece of notation, and explain a simple observation about single-qubit unitary matrices. The *spin flip* operation on an arbitrary two-qubit operator is defined as

$$\tilde{M} := (Y\otimes Y)M^T(Y\otimes Y), \tag{13}$$

where Y is the Pauli sigma y matrix, and the transpose operation is taken with respect to the computational basis. Note that the spin flip operation may also be written as $\tilde{M} = M^T$, where the transpose is taken with respect to a different basis, the *magic basis* [28],

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad i\frac{|00\rangle - |11\rangle}{\sqrt{2}},$$

$$i\frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{14}$$

The observation about single-qubit unitary matrices that we need is the following. Let U be any single-qubit unitary matrix with unit determinant. Then

$$UYU^T = Y, \tag{15}$$

where the transpose is taken in the computational basis. This simple identity is easily verified.

Now suppose U is an arbitrary two-qubit unitary with unit determinant. By definition of the spin flip, and substituting the canonical decomposition, we have

$$\begin{aligned} U\tilde{U} = &(A_1\otimes B_1)U_c(A_2\otimes B_2)(Y\otimes Y)\\ &\times(A_2^T\otimes B_2^T)U_c(A_1^T\otimes B_1^T)(Y\otimes Y). \end{aligned} \tag{16}$$

By the identity Eq. (15) we see that

$$U\tilde{U} = (A_1\otimes B_1)U_c(Y\otimes Y)U_c(A_1^T\otimes B_1^T)(Y\otimes Y). \tag{17}$$

Using the fact that $Y\otimes Y$ commutes with $X\otimes X$, $Y\otimes Y$, and $Z\otimes Z$, we see that $Y\otimes Y$ commutes with U_c, and thus

$$U\tilde{U} = (A_1\otimes B_1)U_c^2(Y\otimes Y)(A_1^T\otimes B_1^T)(Y\otimes Y). \tag{18}$$

Finally, applying Eq. (15) again gives

$$U\tilde{U} = (A_1\otimes B_1)U_c^2(A_1^\dagger\otimes B_1^\dagger). \tag{19}$$

Equation (19) suggests a procedure to determine the canonical parameters for U, based on the observation that

$$\lambda(U\tilde{U}) = \lambda(U_c^2) = (e^{2i\phi_1}, e^{2i\phi_2}, e^{2i\phi_3}, e^{2i\phi_4}), \tag{20}$$

where the ϕ_j are related to the canonical parameters θ_x, θ_y, and θ_z by Eqs. (9)–(12). It is tempting to conclude that one can determine θ_x, θ_y, θ_z from the eigenvalues of $U\tilde{U}$, simply by taking logarithms and inverting the resulting linear equations. Indeed, such a conclusion is reached in Refs. [11] and [27], using arguments similar to those just described. Unfortunately, determining the canonical parameters is not quite as simple as this, because $z \rightarrow e^{iz}$ is not a uniquely invertible function. In particular, $e^{iz} = e^{i(z+2\pi m)}$, where m is any integer, so there is some ambiguity about which branch of the logarithm function to use in calculating the canonical parameters. In fact, we prove later that no one branch of the logarithm function can be used. However, these considerations do allow us to reach the following conclusion.

Lemma 4. Let U be a two-qubit unitary. Then there exists a Hermitian H such that

$$U\tilde{U} = e^{2iH}, \quad \lambda(H) = \phi(U). \tag{21}$$

Moreover, if H is any Hermitian matrix such that $\lambda(U\tilde{U}) = \lambda(e^{2iH})$ then it follows that $\lambda(H) = \phi(U) + \pi\vec{m}$, where $\vec{m}$ is some vector of integers.

Although this lemma is sufficient to prove our later results, there is in fact a simple method for exactly calculating the canonical parameters. Because there are many applications of the canonical decomposition, we describe this method in the appendix. The method will not be needed elsewhere in the paper.

C. The canonical form of a two-qubit Hamiltonian

Finally, we introduce one additional concept, the *canonical form* of a two-qubit Hamiltonian H [3]. Any two-qubit Hamiltonian H can be expanded as

$$H = \sum_{j,k=0}^{3} h_{jk}\sigma_j\otimes\sigma_k. \tag{22}$$

Then let

$$H' := \frac{H+\tilde{H}}{2} = \sum_{j,k\neq 0} h_{jk}\sigma_j\otimes\sigma_k. \tag{23}$$

That is, H' is just the Hamiltonian that results when the local terms in H are removed. It is not difficult to show that H and H' are interchangeable resources for simulation in the sense that, given fast local unitaries, evolution according to H for a time t can be simulated by evolution according to H_c for a time t, and vice versa. Furthermore, by doing appropriate local unitaries, it can be shown [3] that simulating H' (and thus H) is equivalent to simulating the canonical form of H,

$$H_c = h_x X\otimes X + h_y Y\otimes Y + h_z Z\otimes Z, \tag{24}$$

where $h_x \geqslant h_y \geqslant |h_z|$. Once again, H and H_c are interchangeable resources for simulation.

Note that the three parameters h_x, h_y, h_z are completely characterized by the three degrees of freedom in $\lambda(H_c) = \lambda(H+\tilde{H})/2$, just as the three canonical parameters θ_x, θ_y, θ_z are completely characterized by the three degrees of freedom in $\lambda(U_c^2) = \lambda(U\tilde{U})$.

III. SIMULATION OF TWO-QUBIT GATES

We now return to the main purpose of the paper, proving results about the time to simulate a unitary gate using entangling Hamiltonians and fast local gates. We aim to prove the following result.

Theorem 5 (Vidal, Hammerer, Cirac [10,11], cf. Khaneja, Brockett, and Glaser [9]). Let U be a two-qubit unitary operator, and let H be a two-qubit entangling Hamiltonian. Then the minimal time required to simulate U using H and fast local unitaries is the minimal value of t such that there exists a vector of integers $\vec{m}$ satisfying

$$\phi(U) + \pi\vec{m} \prec \frac{\lambda(H+\tilde{H})}{2} t. \tag{25}$$

Note further that only two vectors of integers need to be checked, $\vec{m} = (0,0,0,0)$ and $\vec{m} = (1,1,-1,-1)$, since all the other possibilities give rise to weaker constraints on the minimal time t [10,11]. The difficult part of the proof of theorem 5 is the proof that Eq. (25) is a lower bound on the simulation time t and it is this part of the proof that we focus on simplifying. The proof that this lower bound may be achieved follows from standard results on majorization, and we refer the interested reader to Refs. [10], [11] for details.

To prove that Eq. (25) constrains the minimal time for simulation, we begin by characterizing the canonical decomposition of a product of unitary matrices. Let $\Lambda(U) \coloneqq \lambda(U\tilde{U})$, and define the equivalence relation $A \sim B$ for Hermitian matrices A and B if $\lambda(A) = \lambda(B)$. Then we have the following.

Lemma 6. Let U_j be unitary matrices, and let H_j be Hermitian matrices such that $U_j\tilde{U}_j = e^{2iH_j}$. Then there exist Hermitian matrices K_j such that $H_j \sim K_j$, and

$$\Lambda(U_N \cdots U_1) = \lambda(e^{2i(K_1+\cdots+K_N)}). \tag{26}$$

Proof. We induct on N. The result is trivial for $N=1$, so we need only consider the inductive step. Using the fact $\lambda(AB) = \lambda(BA)$, we have

$$\Lambda(U_{N+1}\cdots U_1) = \lambda(\tilde{U}_{N+1}U_{N+1}U_N\cdots U_1\tilde{U}_1\cdots\tilde{U}_N). \tag{27}$$

By the inductive hypothesis there exist Hermitian K_j' such that $H_j \sim K_j'$ and

$$\lambda(U_N\cdots U_1\tilde{U}_1\cdots\tilde{U}_N) = \lambda(e^{2i(K_1'+\cdots+K_N')}). \tag{28}$$

Therefore, $U_N\cdots U_1\tilde{U}_1\cdots\tilde{U}_N = e^{2i(K_1''+\cdots+K_N'')}$, for some $K_j'' \sim H_j$. Observe also that

$$\tilde{U}_{N+1}U_{N+1} \sim U_{N+1}\tilde{U}_{N+1} = e^{2iH_{N+1}}, \tag{29}$$

and thus $\tilde{U}_{N+1}U_{N+1} = e^{2iK_{N+1}''}$ for some $K_{N+1}'' \sim H_{N+1}$. It follows by substitution that

$$\Lambda(U_{N+1}\cdots U_1) = \lambda(e^{2iK_{N+1}''}e^{2i(K_1''+\cdots+K_N'')}). \tag{30}$$

Applying Thompson's theorem gives

$$\Lambda(U_{N+1}\cdots U_1) = \lambda(e^{2i(K_1+\cdots+K_{N+1})}) \tag{31}$$

for some $K_j \sim K_j'' \sim H_j$, which completes the inductive step of the proof. ■

Given this result, it is straightforward to complete the proof of Eq. (25).

Proof. Write U in the form

$$U = e^{-iHt_1}V_1e^{-iHt_2}V_2\ldots V_{k-1}e^{-iHt_k}, \tag{32}$$

where $t_1,\ldots,t_k$ are times of evolution, $t = t_1+\cdots+t_k$ is the total time for simulation, and V_j are local unitaries. Without loss of generality, we may assume H is in canonical form. Applying lemma 6, we obtain

$$\Lambda(U) = \lambda(e^{2i(H_1t_1+\cdots+H_kt_k)}), \tag{33}$$

where $H_j \sim H$ for each j. Here we have used the observation $V_j\tilde{V}_j = 1$, so all the contributions from local unitaries vanish. It follows from lemma 4 that

$$\phi(U) + \pi\vec{m} = \lambda(H_1t_1+\cdots+H_mt_m), \tag{34}$$

and using Ky Fan's theorem gives

$$\phi(U) + \pi\vec{m} \prec \lambda(H)(t_1+\cdots+t_m), \tag{35}$$

which is Eq. (25), as desired. ■

IV. DISCUSSION

In this paper, we have provided a simplified proof of a lower bound on the time required to simulate a two-qubit unitary gate using a given two-qubit interaction Hamiltonian and local unitaries. The bound follows easily from standard results on majorization together with Thompson's theorem on products of unitary operators.

Although we have described canonical decompositions of two-qubit gates in some detail, we note that our proof does not actually require properties of the decomposition unique to two qubits. In fact, it is straightforward to prove an analog of Eq. (25) for an n-qubit system. For an n-qubit operator M, suppose we define a generalized spin flip $M \rightarrow \tilde{M}$ as some antihomomorphism ($\widetilde{M_1M_2} = \tilde{M}_2\tilde{M}_1$) on the group of $n\times n$

unitary matrices, such that $M\tilde{M}=I$ whenever M is local. For example, the generalized spin flip could be the transpose operation in a basis such that, whenever M is local, M is orthogonal, i.e., $M\tilde{M}=I$. It is not difficult to construct examples of such bases, at least when n is even. An example is the basis obtained by rotating the computational basis using the transformation $(I-iY^{\otimes n})/\sqrt{2}$, for n even. This basis change gives $\tilde{M}=Y^{\otimes n}M^{T}Y^{\otimes n}$, where the transpose is taken in the computational basis, and thus this operation generalizes the transpose in the magic basis.

In this general setting the following lower bound on the time required to implement an n-qubit gate holds.

Corollary 7. Let U be an n-qubit unitary operator, and let H be an n-qubit Hamiltonian. Then the time required to simulate U using H and fast local unitaries satisfies

$$\frac{1}{2}\arg\lambda(U\tilde{U})+\pi\vec{m}\prec\frac{\lambda(H+\tilde{H})}{2}t. \tag{36}$$

for some vector of integers $\vec{m}$.

The proof follows simply by taking the arguments of both sides of Eq. (33) and applying Ky Fan's theorem. All steps leading up to Eq. (33) remain valid for n-qubit systems using the above definition of the generalized spin flip.

Unfortunately, we have not found any interesting examples with $n>2$ for which Eq. (36) provides a nontrivial lower bound on the time required to implement some quantum gate. It would be interesting to construct cases where Eq. (36) (or some similar condition) does give a nontrivial constraint on multipartite gate simulation. One might imagine that such techniques could be used to prove circuit lower bounds on certain quantum computations, although it does not seem likely that such bounds would be especially strong, given the well-known difficulty of this problem.

ACKNOWLEDGMENTS

We thank Aram Harrow and Tobias Osborne for helpful discussions, and Andrew Doherty for an informative seminar on related problems. A.M.C. received support from the Fannie and John Hertz Foundation, and thanks the University of Queensland node of the Center for Quantum Computer Technology for its hospitality. A.M.C. was also supported in part by the Cambridge-MIT Institute, by the Department of Energy under cooperative research agreement No. DE-FC02-94ER40818, and by the National Security Agency and Advanced Research and Development Activity under Army Research Office Contract No. DAAD19-01-1-0656. Finally, we acknowledge the hospitality of the Caltech Institute for Quantum Information, where this work was completed. This work was supported in part by the National Science Foundation under Grant No. EIA-0086038.

APPENDIX: A METHOD FOR COMPUTING THE CANONICAL PARAMETERS OF A TWO-QUBIT UNITARY GATE

In this appendix, we describe a method for computing the canonical parameters of a two-qubit unitary, based on the discussion in Sec. II B. The key is to take logarithms in just the right way. From Eqs. (5) and (9)–(12), we see that

$$\frac{3\pi}{2}\geqslant 2\phi_1\geqslant 2\phi_2\geqslant 2\phi_3\geqslant 2\phi_4\geqslant -\frac{3\pi}{2}. \tag{A1}$$

It is not difficult to find examples where the first or last inequality is saturated, so no single fixed branch of the logarithm function can be used to determine the ϕ_j. One might hope instead that there exists a method for choosing a different branch for each particular U, so that the corresponding $2\phi_j$ lie within that branch. However, even this is not possible in general. To understand this, note that

$$2\phi_1-2\phi_4=4(\theta_x+\theta_y). \tag{A2}$$

In cases where $\theta_x=\theta_y=\pi/4$, we have $2\phi_1-2\phi_4=2\pi$, in which case the values $2\phi_j$ do not lie in *any* one branch.

We now show how to compute the ϕ_j. The idea is that we can first take the argument of the eigenvalues in Eq. (20) over some fixed branch. Then we can systematically determine which of the resulting values have been shifted by 2π from the value $2\phi_j$ (due to an incorrect branch) and correct these values accordingly.

Let S_j, $j=1,...,4$ be defined as

$$2S_j=\arg(e^{2i\phi_j}). \tag{A3}$$

That is, $2S_j$ are the arguments of the eigenvalues of $U\tilde{U}$, where we take the argument over the branch $(-\pi/2,\,3\pi/2]$, so that the S_j are contained in the interval $(-\pi/4,\,3\pi/4]$. Considering the range of values that ϕ_j may take, from Eq. (A1), and the particular branch we are using, it is clear that

$$S_j=\begin{cases}\phi_j+\phi & \text{if } \phi_j\leqslant-\dfrac{\pi}{4},\\ \phi_j & \text{otherwise.}\end{cases} \tag{A4}$$

From Eqs. (9)–(12) we have

$$\phi_1+\phi_2+\phi_3+\phi_4=0. \tag{A5}$$

Combining Eqs. (A4) and (A5), we see that

$$S_1+S_2+S_3+S_4=\pi n, \tag{A6}$$

where n is the number of ϕ_j that are less than or equal to $-\pi/4$. Possible values for n are 0, 1, 2, and 3 [all four ϕ_j cannot simultaneously be $\leqslant-\pi/4$, since that would contradict Eq. (A5)]. Since the ϕ_j obey the ordering in Eq. (A1), then the n values of ϕ_j that are less than or equal to $-\pi/4$ are $\phi_4,\ldots,\phi_{4-n+1}$, and the remaining $4-n$ values greater than $\pi/4$ are $\phi_1,\ldots,\phi_{4-n}$. Thus, using Eq. (A4), we see that the set of values S_j consist of n "shifted" ϕ_j values

$$\phi_4+\pi,\ldots,\phi_{4-n+1}+\pi, \tag{A7}$$

and $4-n$ "nonshifted" values of ϕ_j

$$\phi_1,\ldots,\phi_{4-n}. \tag{A8}$$

Furthermore, all of the shifted values in Eq. (A7) are no less than any of the nonshifted values in Eq. (A8). This is shown by combining Eq. (5) with Eq. (A2), giving $\phi_1-\phi_4\leqslant\pi$, which when combined with Eq. (A1) implies that $\phi_j\leqslant\phi_k+\pi$ for all *j*, *k*, as required. Therefore, the largest *n* values of S_j are guaranteed to be the values in Eq. (A7). Thus subtracting π from the largest *n* values of S_j, gives us $\phi_4,\ldots,\phi_{4-n+1}$, and the remaining $4-n$ values of S_j give us $\phi_1,\ldots,\phi_{4-n}$.

In summary, the nonlocal parameters θ_x, θ_y, and θ_z may be computed as follows. Find the arguments of the eigenvalues of $U\tilde{U}$ over the branch $(-\pi/2,\ 3\pi/2]$. Call these values $2S_j$. Calculate $n=(S_1+S_2+S_3+S_4)/\pi$. Replace the *n* largest values of S_j by those values minus π. The resulting values, when placed in nonincreasing order, are equal to $(\phi_1,\phi_2,\phi_3,\phi_4)$. The parameters θ_x, θ_y, and θ_z are then found by inverting Eqs. (9)–(12).

[1] J. L. Dodd, M. A. Nielsen, M. J. Bremner, and R. T. Thew, Phys. Rev. A **65**, 040301(R) (2002).

[2] P. Wocjan, D. Janzing, and T. Beth, Quantum Inf. Comput. **2**, 117 (2002).

[3] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).

[4] C. H. Bennett, J. I. Cirac, M. S. Leifer, D. W. Leung, N. Linden, S. Popescu, and G. Vidal, Phys. Rev. A **66**, 012305 (2002).

[5] G. Vidal and J. I. Cirac, Phys. Rev. A **66**, 022315 (2002).

[6] J. A. Jones and E. Knill, J. Magn. Reson. **141**, 322 (1999).

[7] D. W. Leung, I. L. Chuang, F. Yamaguchi, and Y. Yamamoto, Phys. Rev. A **61**, 042310 (2000).

[8] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).

[9] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).

[10] G. Vidal, K. Hammerer, and J. I. Cirac, Phys. Rev. Lett. **88**, 237902 (2002).

[11] K. Hammerer, G. Vidal, and J. I. Cirac, Phys. Rev. A **66**, 062321 (2002).

[12] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines, Phys. Rev. A **67**, 052301 (2003).

[13] A. M. Childs, D. W. Leung, and G. Vidal, quant-ph/0303097 (unpublished).

[14] M. A. Nielsen and G. Vidal, Quantum Inf. Comput. **1**, 76 (2001).

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

[16] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its Applications* (Academic Press, New York, 1979).

[17] P. M. Alberti and A. Uhlmann, *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing* (Dordrecht, Boston, 1982).

[18] R. C. Thompson, Linear Multilinear Algebra **19**, 187 (1986).

[19] A. Horn, Pac. J. Math. **12**, 225 (1962).

[20] B. V. Lidskii, Funct. Anal. Appl. **10**, 76 (1982).

[21] W. Fulton, Bull. Am. Math. Soc. **37**, 209 (2000).

[22] A. Knutson, Linear Algebr. Appl. **319**, 61 (2002).

[23] K. Fan, Proc. Natl. Acad. Sci. U.S.A. **35**, 131 (1949).

[24] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).

[25] J. Zhang, J. Vala, K. B. Whaley, and S. Sastry, Phys. Rev. A **67**, 042313 (2003).

[26] Y. Makhlin, Quant. Inf. Proc. **1**, 243 (2002).

[27] M. S. Leifer, L. Henderson, and N. Linden, Phys. Rev. A **67**, 012306 (2002).

[28] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).