Singlet states and the estimation of eigenstates and eigenvalues of an unknown controlled-*U* gate

Mark Hillery
Department of Physics, Hunter College of City University of New York, 695 Park Avenue, New York, New York 10021

Vladimír Bužek
Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratislava, Slovakia
and Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic
(Received 2 May 2001; published 10 September 2001)

We consider several problems that involve finding the eigenvalues and generating the eigenstates of unknown unitary gates. We first examine controlled-*U* gates that act on qubits and assume that we know the eigenvalues. It is then shown how to use singlet states to produce qubits in the eigenstates of the gate. We then remove the assumption that we know the eigenvalues and show how to both find the eigenvalues and produce qubits in the eigenstates. Finally, we look at the case where the unitary operation acts on qutrits and it has two eigenvalues of 1 and one of -1. We are able to use a singlet state to produce a qutrit in the eigenstate corresponding to the -1 eigenvalue.

DOI: 10.1103/PhysRevA.64.042303 PACS number(s): 03.67.−a

I. INTRODUCTION

A common problem, which arises in quantum mechanics, is finding the eigenvalues and eigenstates of an operator, usually the Hamiltonian. The eigenvalues are the values that the observable corresponding to the operator can assume, and the eigenstates are the states of the system in which that observable will have a definite value.

With the advent of quantum algorithms, a natural question to raise is whether there are quantum algorithms that will efficiently find the eigenvalues and eigenvectors of operators. The answer to this question is, in fact, yes. Based on earlier work by Kitaev [1], Cleve *et al.* developed an algorithm that can estimate an eigenvalue if one copy of the eigenstate is provided [2]. This algorithm was analyzed further by Abrams and Lloyd [3]. They pointed out that it is not necessary to have a copy of an eigenstate to use this procedure. One can start with an arbitrary input state, and at the end of the procedure, one will obtain an eigenvalue corresponding to an eigenstate that has a nonzero overlap with the input state. This is not a deterministic procedure; we could obtain any eigenvalue whose eigenstate has a significant overlap with the input vector. In addition, Abrams and Lloyd showed that at the output one has not only the eigenvalue, but a set of qubits that is in a state that is a good approximation to the eigenstate corresponding to the measured eigenvalue. How good this approximation is was recently investigated by Travaglione and Milburn [4].

This procedure requires that one have some knowledge about the eigenstate one is trying to generate and whose eigenvalue one is trying to find. In particular, it is necessary that the input state have a substantial overlap with the desired eigenstate. It may be possible to accomplish this if there is some information available that allows a guess for the state to be made. For example, when finding the ground-state energy of a not-too-complicated Hamiltonian, it might be possible on physical grounds to obtain a rough idea of what the ground state would look like, and this information could be used to design an appropriate input state for the eigenvalue estimation algorithm. In many cases, however, there will be little if any information to guide ones choice, with the result that the input state may have a very small or no overlap with the desired eigenstate.

Here we shall show that a different input state, a singlet state, allows one to find all eigenvalues and eigenstates of an unknown controlled-*U* gate simultaneously. We shall start with the case of a single qubit gate where we know the eigenvalues and wish to generate output qubits in the eigenstates of the gate. We shall then proceed to the case where the gate still operates on only a single qubit, but we do not know either its eigenvalues or its eigenstates. Our object then is to find the eigenvalues and produce output qubits in the eigenstates. Finally, we shall consider a controlled-*U* gate that acts on qutrits, which are three-state quantum systems, and has two eigenvalues of 1 and one eigenvalue of -1. It is possible to use a singlet state to produce a qutrit in the eigenstate corresponding to the eigenvalue -1 with a network that contains only two controlled-*U* gates. This procedure is easily generalized to *D*-dimensional quantum systems, qudits. Given a controlled-*U* gate that acts on qudits and has eigenvalues 1, which is $(D-1)$-fold degenerate, and -1, it is possible to produce a qudit in the eigenstate with eigenvalue -1 by using a network containing $D-1$ controlled-*U* gates.

II. GENERATION OF EIGENSTATES OF A CONTROLLED-*U* GATE WITH KNOWN EIGENVALUES

Consider the following problem. We are given a controlled-*U* gate which acts on single qubits and we would like to generate its eigenstates. We know that the eigenvalues of the gate are 1 and -1, but we have no information about its eigenstates. A measurement-based strategy for doing this would involve sending qubits through the gate and measuring them. For example, we could use the basis states $|0\rangle$ and $|1\rangle$ to obtain information about the matrix elements of *U* in that basis. If we send the state $|1\rangle_a|0\rangle_b$, where *a* is the

control bit and b is the target bit, through the gate, the probability that the target qubit at the output is in the state $|0\rangle_b$ can be measured. This probability is just equal to $|\langle 0|U|0\rangle|^2$. The probability that the target qubit is in the state $|1\rangle_b$ is just $|\langle 1|U|0\rangle|^2$. These measurements give us information about two of the matrix elements of U, and the fact that we know that the eigenvalues are 1 and -1 means that these are the only two we have to know. In particular, we have that

$$\langle 0|U|0\rangle = -\langle 1|U|1\rangle, \quad \langle 0|U|1\rangle = \langle 1|U|0\rangle^*. \tag{1}$$

Information about the relative phase of these matrix elements can be gained by using the input state $(|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$. The probability p_0 that the output vector is in the state $|0\rangle$ is

$$p_0 = |\langle 0|U|0\rangle + e^{i\theta}\langle 0|U|1\rangle|^2. \tag{2}$$

After sending through many qubits we would have an estimate of the matrix elements, and we could then diagonalize the matrix. This information could then be used to generate qubits in the eigenstates of U. This procedure involves many qubits and many uses of the gate. What we shall now present is a quantum strategy that will produce both eigenstates with certainty using only three qubits and requiring only one use of the gate.

Let a and b be the control and target qubits of the gate, as before. To this we add a third qubit, which we shall denote by c. We now define the following states:

$$|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle),$$
$$|\phi_s\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{3}$$

and note that the rotational invariance of the singlet state, $|\phi_s\rangle$, implies that it can also be expressed as

$$|\phi_s\rangle = \frac{1}{\sqrt{2}}(|u_+\rangle|u_-\rangle - |u_-\rangle|u_+\rangle), \tag{4}$$

where $|u_+\rangle$ is the eigenstate of U with eigenvalue 1 and $|u_-\rangle$ is the eigenstate with eigenvalue -1. More explicitly, the transformation specified by

$$V|0\rangle = |u_+\rangle, \quad V|1\rangle = |u_-\rangle \tag{5}$$

is unitary and, because $|\phi_s\rangle$ is invariant under $\mathrm{U}(2)\otimes\mathrm{U}(2)$, we have

$$(V\otimes V)|\phi_s\rangle = |\phi_s\rangle. \tag{6}$$

Because the phase of the eigenstates is arbitrary, in general Eqs. (4) and (6) will be true only up to an overall phase factor, but we shall assume that the phases of $|u_+\rangle$ and $|u_-\rangle$ are such that the phase factor is equal to one.

We now start our three-qubit system in the state

$$|\Psi_{in}\rangle_{abc} = |+x\rangle_a|\phi_s\rangle_{bc}. \tag{7}$$

After qubits a and b go through the controlled-U gate the state of the system is

$$|\Psi_{out}\rangle_{abc} = \frac{1}{2}[|0\rangle_a(|u_+\rangle_b|u_-\rangle_c - |u_-\rangle_b|u_+\rangle_c) + |1\rangle_a(|u_+\rangle_b|u_-\rangle_c + |u_-\rangle_b|u_+\rangle_c)]. \tag{8}$$

We now want to measure the a qubit in the $|\pm x\rangle$ basis. In order to see the result of doing so we can express $|\Psi_{out}\rangle_{abc}$ as

$$|\Psi_{out}\rangle_{abc} = \frac{1}{\sqrt{2}}(|+x\rangle_a|u_+\rangle_b|u_-\rangle_c - |-x\rangle_a|u_-\rangle_b|u_+\rangle_c). \tag{9}$$

This equation implies that if we measure a and get $|+x\rangle$, then qubit b is in the 1 eigenstate and qubit c is in the -1 eigenstate, while if we get $|-x\rangle$, then it is just the other way around. Therefore, with one use of the gate we have, with certainty, generated its two eigenstates.

Now let us see what happens when the eigenvalues are not ± 1 but two other complex numbers of modulus unity. We shall denote the eigenstates as $|u_1\rangle$ and $|u_2\rangle$ and the corresponding eigenvalues as as $e^{i\theta_1}$ and $e^{i\theta_1}$, respectively. We again use the same three-qubit scheme and choose the input state to be $|+x\rangle_a|\phi_s\rangle_{bc}$. The output state is now given by

$$|\Psi_{out}\rangle_{abc} = \frac{1}{\sqrt{2}}(|v_1\rangle_a|u_1\rangle_b|u_2\rangle_c - |v_2\rangle_a|u_2\rangle_b|u_1\rangle_c), \tag{10}$$

where

$$|v_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_1}|1\rangle),$$
$$|v_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_2}|1\rangle). \tag{11}$$

Note that $|v_1\rangle$ and $|v_2\rangle$ are not orthogonal, but because we assume we know the eigenvalues, these vectors are known. At this point we can apply the optimal procedure for distinguishing two nonorthogonal states [5–7]. This is a generalized measurement that can be applied when we are given a state, which is one of two known states, and we want to determine which of the two states it is. The measurement has one of three possible outcomes; it either tells us without error which of the two states we have, or it tells us that it has failed to distinguish the states. Applied to $|v_1\rangle$ and $|v_2\rangle$, the procedure would succeed with a probability of

$$1 - |\langle v_1|v_2\rangle| = 1 - \frac{1}{\sqrt{2}}[1 + \cos(\theta_1 - \theta_2)]^{1/2}. \tag{12}$$

The closer the phase difference between the eigenvalues is to π, the greater the probability of success of this procedure. If

$|v_1\rangle$ is detected at output a, then $|u_1\rangle$ is at output b and $|u_2\rangle$ at c. On the other hand, if $|v_2\rangle$ is detected at a, then $|u_2\rangle$ is at b and $|u_1\rangle$ is at c.

If one allows more than one use of the gate there are other possibilities. Suppose that we know the eigenvalues of U are 1 and i. Then the eigenvalues of U^2 are 1 and -1. We can then apply the above procedure to generate the eigenstates with one modification. The three-qubit initial state is the same, but qubits a and b pass through two controlled-U gates instead of one. Again qubit a is measured at the output in the $|\pm x\rangle$ basis. If $|+x\rangle$ is found, then the eigenstate corresponding to 1 is at output b and that corresponding to i is at output c. If $|-x\rangle$ is found, the b and c outputs are reversed.

As preparation for Sec. III, let us consider one last, harder problem. Suppose that we know that the eigenvalues are not the same, and that they are members of the set $\{1,-1,i,-i\}$. In this case we have partial rather than complete information about the eigenvalues, and we again want to generate qubits in the eigenstates. This can be done using four qubits, a controlled-U gate, and a controlled-U^2 gate. This last gate can be constructed from two controlled-U gates in sequence. Qubit a is the control bit for the controlled-U^2 gate, qubit b is the control bit for the controlled-U gate, and qubit c is the target bit for both. Let $|u_1\rangle$ and $|u_2\rangle$ be the eigenstates of U with corresponding eigenvalues z_1 and z_2, where z_1 and z_2 are members of the set $\{1,-1,i,-i\}$. The input state is

$$|\Psi_{in}\rangle_{abcd}=|+x\rangle_a|+x\rangle_b|\phi_s\rangle_{cd}=|+x\rangle_a|+x\rangle_b\left(\frac{1}{\sqrt{2}}\right)\times(|u_1\rangle_c|u_2\rangle_d-|u_2\rangle_c|u_1\rangle_d). \quad (13)$$

The output state of the network is given by

$$\begin{aligned}|\Psi_{out}\rangle_{abcd}&=G_{ac}(U^2)G_{bc}(U)|\Psi_{in}\rangle_{abcd}\\&=\frac{1}{2\sqrt{2}}[(|00\rangle_{ab}+z_1|01\rangle_{ab}+z_1^2|10\rangle_{ab}\\&\quad+z_1^3|11\rangle_{ab})|u_1\rangle_c|u_2\rangle_d-(|00\rangle_{ab}+z_2|01\rangle_{ab}\\&\quad+z_2^2|10\rangle_{ab}+z_2^3|11\rangle_{ab})|u_2\rangle_c|u_1\rangle_d],\end{aligned} \quad (14)$$

where $G_{jk}(U^n)$ is the operator corresponding to a controlled-U^n gate with control bit j and target bit k. Now consider the vector

$$|\eta(z)\rangle_{ab}=\frac{1}{2}(|00\rangle_{ab}+z|01\rangle_{ab}+z^2|10\rangle_{ab}+z^3|11\rangle_{ab}). \quad (15)$$

The vectors $|\eta(1)\rangle_{ab}$, $|\eta(-1)\rangle_{ab}$, $|\eta(i)\rangle_{ab}$, and $|\eta(-i)\rangle_{ab}$ form an orthonormal basis of the space of the two qubits a and b. If we now measure the two-qubit system ab in this basis, we can determine one of the eigenvalues of U, e.g., if the result of the measurement is $|\eta(1)\rangle_{ab}$, then one of the eigenvalues is 1. The eigenstate corresponding to this eigenvalue will emerge from output c, and the eigenstate corresponding to the other, unknown, eigenvalue will emerge from output d.

This procedure will allow us to find one of the eigenvalues, if we know that they belong to a limited set, and generate both eigenstates. A better procedure would allow us to find both eigenvalues, remove the restriction that they belong to a particular set, and generate both eigenstates. Such an algorithm is presented in Sec. III.

III. APPLICATION OF PHASE ESTIMATION TO FIND UNKNOWN EIGENVALUES AND EIGENVECTORS

Suppose that we have an unkown controlled-U gate, and we want to find its eigenvalues and generate qubits in its eigenstates. This can be done by modifying the phase estimation algorithm of Cleve *et al.* and using a singlet state as the input [2]. One takes two phase-estimation circuits for the same gate and sends into each circuit one of two particles, which together form a singlet state. This avoids the main disadvantage of the original algorithm. There, besides the controlled-U gates, one also needed a qubit prepared in one of the eigenstates. Sending this qubit through the network would then generate an estimate of the eigenvalue for this eigenstate. An alternative is to send in a random qubit, in which case one gets an estimate for a random eigenvalue. In particular, the estimate corresponds to one of the eigenvalues whose eigenstates have a nonzero overlap with the input state. The original qubit is left in a state that is in close approximation to the eigenstate corresponding to the measured eigenvalue [3,4].

Each of the two networks, which we shall label A and B, is constructed as follows. We have n control qubits, which for network A we shall call $A1,A2,\ldots An$, and one target bit, which we shall call A. Each of the control bits is initially in the state $(|0\rangle+|1\rangle)/\sqrt{2}$. Control bit Aj is connected to a gate that does nothing if the control bit is 0, and performs the operation $U^{2^{j-1}}$ if the control bit is 1. The network B is identical. The effect of the entire network is given by

$$|\Psi_{out}\rangle=G_{(Bn)B}(U^{2^{n-1}})\ldots G_{(B1)B}(U)\times G_{(An)A}(U^{2^{n-1}})\ldots G_{(A1)A}(U)|\Psi_{in}\rangle. \quad (16)$$

Let the eigenstates of U be $|u_1\rangle$ and $|u_2\rangle$ with eigenvalues $e^{i\phi_1}$ and $e^{i\phi_2}$, respectively. As before, the singlet state can be expressed in terms of these eigenstates

$$|\phi_s\rangle_{AB}=\frac{1}{\sqrt{2}}(|u_1\rangle_A|u_2\rangle_B-|u_2\rangle_A|u_1\rangle_B). \quad (17)$$

The initial state of the system is then

$$|\Psi_{in}\rangle=\frac{1}{\sqrt{2}2^n}(|u_1\rangle_A|u_2\rangle_B-|u_2\rangle_A|u_1\rangle_B)\times\prod_{j=0}^{n-1}(|0\rangle_{Aj}+|1\rangle_{Aj})\prod_{k=0}^{n-1}(|0\rangle_{Bk}+|1\rangle_{Bk}). \quad (18)$$

After passing through the networks this state becomes

$$|\Psi_{in}\rangle \rightarrow \frac{1}{\sqrt{2}2^n}\Bigg[|u_1\rangle_A \prod_{j=0}^{n-1}(|0\rangle_{Aj}+e^{i2^j\phi_1}|1\rangle_{Aj})|u_2\rangle_B \times \prod_{k=0}^{n-1}(|0\rangle_{Bk}+e^{i2^k\phi_2}|1\rangle_{Bk}) - |u_2\rangle_A \prod_{j=0}^{n-1}(|0\rangle_{Aj} + e^{i2^j\phi_2}|1\rangle_{Aj})|u_1\rangle_B \prod_{k=0}^{n-1}(|0\rangle_{Bk}+e^{i2^k\phi_1}|1\rangle_{Bk})\Bigg]. \tag{19}$$

The products in the above equation can be expressed as a sum over n-digit binary numbers. For example,

$$\prod_{j=0}^{n-1}(|0\rangle_{Aj}+e^{i2^j\phi_1}|1\rangle_{Aj}) = \sum_{y=0}^{2^n-1} e^{i\phi_1 y}|y\rangle_{An,\ldots,A1}. \tag{20}$$

The first digit of the n-digit binary number y corresponds to the state of system An, the second to that of $A(n-1)$, and so on. In the above equation we have indicated this explicitly with subscripts on the state, but in the future these will be omitted and this correspondence will be understood. It is still necessary to indiciate whether $|y\rangle$ is a state of $An,\ldots,A1$ or $Bn,\ldots,B1$, and this will be indicated by the subscripts $\overline{A}$ and $\overline{B}$, respectively. We then have that

$$|\Psi_{initial}\rangle \rightarrow \frac{1}{\sqrt{2}2^n}\Bigg[|u_1\rangle_A\Bigg(\sum_{y=0}^{2^n-1} e^{i\phi_1 y}|y\rangle_{\overline{A}}\Bigg)|u_2\rangle_B \times \Bigg(\sum_{w=0}^{2^n-1} e^{i\phi_2 w}|w\rangle_{\overline{B}}\Bigg) - |u_2\rangle_A \times \Bigg(\sum_{y=0}^{2^n-1} e^{i\phi_2 y}|y\rangle_{\overline{A}}\Bigg)|u_1\rangle_B\Bigg(\sum_{w=0}^{2^n-1} e^{i\phi_1 w}|w\rangle_{\overline{B}}\Bigg)\Bigg]. \tag{21}$$

The next step is to apply the quantum inverse Fourier transform operation to states $\overline{A}$ and $\overline{B}$. This takes the state $|y\rangle$ to

$$|y\rangle \rightarrow \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1} e^{-2\pi i y z/2^n}|z\rangle. \tag{22}$$

Before applying this, however, we want to express the phases ϕ_1 and ϕ_2 in different way. First, let $x_j=\phi_j/(2\pi)$ for $j=1,2$, which implies that $0\leqslant x_j<1$. In addition, let $\overline{x_j}$ be the closest integer to $2^n x_j$ (we assume $\overline{x_j}$ is expressed in binary form) so that

$$x_j = \frac{\overline{x_j}}{2^n}+\delta_j, \tag{23}$$

where $|\delta_j|\leqslant 1/2^{n+1}$. If we now apply the inverse Fourier transform we find that

$$\sum_{y=0}^{2^n-1} e^{2\pi i y[(\overline{x_j}/2^n)+\delta_j]}|y\rangle \rightarrow \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^n-1} e^{2\pi i y(\overline{x_j}-z)/2^n}e^{2\pi i y\delta_j}|z\rangle. \tag{24}$$

It is possible to perform the y summation in the above equation

$$g(z;\overline{x_j},\delta_j) = \frac{1}{2^n}\sum_{y=0}^{2^n-1} e^{2\pi i y(\overline{x_j}-z)/2^n}e^{2\pi i y\delta_j} = \frac{1}{2^n}\frac{1-e^{2\pi i\delta_j 2^n}}{1-e^{2\pi i\{[(\overline{x_j}-z)/2^n]+\delta_j\}}}. \tag{25}$$

This function is peaked about $z=\overline{x_j}$ and the maximum value of its magnitude is greater than $2/\pi$ [2]. After applying the inverse Fourier transform to both systems $\overline{A}$ and $\overline{B}$, our state is

$$|\Psi_{out}\rangle = \frac{1}{\sqrt{2}}\Bigg[|u_1\rangle_A\Bigg(\sum_{z=0}^{2^n-1} g(z;\overline{x_1},\delta_1)|z\rangle_{\overline{A}}\Bigg)|u_2\rangle_B \times \Bigg(\sum_{s=0}^{2^n-1} g(s;\overline{x_2},\delta_2)|s\rangle_{\overline{B}}\Bigg) - |u_2\rangle_A\Bigg(\sum_{z=0}^{2^n-1} g(z;\overline{x_2},\delta_2)|z\rangle_{\overline{A}}\Bigg)|u_1\rangle_B \times \Bigg(\sum_{s=0}^{2^n-1} g(s;\overline{x_1},\delta_1)|s\rangle_{\overline{B}}\Bigg)\Bigg]. \tag{26}$$

We now measure both systems $\overline{A}$ and $\overline{B}$ in the computational basis. The most likely results are either $\overline{x_1}$ for $\overline{A}$ and $\overline{x_2}$ for $\overline{B}$, in which case qubit A is in $|u_1\rangle$ and B is in $|u_2\rangle$, or $\overline{x_2}$ for $\overline{A}$ and $\overline{x_1}$ for $\overline{B}$, in which case qubit A is in $|u_2\rangle$ and B is in $|u_1\rangle$. In either case we have both the eigenvalues (to n places in base 2) and qubits in the eigenvectors.

IV. HIGHER-DIMENSIONAL SYSTEMS

The reasoning in the preceding sections can be extended from qubits to qudits, D-dimensional quantum systems. The fully antisymmetric state of D D-dimensional quantum systems is a $U(D)$ singlet [8]. If we denote the computational basis states by $|n\rangle$, where $n=0,1,\ldots,D-1$, this state can be expressed as

$$|\phi_s(D)\rangle = \frac{1}{\sqrt{D!}}\sum_{j_1=0}^{D-1}\cdots\sum_{j_D=0}^{D-1}\varepsilon_{j_1,\ldots,j_D}|j_1\rangle\cdots|j_D\rangle, \tag{27}$$

where $\varepsilon_{j_1,\ldots,j_D}$ is the totally antisymmetric tensor of rank D. Now consider a unitary operator U whose eigenstates are

$|u_j\rangle$, where $j=1,\ldots,D$. The fact that $|\phi_s(D)\rangle$ is a singlet means that it can be expressed as

$$|\phi_s(D)\rangle=\frac{1}{\sqrt{D!}}e^{i\mu}\sum_{j_1=1}^{D}\cdots\sum_{j_D=1}^{D}\varepsilon_{j_1,\ldots,j_D}|u_{j_1}\rangle\cdots|u_{j_D}\rangle, \tag{28}$$

where $e^{i\mu}$ is a phase factor that depends on how the phases of the eigenstates are chosen. We shall subsequently assume that they have been chosen so that $\mu=0$.

Let us now consider the following problem for the case $D=3$; its generalization to the case of arbitrary dimension is straightforward. We are given a controlled-U gate, where the control is a qubit and the target is a qutrit. If the control qubit is in the state $|0\rangle$ nothing happens to the target qutrit, and if it is in the state $|1\rangle$, the operation U is performed on the qutrit. This gate corresponds to the operator $G_{jk}(U)$, where j is the control qubit and k is the target qutrit. We shall assume that the operator U has eigenvalues 1 and -1, where the eigenvalue 1 is degenerate, and we would like to produce a qutrit in the eigenstate corresponding to -1.

This can be done with two controlled-U gates, two qubits, and three qutrits. The initial state of the system is

$$|\Psi_{in}\rangle_{a\cdots e}=|+x\rangle_a|+x\rangle_b|\phi_s(3)\rangle_{cde}. \tag{29}$$

Particles a and b are qubits and c, d, and e are qutrits. Qubit a is the control bit for qutrit c and qubit b is the control bit for qutrit d. The output state is given by

$$|\Psi_{out}\rangle_{a\cdots e}=G_{ac}(U)G_{bd}(U)|\Psi_{in}\rangle_{a\cdots e}. \tag{30}$$

Let $|u_1\rangle$ and $|u_2\rangle$ be orthonormal eigenstates of U with eigenvalue 1 and $|v\rangle$ be the eigenstate with eigenvalue -1. In terms of these states we have that

$$\begin{aligned}|\Psi_{out}\rangle_{a\cdots e}=\frac{1}{\sqrt{6}}[&|-x\rangle_a|+x\rangle_b(|vu_1u_2\rangle_{cde}-|vu_2u_1\rangle_{cde})\\&+|+x\rangle_a|-x\rangle_b(|u_2vu_1\rangle_{cde}-|u_1vu_2\rangle_{cde})\\&+|+x\rangle_a|+x\rangle_b(|u_1u_2v\rangle_{cde}-|u_2u_1v\rangle_{cde})].\end{aligned} \tag{31}$$

We now measure qubits a and b in the $|\pm x\rangle$ basis. If we find a in the $|-x\rangle$ state, then qutrit c is in the eigenstate with eigenvalue -1, while if qubit b is in the $|-x\rangle$ state, then it is qutrit d that is in the -1 eigenstate. Finally, if both of these qubits is found to be in the $|+x\rangle$ state, then qutrit e is in the -1 eigenstate.

In the corresponding problem for qudits, U has eigenvalues -1, which is nondegenerate, and 1, which is $(D-1)$-fold degenerate. The object is to produce a qudit in the eigenstate corresponding to -1. To do so one uses a network consisting of $D-1$ qubits, D qudits in a singlet state, and $D-1$ controlled-U gates. The procedure is a simple generalization of the one just discussed for qutrits.

V. CONCLUSION

We have shown that singlet states in combination with controlled-U gates can be used to produce qubits or qudits, in eigenstates of the operator U. If U is the evolution operator corresponding to some Hamiltonian, its eigenstates are just those of the Hamiltonian. This procedure will not tell us what those eigenstates are, but we can perform measurements on the qudits in those states in order to gain information about them. We may also simply be interested in performing further operations on these states without measuring them first, and we now have a way of producing them.

If singlet states are combined with the phase-estimation algorithm for finding eigenvalues of U, we can, in a certain sense, diagonalize the operator. We saw that for qubits we both knew the eigenvalues, at least to a level of approximation that we can determine, and we produced qubits in states that are very close to the eigenstates of U. This procedure should generalize to qudits.

ACKNOWLEDGMENTS

This research was supported by the National Science Foundation under Grant No. PHY-9970507, and by the European Union project EQUIP under Contract No. IST-1999-11053.

[1] A. Kitaev, e-print quant-ph/9511026.
[2] R. Cleve, A. Ekert, C. Macchiavelo, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998); e-print quant-ph/9708016.
[3] D.S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999).
[4] B.C. Travaglione and G.J. Milburn, e-print quant-ph/0008053.
[5] I.D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[6] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[7] A. Peres, Phys. Lett. A **128**, 19 (1988).
[8] See, for example, H. Georgi, *Lie Algebras in Particle Physics: from Isospin to Unified Theories* (Benjamin, Reading, 1982), p. 114.