Fast protocols for local implementation of bipartite nonlocal unitaries

Li Yu, Robert B. Griffiths, and Scott M. Cohen

Phys. Rev. A **85**, 012304 — Published 4 January 2012

DOI: 10.1103/PhysRevA.85.012304

Fast protocols for local implementation of bipartite nonlocal unitaries

Li Yu[1],* Robert B. Griffiths[1], and Scott M. Cohen[1,2]
[1]*Department of Physics, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213*
[2]*Department of Physics, Duquesne University, Pittsburgh, Pennsylvania 15282*

In certain cases the communication time required to deterministically implement a nonlocal bipartite unitary using prior entanglement and LOCC (local operations and classical communication) can be reduced by a factor of two. We introduce two such "fast" protocols and illustrate them with various examples. For some simple unitaries, the entanglement resource is used quite efficiently. The problem of exactly which unitaries can be implemented by these two protocols remains unsolved, though there is some evidence that the set of implementable unitaries may expand at the cost of using more entanglement.

PACS numbers: 03.67.Ac, 03.67.Dd, 03.67.Lx

I. INTRODUCTION

A central problem in quantum information theory is that of interconversion between resources, for example, how to use communication channels to produce entanglement between distant parties, or how to use such entanglement to carry out nonlocal operations. In particular, the use of prior entanglement assisted by classical communication to carry out nonlocal unitaries has been the subject of various studies [1–3]; for a more extensive list see [3].

In this paper we add *time* as a resource to be considered along with entanglement cost when constructing protocols for bipartite nonlocal unitaries (nonlocal gates). The ability to implement nonlocal unitaries rapidly may be particularly relevant in the context of distributed quantum computation [4–7], where less time consumption means less decoherence; or in position-based quantum cryptography [8–11], where it may allow certain position verification schemes to be broken.

The usual protocols for bipartite unitaries, such as those in [3], have the following general structure: Alice carries out local operations and measurements, and sends the measurement results through a classical communication channel to Bob, who then carries out corresponding operations and measurements, and sends the measurement results back to Alice using classical communication. Finally, Alice performs additional local operations that may depend on the previous measurement results of both parties. When the distance between the two parties is large the total time required for the protocol will be dominated by the two rounds of communication, thus double the minimum time for a signal to pass from one to the other. However, there exist nonlocal unitaries which can be implemented by a protocol in which Alice and Bob carry out local operations and measurements at the same time, and then simultaneously send the results to the other party, and finally perform local operations depending on the received messages to complete the protocol. This reduces the total communication time by a factor of two [1]. We are interested in identifying which bipartite unitaries can be carried out using such a *fast* protocol, and also in finding the associated entanglement cost. The crucial distinction between a fast and slow protocol of the form considered here is that for the latter, Bob needs to wait for a message from Alice before choosing the basis in which to carry out his measurement ("choosing the measurement basis" is equivalent to choosing what local gates to do before his measurement), whereas in the former this basis can be fixed in advance.

We have identified two classes of nonlocal unitary that lend themselves to a fast protocol: *controlled* unitaries of the form shown in (1) below, and *group* unitaries of the form shown in (9). The slow versions of both were considered in our previous work [3], where we showed that controlled unitary protocols, while useful for understanding how such protocols work, can always be replaced by group unitary protocols that make use of the same resources. Our fast protocols represent special cases, i.e., special groups and parameter choices, of the slow protocols discussed previously, and once again the controlled kind can be replaced by the group kind. By increasing the amount of entanglement expended, additional unitaries can be carried out using these fast protocols. In some cases this allows an arbitrarily close approximation to a unitary which cannot be carried out exactly by these methods. A still more general class of slow protocols, corresponding to Eq. (18) in [3], also has a fast version, but we have yet to find examples of unitaries it can carry out that cannot be implemented by our other fast protocols.

The protocols we consider are deterministic—they succeed with probability one—and use a definite amount of entanglement determined in advance. Such deterministic fast protocols have previously been studied by Groisman and Reznik [12] for a CNOT gate on two qubits, and by Dang and Fan [13] its counterpart on two qudits. In

* liy@andrew.cmu.edu

[1] There may be in practice other temporal costs that need to be taken into account, such as that required to produce the initial entangled state. We are ignoring these in the present paper.

addition Buhrman et al. [11] and Beigi and König [14] have published approximate schemes for what they call "instantaneous quantum computation", equivalent to a fast bipartite unitary in our language. These protocols, unlike ours, can be used, to approximately carry out any bipartite unitary. The one in [11], which is based on the nonlocal measurement protocol in [15], has a probability of success less than 1, so it is not deterministic, but this probability can be made arbitrarily close to 1 by using sufficient entanglement. The protocol in [14] uses a fixed amount of entanglement to implement with probability 1 a bipartite quantum operation (completely positive trace preserving map) which is close to the desired unitary, and it can be made arbitrarily close by using sufficient entanglement. The term "instantaneous" is not unrelated to the idea of an "instantaneous measurement" as discussed in [15–17], where the terminology seems somewhat misleading in that completing their protocols actually requires a finite communication time, e.g., the parties must send the results to headquarters (or to each other) in order to complete the identification of the measured state. In the same way, "instantaneous quantum computation" actually requires a finite communication time, the same as in our fast protocol.

The paper is organized as follows. In Sec. II we consider controlled unitaries of the form Eq. (1), where the unitaries being controlled form an Abelian group. (Appendix A contains an argument, which may be of more general interest, that allows projectors P_k in this formula to be replaced by projectors of rank 1, i.e., pure states.) In addition we show how subsets of the collection of unitaries representing an Abelian group can be employed to generate fast unitaries otherwise not accessible by our protocol. Section III is devoted to group unitaries of the form (9), including a significant number of examples. We also present an argument showing that the controlled-Abelian unitaries of Sec. II can be transformed to group unitaries of the form (9). The concluding Sec. IV contains a brief summary along with an indication of some open problems.

II. FAST PROTOCOL FOR CONTROLLED-ABELIAN-GROUP UNITARIES

In this section we construct a fast protocol for any controlled-Abelian-group unitary of the form

$$\mathcal{U} = \sum_{k=0}^{N-1} P_k \otimes V_k, \tag{1}$$

where the P_k are orthogonal projectors, possibly of rank greater than 1, on a Hilbert space $\mathcal{H}_A$ of dimension d_A. The $\{V_k\}$ are unitary operators on a Hilbert space $\mathcal{H}_B$ of dimension d_B, that form a representation of an Abelian group G of order N. As shown in Appendix A 2, it suffices to consider projectors of rank 1. That is, a scheme for implementing

$$\mathcal{U} = \sum_{k=0}^{N-1} |k\rangle\langle k| \otimes V_k, \tag{2}$$

where $|k\rangle$ denotes a ket belonging to a standard (or computational) orthonormal basis, is easily extended to one that carries out the more general (1). In addition we shall consider cases, Sec. II C, in which the $\{V_k\}$ form a *subset* of an Abelian group, with the sum in (1) restricted to a subset S of the integers from 0 to $N-1$.

A. Fast protocol for controlled-cyclic-group unitaries

The simplest Abelian group is a cyclic group, so we start with the case where the $\{V_k\}$ in (2) are a representation of such a group. (It suffices to consider ordinary representations, since a projective representation of a cyclic group is equivalent to an ordinary representation, see Sec. 12.2.4 of [24].) It will be convenient to let V_0 be the identity and $V_k = V_1^k$. The slow protocol [3] for this case, which works for any collection $\{V_k\}$ of unitaries on B, is shown in Fig. 1, where

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle_a \otimes |j\rangle_b \tag{3}$$

is a fully entangled state on the ancillary systems a and b associated with A and B, respectively, and the gates X, Z, and F (the Fourier matrix) are defined by

$$X = \sum_{j=0}^{N-1} |j \ominus 1\rangle\langle j|, \quad Z = \sum_{k=0}^{N-1} e^{2\pi i k/N} |k\rangle\langle k|,$$
$$F = \frac{1}{\sqrt{N}} \sum_{m,k=0}^{N-1} e^{2\pi i m k/N} |m\rangle\langle k|. \tag{4}$$

Here $j \ominus 1$ denotes $(j-1) \mod N$, so $X^l|j\rangle = |j \ominus l\rangle$. The symbols resembling "D" in Fig. 1 represent measurements in the standard basis.

The slow protocol proceeds by Alice carrying out the operations indicated on the left side of Fig. 1, and then sending the outcome l of the measurement on a to Bob over a classical channel. He uses it to carry out a gate X^l, followed by the other operations in the center of the figure. His final measurement outcome m is sent to Alice over another classical channel, who uses it to perform an additional gate $Z_m = Z^{-m}$ that completes the protocol.

A faster protocol can be constructed if the two rounds of classical communication can be carried out simultaneously instead of consecutively. This is possible if Bob can carry out various operations, including a measurement, in advance of receiving the value of l from Alice, as in Fig. 2. The classical signals can then be sent simultaneously, and the protocol is completed when both Alice

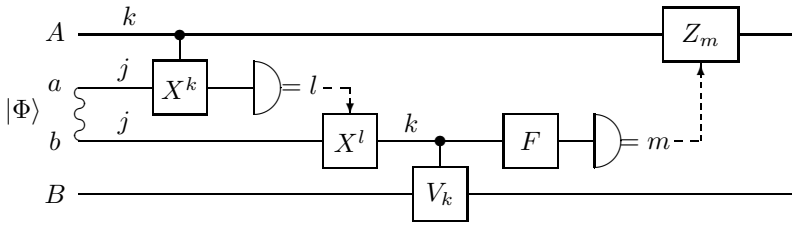

FIG. 1. The slow protocol in Sec. III of [3] for implementing the unitary $\mathcal{U} = \sum_{k=0}^{N-1} |k\rangle\langle k| \otimes V_k$.

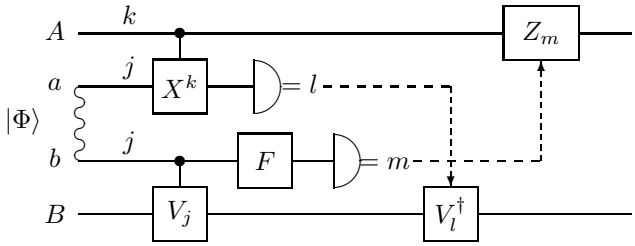

FIG. 2. The fast protocol for implementing the unitary $\mathcal{U} = \sum_{k=0}^{N-1} |k\rangle\langle k| \otimes V_k$.

and Bob make final corrections that depend on the signals they receive. In order to change the slow protocol into a fast protocol, one must, in effect, push the X^l gate in Fig. 1 through the two gates that follow it in order to arrive at the situation in Fig. 2. The two steps are:

1. Commute X^l with the controlled-V_k gate: the X^l itself passes through the control node unchanged, but leaves the V gate controlled by state $|j\rangle$ instead of $|k\rangle$, so V_j instead of V_k acts on B. This can be compensated at the end of the protocol by a local unitary correction of $V_l^\dagger$, with $l = j \ominus k$ (see the discussion below).

2. Commute X^l with F: we have that $FX^l = Z^{-l}F$, and since the Z^{-l} are diagonal unitaries, they do not affect the measurement result m in the standard basis, and thus Z^{-l} is absent from the fast protocol in Fig. 2. (Due to the removal of Z^{-l} there is an unimportant global phase, dependent on l and m, that is introduced in the implementation of $\mathcal{U}$.)

The final correction $V_l^\dagger$ is possible because the $\{V_k\}$ form a cyclic group: the net operation on B is $V_l^\dagger V_j = V_{j\ominus l} = V_{j\ominus(j\ominus k)} = V_k$, where $l = j \ominus k$ follows from Fig. 1 and the definition of the X^l gate. This is an extra restriction over the slow protocol, where the V_k can be arbitrary unitaries.

Example 1.
Case (i). $\mathcal{U}$ is the N-dimensional CNOT gate, with $N = d = d_A = d_B$, and $V_k = X^k$ form a cyclic group. This is the class of unitaries implementable by Dang and Fan's protocol shown in Fig. 2 of [13].

Case (ii). $\mathcal{U}$ is a controlled unitary of the form (2) with $N = d_A = 3$, $d_B = 2$, $V_k = \mathrm{diag}(1, e^{2\pi ik/3})$, $k = 0, 1, 2$. (The V_k are not shift operators, so this is more general than the protocol in [13].)

B. Generalization to a controlled-Abelian-group

The fast protocol for controlled-cyclic-group unitaries is easily generalized to the case where the V_k in (1) form an ordinary representation of an Abelian group G of order N. Again it suffices (Appendix A 2) to consider the case (2) where the P_k are rank 1 projectors. Any finite Abelian group is the direct sum (direct product) of η cycles, and it is convenient to adopt a label k for elements of G that reflects this structure, by thinking of it as an η-tuple of integers,

$$k = (k_1, k_2, \ldots k_\eta), \tag{5}$$

with $0 \le k_i \le r_i - 1$, where r_i is the length of the i-th cycle. In this way group multiplication, with $k = (0, 0, \ldots 0)$ the identity, is the same as vector addition, modulo r_i for the i-th component. Similarly, the j labels on the systems a and b in Fig. 2, and the measurement outcomes l and m, can also written as η-tuples: $j = (j_1, j_2, \ldots j_\eta)$, etc. In the following we will make use of the inner product of two η-tuples such as $(j \cdot m) = \sum_{i=1}^{\eta} j_i m_i$.

The X, Z, and F gates are now appropriate tensor products of the cyclic group gates in (4); e.g., X^k understood as $\bigotimes_{i=1}^{\eta} X_i^{k_i}$ and $X^k|j\rangle = |j \ominus k\rangle$, using the obvious η-tuple definition of $j \ominus k$. The Z_m gate in Fig. 2 is the tensor product of the $Z_i^{-m_i}$ gates for the different

cycles,

$$Z_m = \sum_k e^{-2\pi i(k\cdot m)/N} |k\rangle\langle k|. \tag{6}$$

Here is why the protocol works. Assume an initial product state $|k\rangle \otimes |\omega_k\rangle$ on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then the operator implemented on B is $V_l^\dagger V_j = V_{j\ominus k}^\dagger V_j = V_{k\ominus j} V_j = V_k$. The F gate on b before the measurement gives rise to a phase $e^{2\pi i(j\cdot m)/N}$, which is partially compensated by the phase $e^{-2\pi i(k\cdot m)/N}$ in the Z_m gate on A, and since $j = k \oplus l$, we are left with an overall phase of $e^{2\pi i(l\cdot m)/N}$. Since this phase is independent of k, a superposition of initial product states of this form for different k will also be transformed by $\mathcal{U}$, up to an overall phase that is of no concern.

Note that the V_k themselves may, but need not, be tensor products, as illustrated in the following example.

Example 2.
Case (i): $d_A = d_B = 4$. The V_k defined by

$$\begin{aligned} V_{(0,0)} &= \mathrm{diag}(1,1,1,1), & V_{(0,1)} &= \mathrm{diag}(1,1,-1,-1), \\ V_{(1,0)} &= \mathrm{diag}(1,-1,1,-1), & V_{(1,1)} &= \mathrm{diag}(1,-1,-1,1), \end{aligned} \tag{7}$$

are tensor products, and form a group $C_2 \times C_2$. If one regards $\mathcal{H}_A$ as well as $\mathcal{H}_B$ as a tensor product of two qubits, the $\mathcal{U}$ defined by (2) is itself a tensor product $\mathcal{U} = \mathcal{U}_1 \otimes \mathcal{U}_2$, with each factor a controlled-cyclic group unitary with one qubit on the A and the other on the B side. Thus $\mathcal{U}$ can be implemented by an overall protocol which is just two smaller protocols running in parallel with each other, one for $\mathcal{U}_1$ and the other for $\mathcal{U}_2$.

Case (ii): $d_B = 3$. Modify the V_k in (7) by keeping only the first three rows and columns, so they are no longer tensor products, though they still form a group $C_2 \times C_2$. Consequently, the protocol that carries out $\mathcal{U}$ can no longer be viewed as two smaller protocols running in parallel.

C. Controlled subset of an Abelian group

Assume that the $\{V_k\}$ in (1) form an ordinary representation of an Abelian group of order N, but the sum over k is restricted to some subset S of the set of N η-tuples defined in the last subsection. It will suffice once again to consider the case of rank-one projectors, i.e., (2). The j, l, and m in Fig. 2 run over the same range as before, but k is restricted to the set S. Therefore the dimension $d_A = n$ of $\mathcal{H}_A$ is less than the Schmidt rank of $|\Phi\rangle$, which is the order N of the group. It is convenient to use the elements of S to label the kets that form the basis of $\mathcal{H}_A$ in (2) (corresponding to the projectors in (1)). The operator Z_m is now given by (6), but with k restricted to S. The reason that the fast protocol in Fig. 2 will work in this case is the same as given above in Sec. II B; the fact that k is restricted to a subset makes no difference.

The significance of this extension of the result in Sec. II B is that it enlarges the class of fast unitaries that can be carried out using a protocol of this sort, though perhaps with a significant increase in the entanglement cost. This is illustrated by the following example, which shows that in certain cases one can approximate a continuous family of unitaries using sufficient entanglement (a large enough N).

Example 3.
Consider a unitary on two qubits A and B of the form

$$\mathcal{U} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes R, \tag{8}$$

where $R = V_m = \mathrm{diag}(1, e^{2\pi i m/N})$ for some integer $m < N$. By relabeling $|1\rangle\langle 1|$ on A as $|m\rangle\langle m|$, we see that (8) is of the form (2) with k in the sum restricted to the two values in $S = \{0, m\}$. Thus $\mathcal{U}$ can be carried out in a fast way at an entanglement cost of $\log_2 N$ ebits. In general, any two-qubit controlled unitary is of the form (8) (up to local unitaries on A and B, before and after $\mathcal{U}$) with $R = \mathrm{diag}(1, e^{i\phi})$ for some real number ϕ. Since ϕ can be approximated by 2π multiplied by a rational number m/N with large enough N, any two-qubit controlled unitary can be approximately implemented (up to local unitaries) using this fast protocol by setting R equal to $\mathrm{diag}(1, e^{2\pi i m/N})$ for suitable m and N; the entanglement cost is again $\log_2 N$ ebits.

A further generalization to arbitrary d_A and d_B is possible for any unitary $\mathcal{U}$ which is diagonal in a product of bases, a basis on $\mathcal{H}_A$ and another on $\mathcal{H}_B$. When such a diagonal $\mathcal{U}$ is written in the form (2), the unitaries V_k are diagonal. Each diagonal element of V_k is approximately an integer root of unity, hence each V_k is approximately an integer root of the identity operator, and the whole set $\{V_k\}$ can be approximated by a subset of an ordinary representation of an Abelian group of sufficient size. Thus any bipartite unitary diagonal in a product of bases can be approximately implemented by a fast protocol.

III. FAST PROTOCOL FOR DOUBLE-GROUP UNITARIES

In this section we consider a fast protocol for "double-group" unitaries of the form

$$\mathcal{U} = \sum_{f\in G} c(f)\, \Gamma(f) = \sum_{f\in G} c(f)\, U(f) \otimes V(f), \tag{9}$$

where G is a group of order N, $U(f)$ and $V(f)$ are unitaries on Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of dimension d_A and d_B respectively, and the operators $\Gamma(f) = U(f) \otimes V(f)$ form a projective representation of G, in the sense that

$$\Gamma(g)\Gamma(h) = \lambda(g,h)\Gamma(gh). \tag{10}$$

The collection $\{\lambda(g,h)\}$ of complex numbers of unit magnitude is known as the factor system. Similarly, $\{U(f)\}$ and $\{V(f)\}$ each form a projective unitary representation

of G with individual factor systems which may differ from one another, whose product for a given g and h is $\lambda(g,h)$. From Sec. 12.2.1 of [24], for our purposes we can assume the factor system $\{\lambda(g,h)\}$ is *standard*, that is,

$$\lambda(e,e) = \lambda(e,f) = \lambda(f,e) = 1, \ \ \forall f \in G. \tag{11}$$

where e is the identity element in G.

A. Protocol

The slow protocol in Sec. IV D of [3] for implementing unitaries of the type (9) is shown in Fig. 3. The two parties share a maximally entangled state

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{f\in G} |f\rangle_a \otimes |f\rangle_b, \tag{12}$$

on the ancillary systems a, b, each of dimension N, the order of G. Alice and Bob perform controlled-$U(f)$ and controlled-$V(f)$ gates on aA and bB, respectively. Alice follows this with a T gate on a, where in the standard basis T is a complex Hadamard matrix $\hat{T}$ divided by $\sqrt{N}$, i.e., a unitary with all elements of the same magnitude $1/\sqrt{N}$. Then she does a measurement on a in the standard basis and sends the result l to Bob. Bob carries out a Z_l gate on b, where each Z_l is a diagonal unitary matrix whose diagonal elements are the complex conjugates of those in the l-th row of $\hat{T}$. Thus T and Z_l generalize the Fourier gate F and the Z^{-l} gate in our previous paper [3]. This more general choice does not extend the set of unitaries the slow protocol can implement, since the phases in T and Z_l cancel each other, but it allows the fast protocol to implement a larger set of unitaries than would otherwise be possible.

Next, Bob applies a unitary gate

$$C = \sum_{f,g\in G} \lambda(g, g^{-1}f)\, c(g^{-1}f)\, |g\rangle\langle f| \tag{13}$$

to b, where $\lambda(g,h)$ is defined in (10) and the coefficients $c(f)$ are those in (9). (The coefficients $c(f)$ are not uniquely defined by $\mathcal{U}$ if the $\Gamma(f)$ are linearly dependent, but there is always at least one choice for which C is unitary, Theorem 7 of [3].) Then he measures b in the standard basis and sends the result m to Alice. To complete the protocol Alice and Bob apply unitary corrections $(U(m))^\dagger$ and $(V(m))^\dagger$ to their respective systems.

The slow protocol in Fig. 3 can be replaced with the fast protocol in Fig. 4 provided the Z_l gate in the former, which in effect determines the basis for Bob's measurement, can be eliminated at the cost of re-interpreting the outcome m of his measurement. A sufficient condition for this is that for every l there exists a *complex permutation* matrix $\tilde{P}_l$ (exactly one nonzero element of magnitude one in each row and in each column) such that

$$CZ_l = \tilde{P}_l C. \tag{14}$$

The effect of $\tilde{P}_l$ is simply to permute the measurement outcomes, which can then be re-interpreted once l is known. The phases in $\tilde{P}_l$ would only introduce a global phase for the implemented $\mathcal{U}$ (dependent on l and m) and are therefore of no concern.

A useful procedure for generating C and T matrices for which (14) holds employs the *character table* $\hat{K}$ of an Abelian group H of order N. This is an $N \times N$ matrix, all elements of which are of magnitude 1, with columns labeled by elements of H and rows by its distinct irreducible representations, all of which are one-dimensional. Because the representations are one-dimensional, each row is itself a representation (i.e., the character is the representation "matrix"). The element-wise product of two columns is another column, since each row is a representation of the group; likewise the element wise product of two rows is another row, since the (tensor) product of two representations is a representation. Thus the transpose of a character table is again a character table. The complex conjugate of any column (or row) is another column (row) of $\hat{K}$ corresponding to the inverse of the group element. The actual order of the columns or the rows is arbitrary, though it is often convenient to assume that the first row and the first column contain only 1's. Since $K = \hat{K}/\sqrt{N}$ is a unitary matrix, a character table $\hat{K}$ is a special case of a complex Hadamard matrix: one whose elements are all of magnitude 1, and whose rows (and columns) are mutually orthogonal. If H is a cyclic group C_N, then up to permutations of rows or columns $\hat{K} = \hat{F} = \sqrt{N}\, F$, with F the Fourier matrix (4); similarly if H is the direct product (sum) of cycles, $\hat{K}$ is the tensor product of the corresponding Fourier matrices [19].

Theorem 1.
(a) Let $\hat{K}$ be the character table of an Abelian group H of order N, and define

$$\hat{T} = \sqrt{N}\, T = L\hat{K}, \quad \hat{C} = \sqrt{N}\, C = M\hat{K}D, \tag{15}$$

where L and M are complex permutation matrices, and D a diagonal matrix with diagonal elements of magnitude 1, thus a diagonal unitary. Let Z_l be the diagonal matrix with diagonal elements equal to the complex conjugates of those forming row l of $\hat{T}$. Then there exist complex permutation matrices $\tilde{P}_l$ such that (14) *is satisfied for every l.*

(b) If the rows of an $N \times N$ matrix $\hat{T}$ are linearly independent and form a (necessarily Abelian) group H up to phases under element-wise multiplication, then $\hat{T}$ is of the form given in (15).

The proof is in Appendix B. Note that the group H need not be isomorphic to the group G represented by $\{\Gamma(f)\}$ although they are of the same order—see Example 8 in Sec. III C with $n > 2$. The matrix $\hat{T}$ defined in (15) has the property that the rows under element-wise products form the Abelian group H up to a possible phase factor determined by L.

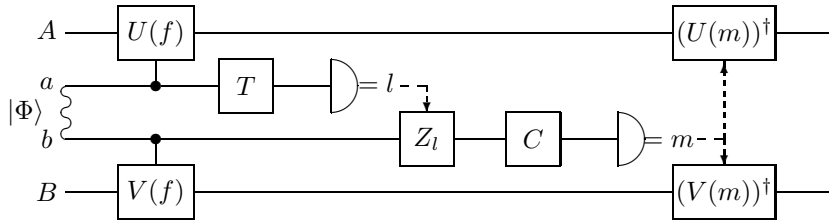

FIG. 3. The slow protocol that implements the unitary $\mathcal{U}$ in (9).

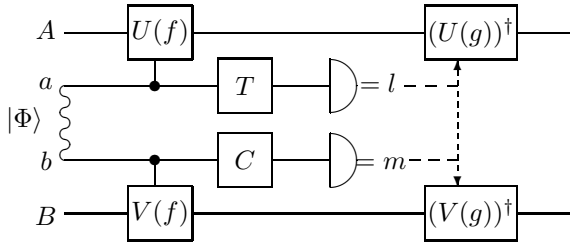

FIG. 4. The fast protocol that implements the unitary $\mathcal{U}$ in (9) when the conditions given in Theorem 1 are satisfied. The g for the final corrections depends on both measurement outcomes l and m.

One consequence of (15) is

$$C = PTD, \tag{16}$$

where P is a complex permutation matrix and D is a diagonal unitary. When the matrix C is of the form (13), the fact that all its elements are of the same magnitude $1/\sqrt{N}$, as implied by (15), means that the same is true of the $c(f)$. A partial answer to the question of whether (14) implies that T and C have the form given in (15) is provided by the following theorem, whose proof is also in Appendix B.

Theorem 2. *For each l let Z_l be the diagonal matrix whose elements are the complex conjugates of those forming row l of a complex Hadamard matrix $\tilde{T} = \sqrt{N}T$. If there exists a unitary matrix C without a zero element in its first row, and complex permutation matrices $\tilde{P}_l$ such that Eq.* (14) *holds for every l, then the matrices Z_l form an Abelian group up to phases, and* (15) *and* (16) *hold.*

It is worth noting that with T and C of the form (15) there is a symmetrical version of the fast protocol in Fig. 4 in which the C gate on the B side is replaced with T. This requires that the entangled resource $|\Phi\rangle$ be changed to

$$|\Phi'\rangle = (I \otimes D)|\Phi\rangle. \tag{17}$$

The reason this works is that the changes produced by P in (16) in the measurement outcome m can always be compensated by altering the function $g(l, m)$ that determines the final corrections. The following is a simple example.

Example 4.
The two-qubit unitary

$$\mathcal{U} = \frac{1}{\sqrt{2}}(I_A \otimes I_B + iZ_A \otimes Z_B), \tag{18}$$

where Z_A and Z_B are Pauli σ_z gates on A and B, is equivalent under local unitaries to a CNOT gate. It is of the form (9) with G the cyclic group C_2 of order 2, and can be implemented by the fast protocol in Fig. 4 using the matrices

$$T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad C = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{19}$$

where the rows of T multiplied by $\sqrt{2}$ form a group $H = C_2$. Because T and C change the measurement basis, Alice and Bob effectively perform measurements of σ_x and σ_y, respectively; this is the same thing (with the parties interchanged) as the fast protocol in [12]. An equivalent symmetrized protocol in which C is replaced by T employs a resource state $|\Phi'\rangle = \frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$, and both parties perform a σ_x measurement.

B. Which unitaries can be carried out using the fast protocol?

Given a particular bipartite unitary $\mathcal{U}$, can it be implemented using the fast double-group protocol? Any such $\mathcal{U}$ can always be written in the form (9) using a sufficiently large group (see Sec. V A of [3]), and typically there are many different ways of constructing such an expansion. However, for our fast protocol to work, assuming that T and C are of the form given in (15), one must find a *particular* expansion, a particular group G and unitaries $U(f)$ and $V(f)$ along with expansion coefficients $c(f)$, that satisfy appropriate conditions. In particular, (i) the $c(f)$ must all be of the same magnitude $1/\sqrt{N}$, as noted following (16). But two additional conditions must be checked: (ii) the matrix C defined in (13) must be unitary, and (iii) C must be related to the

character table of some group H as in (15). Condition (iii) can be checked in the following way. Multiply each row and then each column of $\hat{C} = \sqrt{N}\,C$ by a suitable phase such that the resulting matrix $\hat{C}' = Q\hat{C}R$, where Q and R are diagonal unitaries, has 1's in the first row and first column. Then check whether its rows (alternatively, its columns) form a group H under component-wise multiplication. If this is so, then $\hat{C}'$ is a character table of H. Equating it to $\hat{K}$ in (15), letting $D = R^{-1}$ and $M = Q^{-1}$, and choosing any complex permutation matrix L, we arrive at a T which along with this C satisfies the conditions of Theorem 1. Thus, provided (i), (ii), and (iii) are satisfied there is in fact a fast unitary $\mathcal{U}$.

The scheme just described provides a useful approach for constructing examples. Start with a group G and (projective) unitary representations $\{U(f)\}$ and $\{V(f)\}$ on $\mathcal{H}_A$ and $\mathcal{H}_B$, and look for a set of coefficients $\{c(f)\}$ of equal magnitude such that C given by (13) is unitary, and satisfies condition (iii) in the preceding paragraph. The search is aided by noting that any factor system, see Sec. 12.2.2 of [24], is equivalent to a *normalized* factor system in which each $\lambda(g, f)$ is an N-th root of 1. A consequence, proved in Appendix B, is the following:

Theorem 3. *Let $\Gamma(f)$ in (9) be a projective representation of a group G of order N with a normalized (see above) factor system $\lambda(g, h)$, (10). Assume the matrix C defined in (13) is of the form given in (15). Then the coefficients $\{c(f)\}$ in (13) can be written in the form*

$$c(f) = (\gamma/\sqrt{N}\,)\exp[\,2\pi i k(f)/N^2\,], \tag{20}$$

where $k(f)$ is an integer that depends upon f, and γ is a phase factor independent of f.

The theorem justifies the following exhaustive, albeit tedious, search procedure for possible sets of coefficients $c(f)$, assuming they all have the same magnitude, once a group G, a projective representation of G, and a normalized factor system have been chosen. Consider all possible sets of coefficients of the form (20), setting $\gamma = 1$ and $c(e) = 1/\sqrt{N}$ for the identity e of G, as the global phase of $\mathcal{U}$ is unimportant. For each set, check that the matrix C given by (13) is unitary. Then see if the rows of the corresponding $\hat{C}'$, constructed as described above, form a group under component-wise multiplication. Using this procedure we have been able to show that if $N = 2$, so the group is C_2, the only two-qubit unitaries that can be implemented by our fast protocol are either trivial products of unitaries or else equivalent under local unitaries to a CNOT gate. (Note that there are additional fast two-qubit unitaries that can be carried out using a bigger group, thus larger N and more entanglement.)

Both conditions (ii) and (iii) are nontrivial requirements. Not every case in which the $c(f)$ are of equal magnitude will lead to a unitary matrix C. For example, if $c(f) = 1/\sqrt{N}$ for every f and $\{\Gamma(f)\}$ is an ordinary representation of G, so $\lambda(g, h) = 1$, then (13) obviously does not define a unitary matrix. And even if C is unitary, condition (iii) may not hold. For example, the unitary in Eq. (58) of [3] with $c(0,0) = c(1,0) = 1/2$, $c(0,1) = e^{i\alpha}/2$, $c(1,1) = -e^{i\alpha}/2$, assuming α is not an integer multiple of $\pi/4$, results in a $\hat{C}'$ matrix whose rows do not form a group.

For every ordinary representation of an Abelian group G there is a corresponding fast protocol, as the group is a direct product (sum) of cycles, and one can apply the construction in Example 6 below. For general projective representations or non-Abelian groups the matter remains open.

C. Examples

The examples which follow represent just a few of the unitaries that can be carried out by our double-unitary fast protocol. Examples 5 and 6 make relatively efficient use of entanglement resources, in that the order of the group, which is the rank of the fully-entangled resource state, is equal to the Schmidt rank (or Schmidt number [18]) of $\mathcal{U}$—the minimum number of summands required to represent it as a sum of products of operators on A and B—of $\mathcal{U}$. Examples 7 and 8, the latter involving a non-Abelian group G, illustrate how the class of fast unitaries can be significantly expanded by using more entanglement.

Note that any two-qubit unitary is equivalent under local unitaries to one of the form, see [20],

$$\mathcal{U} = \exp[\,i(\alpha\sigma_x \otimes \sigma_x + \beta\sigma_y \otimes \sigma_y + \gamma\sigma_z \otimes \sigma_z)\,], \tag{21}$$

where α, β, and γ are real numbers that can be calculated from the matrix of $\mathcal{U}$ (see e.g. the appendix of [21] for the method of calculation). For the two-qubit examples below we give the values of α, β, and γ.

Example 5.
In the two-qubit unitary

$$\mathcal{U} = c(0)I \otimes I + c(1)X \otimes X + c(2)Z \otimes Z + c(3)XZ \otimes XZ, \tag{22}$$

with I the identity, X and Z the Pauli operators σ_x and σ_z, and G the group $C_2 \times C_2$, the method of search indicated in Sec. III B yields the following possibilities for $c = (c(0), c(1), c(2), c(3))$.

(a) The case $c = (1, 1, 1, -1)/2$ is equivalent to the SWAP gate defined in [22], in which the two qubits are interchanged; $\alpha = \beta = \gamma = \pi/4$ in (21). An alternative fast protocol for this gate consists of teleportation done simultaneously in both directions.

(b) The case $c = (1, i, 1, -i)/2$ implements the U_{XY} gate as defined in [22], equivalent under local unitaries to the double-CNOT or DCNOT gate defined in [21]; $\alpha = \beta = \pi/4$, $\gamma = 0$.

(c) The case $c = (1, 1, \zeta, \zeta^5)/2$, where $\zeta = e^{i\pi/4}$; $\alpha = \beta = \pi/4$, $\gamma = \pi/8$.

In each case the entanglement resource of two ebits required to carry out the protocol is the minimum possible

amount, since the unitary is capable of creating two ebits of entanglement.

Example 6.

When the $\{\Gamma(f)\}$, with f an integer between 0 and $N-1$, form an ordinary representation of the cyclic group C_N of order N, the coefficients

$$c(f) = \begin{cases} (1/\sqrt{N})\exp(-i\pi f^2/N), & N \text{ even}, \\ (1/\sqrt{N})\exp(-i\pi f(f+1)/N), & N \text{ odd}, \end{cases} \tag{23}$$

will provide a fast implementation of (9). In particular with $U(f) = V(f) = Z^{-f}$ this becomes

$$\mathcal{U} = \sum_{f=0}^{N-1} c(f) Z^{-f} \otimes Z^{-f}. \tag{24}$$

The method of proof of Theorem 4 can be used to show the equivalence of (24) with $\mathcal{U} = \sum_{k=0}^{N-1} |k\rangle\langle k| \otimes Z^k$, which in turn is locally equivalent to the N-dimensional CNOT gate of Example 1.

Example 7.

The unitary

$$\mathcal{U} = \frac{1}{2\sqrt{2}}(I\otimes I + X\otimes X + \zeta Z\otimes Z + \zeta^5 XZ\otimes XZ + \zeta^3 I\otimes I + \zeta^7 X\otimes X + \zeta^2 Z\otimes Z + \zeta^2 XZ\otimes XZ), \tag{25}$$

of Schmidt rank 4 on two qubits, where $\zeta = e^{i\pi/4}$ and the operators are the same as in Example 5, employs an unfaithful (each operator, e.g. $X\otimes X$, appears twice in the sum) representation of the Abelian group $C_2\times C_2\times C_2$, with the eight coefficients being the corresponding $c(f)$. It can be verified that this $\{c(f)\}$ set satisfies the requirements for the fast protocol. As this group is of order 8 the protocol requires a resource of 3 ebits, and we have not found any fast protocol which can implement this unitary using less entanglement. It corresponds to $\alpha = \pi/4, \beta = \pi/8, \gamma = 0$ in (21) (the B gate of [23]).

Example 8.

For any given integer $n \geq 2$, let $U(f) = V(f)$ $(0 \leq f \leq 2n-1)$ be the 2×2 matrices

$$0 \leq f \leq n-1: \begin{pmatrix} \cos(2f\pi/n) & -\sin(2f\pi/n) \\ \sin(2f\pi/n) & \cos(2f\pi/n) \end{pmatrix},$$
$$n \leq f \leq 2n-1: \begin{pmatrix} -\cos(2f\pi/n) & -\sin(2f\pi/n) \\ -\sin(2f\pi/n) & \cos(2f\pi/n) \end{pmatrix}. \tag{26}$$

They form an irreducible ordinary representation of the dihedral group D_n of order $N = 2n$, where the first kind in (26) correspond to rotations and the second kind to reflections. Let

$$c(f) = \begin{cases} (\epsilon(f)/\sqrt{2n})\exp[\,i\pi m f^2/n\,], & n \text{ even}, \\ (\epsilon(f)/\sqrt{2n})\exp[\,i\pi m f(f+1)/n\,], & n \text{ odd}, \end{cases} \tag{27}$$

where m is any positive integer coprime with n, and $\epsilon(f)$ is 1 for $0 \leq f \leq n-1$ and i for $f \geq n$. It can be verified that these $\{c(f)\}$ sets satisfy the requirements for the fast protocol. The two-qubit unitary constructed in this way is locally equivalent to (21) with $\alpha = \pi/4$, $\gamma = 0$, and β, which necessarily lies in the interval $[0, \pi/4]$, depending on m and n in a manner we have not studied in detail. It may be that the possible set of β values is dense in $[0, \pi/4]$.

D. Relationship to controlled-Abelian-group unitaries

The following theorem, proved in Appendix C, shows that the family of unitaries for which fast protocols were constructed in Sec. II can also be realized using our fast protocol for double-group unitaries. The converse is not true, since, for instance, the 2-qubit SWAP gate in Example 5 cannot be realized as a controlled-Abelian-group unitary, as it is of Schmidt rank 4, while a controlled unitary on 2 qubits cannot have Schmidt rank greater than 2.

Theorem 4. *Let $\mathcal{U}$ be a controlled-Abelian-group unitary of the form* (1)*, where the V_k are a subset of an ordinary representation of an Abelian group G of order N. Then $\mathcal{U}$ is equivalent under local unitaries to*

$$\mathcal{W} = \sum_{f=0}^{N-1} c(f) Q(f) \otimes R(f), \tag{28}$$

where the $c(f)$ are complex coefficients, the $Q(f)$ are linear combinations of P_k's, and $\{Q(f)\}$, $\{R(f)\}$, $\{Q(f)\otimes R(f)\}$ are all ordinary representations of the group G. In addition the $c(f)$ can be chosen to satisfy the requirements for the fast protocol as given in Sec. III B. Hence all controlled-Abelian-group unitaries of the form discussed in Sec. II can be implemented by our fast double-group unitary protocol, without using more entanglement.

IV. CONCLUSIONS

Any nonlocal unitary can be carried out deterministically by means of local operations and classical communication provided an appropriate entangled resource is available. However, teleportation and various more efficient schemes typically require two rounds of classical communication, and hence the minimum total amount of time required to complete the protocol is twice the time required for one-way communication. In certain cases there are fast protocols in which the minimum total time is only half as long, and in this paper we have discussed two protocols for fast bipartite unitaries. The first is shown in Fig. 2: it carries out a controlled-Abelian-group unitary of the form (1), including cases in which only a subset of the collection $\{V_k\}$ that form an Abelian group

appear in the sum. The second, shown in Fig. 4, will carry out a double-group unitary of the form (9), provided the coefficients $c(f)$ satisfy appropriate conditions. We have shown, Sec. III D, that unitaries which can be carried out by the first protocol can also be carried out by the second, though the converse is not true, e.g., Example 5. We have constructed some examples for both protocols.

Note, however, that we have not been able to answer the fundamental question as to precisely *which* unitaries can be carried out *exactly* using a fast protocol and a fixed entanglement resource specified in advance. We do not know the answer even for fast protocols of the two types considered in this paper. Finding examples for our double-group protocol is not at all trivial; see the discussion in Sec. III B. In Sec. II C we discussed cases in which subsets of a group can be used to carry out a fast controlled unitary protocol at the cost of greater entanglement. See in particular Example 3, where we showed that any unitary in a particular continuous family can be approximated arbitrarily closely by a unitary implementable by a deterministic fast protocol, provided one is willing to use up enough entanglement. This is similar in spirit to the results in [11] and [14]. Their protocols may need less or more entanglement than our protocols, depending on the form of the unitary. In certain situations, e.g., Example 5, our protocol uses the minimum possible entanglement. It would be nice if these issues could be clarified in terms of some basic principle(s) of quantum information theory.

Another question we have not been able to answer is whether unitaries of the more general form $\sum_f U(f) \otimes W(f)$, where the $U(f)$ form an ordinary or projective representation of a group, but $W(f)$ need not do so, can be carried out by means of a fast protocol. A slow protocol was found in our earlier work [3], and we have constructed a fast version for that protocol, but it seems to only work for those unitaries implementable by our fast double-group protocol of Sec. III. Again, this may reflect some fundamental principle of quantum information, but if so we have not been able to identify it.

V. ACKNOWLEDGMENTS

We thank Serge Fehr, Hoi Kwan Lau and Shiang Yong Looi for helpful discussions, including those on the connections of this work with the topics of instantaneous measurement and position-based quantum cryptography. Patrick Coles read some of the appendices and made helpful suggestions. This work has been supported in part by the National Science Foundation through Grants PHY-0456951 and PHY-0757251. SMC has also been supported by a grant from the Research Corporation.

Appendix A: General considerations in protocols

In this section, we consider implementation of $\mathcal{U}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ using a different $\mathcal{U}'$ and use these ideas below to show that consideration of controlled-unitaries can be restricted to those with rank-1 projectors. A scheme is shown in Fig. 5, which is valid for both the fast and slow protocols. If the protocol for $\mathcal{U}'$ is fast, then the whole protocol is fast.

The circuit in Fig. 5 can be used for the following two situations, to be discussed in detail in the two subsections below. The first situation, called "extension", is that we extend the space of $\mathcal{H}_A$ to $\mathcal{H}_{E'}$, and the unitary $\mathcal{U}' : \mathcal{H}_{E'} \otimes \mathcal{H}_B \to \mathcal{H}_{E'} \otimes \mathcal{H}_B$ is an extension of $\mathcal{U}$, where $\mathcal{U}$ is any unitary on $\mathcal{H}_A \otimes \mathcal{H}_B$. The second situation, called "compression with extension", is only for general controlled unitaries $\mathcal{U}$ of the form (1). The protocol replaces the higher-rank projectors on $\mathcal{H}_A$ in $\mathcal{U}$ with rank-one projectors on $\mathcal{H}_{E'}$ in $\mathcal{U}'$, while adding more projectors if needed. Applications are found in Sec. II. Note that while Fig. 5 shows an extension (and compression in the case of controlled unitaries) on the A side, one can just as well do this on the B side, or both sides.

The input state for the whole protocol is any state on AB together with some fixed state on the ancilla E denoted by $|0\rangle_E$. The map $S : \mathcal{H}_A \otimes \mathcal{H}_E \to \mathcal{H}_{A'} \otimes \mathcal{H}_{E'}$ is unitary, and $S^\dagger$ is its inverse. The unitary S obviously has its input dimension equal to its output dimension: $d_A d_E = d_{A'} d_{E'}$, where $d_{E'}$ is determined by $\mathcal{U}'$, see below, d_A may be unequal to $d_{A'}$, and d_E may be unequal to $d_{E'}$.

1. Extending the Hilbert space in protocols

Here we consider the first type of extension, where $\mathcal{U}'$ is the direct sum of $\mathcal{U}_0$ (the same as $\mathcal{U}$ but on a different space) and another unitary $\mathcal{R}$. Dimension $d_{E'}$ is fixed by $\mathcal{U}'$ and is greater than d_A. One can always choose d_E to be equal to $d_{E'}$, but in general may choose d_E to be less than $d_{E'}$. The action of the unitary S on the actual input space is determined by the following equation:

$$S(|k\rangle_A \otimes |0\rangle_E) = |0\rangle_{A'} \otimes |k\rangle_{E'}, \;\; k = 0, 1, \cdots, d_A - 1, \tag{A1}$$

where $\{|k\rangle_A\}$ is an orthonormal basis of $\mathcal{H}_A$. The requirements for S in this equation can be extended to a full definition of a unitary. The effect of S is to transfer Alice's input state into $\mathcal{H}_{E'}$. Define $\mathcal{H}_{\bar{A}}$ to be the span of $\{|k\rangle_{E'} : 0 \le k \le d_A - 1\}$. Then $\mathcal{H}_{E'} = \mathcal{H}_{\bar{A}} \oplus \mathcal{H}_R$, where $\mathcal{H}_R$ is a space orthogonal to $\mathcal{H}_{\bar{A}}$. Then the correct form of $\mathcal{U}'$ should be $\mathcal{U}' = \mathcal{U}_0 \oplus \mathcal{R}$, where $\mathcal{U}_0 : \mathcal{H}_{\bar{A}} \otimes \mathcal{H}_B \to \mathcal{H}_{\bar{A}} \otimes \mathcal{H}_B$ is the same as the original unitary $\mathcal{U}$ except it is on a different space, and $\mathcal{R} : \mathcal{H}_R \otimes \mathcal{H}_B \to \mathcal{H}_R \otimes \mathcal{H}_B$ is an arbitrary unitary.

Now we prove that the circuit defined in Fig. 5 applied to $|0\rangle_E \otimes |\psi\rangle_{AB}$ yields $|0\rangle_E \otimes \mathcal{U}|\psi\rangle_{AB}$.

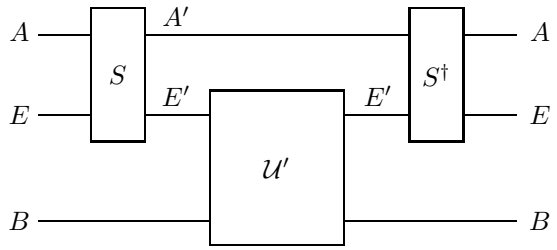

FIG. 5. A scheme for implementing $\mathcal{U}$ using a protocol for $\mathcal{U}'$.

Proof. Suppose the input state on $\mathcal{H}_{AB}$ is $|\psi\rangle_{AB} = |k\rangle_A|q\rangle_B$. Then

$$\begin{aligned}
|k\rangle_A|0\rangle_E|q\rangle_B &\xrightarrow{S} |0\rangle_{A'}|k\rangle_{E'}|q\rangle_B \\
&\xrightarrow{\mathcal{U}'} |0\rangle_{A'}\otimes\mathcal{U}'(|k\rangle_{E'}|q\rangle_B) \\
&= |0\rangle_{A'}\otimes\mathcal{U}(|k\rangle_{E'}|q\rangle_B) \\
&= |0\rangle_{A'}\otimes\sum_{j=0}^{d_A-1}\sum_{p=0}^{d_B-1}\langle jp|\mathcal{U}|kq\rangle|j\rangle_{E'}|p\rangle_B \\
&\xrightarrow{S^\dagger} |0\rangle_E\otimes\sum_{j=0}^{d_A-1}\sum_{p=0}^{d_B-1}\langle jp|\mathcal{U}|kq\rangle|j\rangle_A|p\rangle_B \\
&= |0\rangle_E\otimes\mathcal{U}(|k\rangle_A|q\rangle_B) \qquad \text{(A2)}
\end{aligned}$$

The argument can be extended by linearity to superpositions of the states $|k\rangle_A|q\rangle_B$. □

As a side remark, the derivations above should still work if we replace the unitary S by an isometry $\mathcal{V} = S|0\rangle_E$, replace $S^\dagger$ by $\mathcal{V}^\dagger$, and remove system E from the circuit in Fig. 5. It can be verified that the overall operation of the circuit is $(\mathcal{V}^\dagger\otimes I_B)(I_{A'}\otimes\mathcal{U}')(\mathcal{V}\otimes I_B) = \mathcal{U}$. We chose to present the argument using the unitary S rather than the isometry $\mathcal{V}$ in order to show that the scheme has no trouble finding an experimental implementation. The same remark also applies to the next subsection.

The current extension technique was useful in finding the protocols in Secs. II C and the Example 8 in III C, but it turns out that those protocols (for the particular types of unitaries) can be simplified such that no extension is needed, which is why we have not explicitly mentioned this idea of extension in those sections.

2. Controlled unitaries: Conversion of higher rank projectors into rank-one projectors

For general controlled unitaries $\mathcal{U}$ of the form (1) (not limited to those implementable by the fast protocols in this paper), we now consider a procedure that compresses the higher-rank projectors on $\mathcal{H}_A$ into rank-one-projectors on $\mathcal{H}_{E'}$, while adding more projectors if needed. The form of $\mathcal{U}'$ is

$$\mathcal{U}' = \sum_{k=0}^{N'-1}|k\rangle\langle k|_{E'}\otimes V_k \qquad \text{(A3)}$$

where $N' \geq N$. Apparently $d_{E'} = N'$.

The steps of the protocol are similar to those in Appendix A 1, but with the following change to the requirements on S (and accordingly $S^\dagger$):

$$S(|k,r\rangle_A\otimes|0\rangle_E) = |r\rangle_{A'}\otimes|k\rangle_{E'}, \qquad \text{(A4)}$$

where (k,r) is the label for the states in a specific basis of $\mathcal{H}_A$, with k ($0\leq k\leq N-1$) labeling which projector P_k, and $r\in\{0,1,\cdots,\text{rank}(P_k)-1\}$ labeling which basis state in the support of P_k. Note the range of r depends on k, and because of this, $d_{A'}$ should be at least the maximum rank among the P_k's ($0\leq k\leq N-1$), while satisfying $d_Ad_E = d_{A'}d_{E'}$. The requirements for S in (A4) can be extended to a full definition of a unitary. The effect of S is to transfer the information about "which k" into $\mathcal{H}_{E'}$, and that information is used in the controlled unitary $\mathcal{U}'$, and then transferred back to $\mathcal{H}_A$ by $S^\dagger$.

The final state of the protocol is $|0\rangle_E\otimes\mathcal{U}|\psi\rangle_{AB}$, and the proof for the correctness of the protocol is similar to that in Appendix A 1:

Proof. Suppose the input state on $\mathcal{H}_{AB}$ is $|\psi\rangle_{AB} = |k,r\rangle_A|q\rangle_B$. Then

$$\begin{aligned}
|k,r\rangle_A|0\rangle_E|q\rangle_B &\xrightarrow{S} |r\rangle_{A'}|k\rangle_{E'}|q\rangle_B \\
&\xrightarrow{\mathcal{U}'} |r\rangle_{A'}\otimes\mathcal{U}'(|k\rangle_{E'}|q\rangle_B) \\
&= |r\rangle_{A'}\otimes|k\rangle_{E'}\otimes V_k|q\rangle_B) \\
&\xrightarrow{S^\dagger} |0\rangle_E\otimes|k,r\rangle_A\otimes V_k|q\rangle_B \\
&= |0\rangle_E\otimes\mathcal{U}(|k,r\rangle_A|q\rangle_B) \qquad \text{(A5)}
\end{aligned}$$

The argument can be extended by linearity to superpositions of the states $|k,r\rangle_A|q\rangle_B$. □

As noted above, for the current subsection it is also plausible to replace the unitary S by an isometry $\mathcal{V} = S|0\rangle_E = \sum_k\sum_r|r\rangle_{A'}|k\rangle_{E'}\langle k,r|_A$, replace $S^\dagger$ by $\mathcal{V}^\dagger$, and remove system E from the circuit in Fig. 5. Using the

definition of $\mathcal{U}'$ in (A3), it can be verified that the overall operation of the circuit is $(\mathcal{V}^\dagger \otimes I_B)(I_{A'} \otimes \mathcal{U}')(\mathcal{V} \otimes I_B) = \mathcal{U}$, where $\mathcal{U}$ is of the form (1).

Appendix B: Proofs of Theorems 1, 2, 3

Proof of Theorem 1.

(a) We need to show, see (14) and note that both D and Z_l are diagonal matrices, that

$$\begin{aligned}\tilde{P}_l = CZ_lC^\dagger &= (1/N)M\hat{K}DZ_lD^\dagger\hat{K}^\dagger M^\dagger \\ &= (1/N)M\hat{K}Z_l\hat{K}^\dagger M^\dagger \end{aligned} \tag{B1}$$

is a complex permutation matrix. The diagonal elements of Z_l are complex conjugates of the elements in a row of $\hat{T}$ and thus, (15), equal to a common phase factor times those in a particular row, say row m, of the character table $\hat{K}$; recall that the complex conjugate of a row in $\hat{K}$ is always another row of $\hat{K}$. Now the matrix $\hat{K}Z_l$ is the matrix $\hat{K}$ with each column multiplied by the corresponding diagonal element of Z_l. Thus the j-th row of $\hat{K}Z_l$ is the element-wise product of row j of $\hat{K}$ with row m of $\hat{K}$, up to an overall phase that depends on j. But since the rows of $\hat{K}$ form a group under element-wise products, this means that $\hat{K}Z_l = Q_l\hat{K}$ for a suitable complex permutation matrix Q_l. Since $\hat{K}\hat{K}^\dagger = NI$, (B1) tells us that $\tilde{P}_l = MQ_lM^\dagger$, and because M, Q_l, and $M^\dagger$ are all complex permutation matrices, so is $\tilde{P}_l$.

(b) The rows of $\hat{T}$ are the elements of a group H in the following sense. The element-wise product of any two rows is, up to a phase, a third row, and the fact that the rows are linearly independent means that this third row is uniquely determined. That is, there is a well-defined associative group multiplication, which is commutative, so the group H is Abelian. There is necessarily one row consisting of identical elements; this is the identity element of H. Given any row, there is another row which is, element by element, its complex conjugate, up to a single phase for the whole row; these two rows are inverses of each other. Hence the group H is well-defined. Obviously, each column of $\hat{T}$ consists of elements (viewed as 1×1 matrices) that form an irreducible representation of H under the multiplication of complex numbers, and all the elements of $\hat{T}$ are of magnitude 1.

Divide each row by its first element to form the matrix $\hat{T}'$, whose rows again form the group H, but now without additional phases since the first element of each row is 1. Since the rows of $\hat{T}$ are linearly independent, so are the rows of $\hat{T}'$, and hence also its columns. Thus each column of $\hat{T}'$ forms a distinct irreducible representation of the group H. All the N distinct irreducible representations of H are included in the columns of $\hat{T}'$, thus $\hat{T}'$ is the transpose of a character table of the Abelian group H, and such a transpose is itself a character table of H (see the discussion preceding Theorem 1). Hence we can identify $\hat{T}'$ as the $\hat{K}$ in (15), and the phases used to change $\hat{T}$ to $\hat{T}'$ can be included in the matrix L in (15). □

Proof of Theorem 2.

Let $\hat{C} = \sqrt{N}C$ and rewrite (14) in the equivalent form

$$\hat{C}Z_l = \tilde{P}_l\hat{C}. \tag{B2}$$

The matrix on the left is obtained from $\hat{C}$ by multiplying each column by the corresponding diagonal element of Z_l, while the one on the right is obtained by some permutation of the rows of $\hat{C}$, with an additional overall phase for each row. Consider the special case in which the first row of $\hat{C}$ consists of 1's. Then the first row of $\hat{C}Z_l$ is $\breve{Z}_l$, the row vector whose elements are the diagonal elements of Z_l, and according to (B2), it is equal to the first row of $\tilde{P}_l\hat{C}$, i.e., a phase times some other row of $\hat{C}$. As the $\breve{Z}_l$ are linearly independent (they are complex conjugates of the rows of the Hadamard matrix $\hat{T}$), it follows by equating, for each l, the first row on the left side of (B2) with that on the right side, that the element-wise product of the first row of $\hat{C}$ and the $\breve{Z}_l$ for all possible values of l generates all the rows of $\hat{C}$ up to a phase, i.e., each row of $\hat{C}$ is a phase times one of the $\breve{Z}_l$. Then according to (B2), the element-wise product of any row of $\hat{C}$ with any $\breve{Z}_l$, i.e. the element-wise product of any two rows of $\hat{C}$ up to a phase, is always a third row of $\hat{C}$ up to a phase. Similarly the product of any two of the matrices in the set $\{Z_l\}$ is a third, up to a phase; this is an associative group product. The first row of $\hat{C}$ is equal to one of the $\breve{Z}_l$ up to a phase, and this Z_l corresponds to the group identity. Because the first row of $\hat{C}$ consists of 1's, there is a row of $\tilde{P}_l\hat{C}$, say row m, which consists of equal elements. Then the m-th row of $\hat{C}$, see (B2), identifies the group inverse of Z_l. Thus the Z_l under matrix products form a group (denoted by H) up to phases. For any Z_l, its complex conjugate Z_l^* is the matrix inverse of Z_l, and hence some $Z_{l'}$ up to a phase. Consequently all the different rows of $\hat{T}$, the complex conjugates of $\breve{Z}_l$, are equal to the different $\breve{Z}_{l'}$ up to phases and a permutation of the ordering, hence these rows form the group H up to phases under element-wise multiplication. Then according to Theorem 1(b), H must be Abelian, and $\hat{T}$ is of the form given in (15). Since the rows of $\hat{T}$ are a permutation of the different $\breve{Z}_{l'}$ up to phases, they are also a permutation of the rows of $\hat{C}$ up to phases. Thus $\hat{C}$ is of the form (15) with $D = I$. Hence for the special case under consideration, (15) is satisfied, and then (16) follows from (15).

Next consider the more general case in which the elements of the first row of $\hat{C}$ are all nonzero. Form $\hat{C}'$ from $\hat{C}$ by dividing every column of $\hat{C}$ by the corresponding element on the first row. This means that $\hat{C}' = \hat{C}Q$, where Q is a diagonal matrix. Since Q commutes with every Z_l, we can replace $\hat{C}$ on both sides of (B2) with $\hat{C}'$. As the first row of $\hat{C}'$ consists of 1's, the argument given above shows that the $\{Z_l\}$ form an Abelian group up to phases, and the rows of $\hat{C}'$ are, up to phases, some

permutation of the rows of $\hat{T}$, and $\hat{T}$ is of the form given in (15), again according to Theorem 1(b). Thus the different columns of $\hat{C}'$ all have the same normalization, and since the same is true of $\hat{C}$, as C is assumed to be a unitary matrix, it follows that the diagonal elements of Q all have magnitude 1, and one can set $D = Q^{-1}$ in (15). Then (16) follows from (15). □

Proof of Theorem 3.

The coefficients $c(f)$ must all be of the same magnitude, $1/\sqrt{N}$, see the remark following Theorem 1, and without loss of generality γ can be chosen such that $c(e) = 1/\sqrt{N}$ in (20), where e is the group identity. First consider the case that $\{\Gamma(f)\}$ is an ordinary representation of G, so that $\lambda(g,h) = 1$. Choose any group element $r \neq e$ and assume it has order p, which means that p divides N and $r^p = e$. The first row of C, corresponding to $g = e$ in (13), contains $c(e), c(r), c(r^2), \cdots, c(r^{p-1})$ in some order, interspersed with other coefficients $c(f)$. Now consider the row of C corresponding to $g = r^{p-1} = r^{-1}$ in (13). It is related to the first row as indicated here,

$$\begin{pmatrix} c(e) & c(r) & c(r^2) & \cdots & c(r^{p-1}) & \cdots \\ c(r) & c(r^2) & \cdots & c(r^{p-1}) & c(e) & \cdots \end{pmatrix}, \qquad \text{(B3)}$$

where only the relevant columns are shown, rearranged in a convenient order.

Let us define the $\hat{C}'$ matrix, as in the first paragraph of Sec. III B, to be the one obtained from $\hat{C} = \sqrt{N}\, C$ by multiplying each row and each column by some phase, so that all the elements in the first row and first column are equal to 1. This is a character table, so every element is an N-th root of 1. Equivalently, $\hat{C}'$ is obtained from C by dividing each column of C by the corresponding element in the first row, and then in the resulting matrix dividing each row by its first element. Consequently, applying this process to the rows and columns shown in (B3), we conclude that

$$\frac{c(r^2)}{c(r)^2} = \phi_1\sqrt{N}, \quad \frac{c(r^3)}{c(r)c(r^2)} = \phi_2\sqrt{N}, \quad \ldots, \quad \frac{c(e)}{c(r)c(r^{p-1})} = \phi_{p-1}\sqrt{N}, \qquad \text{(B4)}$$

where each ϕ_j is an N-th root of 1. The product of these $p-1$ equations,

$$c(e)/[c(r)]^p = \phi_1\phi_2\cdots\phi_{p-1}(\sqrt{N})^{p-1}, \qquad \text{(B5)}$$

implies, since $c(e) = 1/\sqrt{N}$, that $\sqrt{N}\, c(r)$ must be a p-th root of a number which is itself an N-th root of 1, and because p divides N, $c(r)$ is of the form (20). This completes the argument for an ordinary representation.

When the $\{\Gamma(r)\}$ form a projective representation of G with a standard factor system (11), the first row in (B3) is the same, but the second row will be multiplied by appropriate factors $\lambda(g,h)$. Since we are assuming a normalized factor system, all these additional factors are themselves N-th roots of 1, so (B4) still holds for ϕ_j which are N-th roots of 1, and the rest of the argument is the same as before. □

Appendix C: Proof of Theorem 4

In this appendix, we prove Theorem 4, which says that the controlled unitary $\mathcal{U} = \sum_{k=0}^{N-1} P_k^A \otimes V_k^B$ given by (1), where P_k^A are orthogonal projectors, and $\{V_k^B\}$ form a subset of an ordinary representation of an Abelian group G, is equivalent to

$$\mathcal{W} = \sum_{f=0}^{N-1} c(f) Q(f) \otimes R(f) \qquad \text{(C1)}$$

under local unitaries, where $c(f)$ are complex coefficients (will be defined in (C3)), and $Q(f)$ are linear combinations of P_k^A, and $\{Q(f) \otimes R(f)\}$ is an ordinary representation of G. In addition, the $c(f)$ can be chosen to satisfy the requirements for the fast protocol, hence all controlled-Abelian-group unitaries can be implemented by the fast double-group unitary protocol.

We first prove the case that $\{V_k^B\}$ form a whole representation, not a subset, and at the end we will remark that the proof also works in the "subset" case. The proof is by explicitly constructing a $\mathcal{W}$ and showing that it is equivalent to $\mathcal{U}$ under local unitaries. Any Abelian group is a direct sum of cyclic groups, so $G = C_{r_1} \oplus C_{r_2} \oplus \cdots \oplus C_{r_\eta}$, where $\eta \geq 1$, and r_i is the order of the cyclic group C_{r_i}. Then $N = |G| = \prod_{i=1}^{\eta} r_i$. The group element k is relabeled by a vector $k = (k_1, k_2, \cdots, k_\eta)$, where $0 \leq k_i \leq r_i - 1$. We use the convention that k is the sequential numbering (starting from 0) for the vectors in lexicographical order, so that $k = 0$ corresponds to $(0, 0, \cdots, 0)$, and $k = 1$ corresponds to $(0, 0, \cdots, 1)$, etc. Suppose $\{V_k^B\}$ has been diagonalized under a suitable unitary similarity transform, then $\{V_k^B\}$ is the direct sum of some irreducible representations (possibly with redundancy). All possible irreducible representations of G are one-dimensional, and have the form

$$R^q(k) = \prod_{s=1}^{\eta} \exp(2\pi i q_s k_s / r_s), \qquad \text{(C2)}$$

where $q = (q_1, q_2, \cdots, q_\eta)$ is the label for irreducible representations (some may be missing from $\{V_k^B\}$, but we still include them in this labeling scheme for convenience). Denote the computational basis of $\mathcal{H}_B$ by $\{|b\rangle\}$, $b = 0, 1, \cdots, d_B - 1$, then the b-th diagonal elements in V_k^B determine an irreducible representation labeled by q_b, $0 \leq q_b \leq N-1$. The q_b can be written in the vector form (see (C2) and the sentence after that), and the components in the vector q_b will be denoted by $q_{b,s}$.

As discussed above, for every $f \in G$ we can represent f using a set of integers: $f = (f_1, f_2, \cdots, f_\eta)$, with

group multiplication corresponding to vector addition (modulo r_s for the s-th element of the vector). Define $c(f)=\prod_{s=1}^{\eta} c_s(f_s)$, where $c_s(f_s)$ is defined by (basically the same as in Example 6)

$$c_s(f_s)=\frac{1}{\sqrt{r_s}}\exp[-\pi i f_s(r_s \bmod 2+f_s)/r_s], \qquad f_s=0,1,\cdots,r_s-1. \tag{C3}$$

We choose the $Q(f)$ to be

$$Q(f)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\left[\prod_{s=1}^{\eta}\exp(-2\pi i f_s k_s/r_s)\right]P_k^A, \tag{C4}$$

where (k_s) is the vector labeling for k. Define $R(f)$ as

$$R(f)=\frac{1}{\sqrt{N}}\sum_{b=0}^{d_B-1}\left[\prod_{s=1}^{\eta}\exp(-2\pi i f_s q_{b,s}/r_s)\right]|b\rangle\langle b|, \tag{C5}$$

where $q_{b,s}$ are the components in the vector labeling for q_b. It is not hard to verify that $\{Q(f)\otimes R(f)\}$ is an ordinary representation of G, and the coefficients $c(f)$ form a unitary C matrix of the type (13), hence $\mathcal{W}$ is unitary.

With the above choices of $Q(f)$ and $R(f)$,

$$\mathcal{W}|k\rangle|b\rangle=\frac{1}{\sqrt{N}}\sum_{f=0}^{N-1}\left(\prod_{s=1}^{\eta}\exp[-\pi i f_s(r_s \bmod 2+f_s+2k_s+2q_{b,s})/r_s]\right)|k\rangle|b\rangle, \tag{C6}$$

where $0\le k\le N-1,\ 0\le b\le d_B-1$, and $|k\rangle$ is any eigenstate of P_k^A. Denote the phase factor in front of $|k\rangle|b\rangle$ in the above equation by ζ_{kb}, then

$$\begin{aligned}\zeta_{kb}&=\frac{1}{\sqrt{N}}\prod_{s=1}^{\eta}\sum_{j=0}^{r_s-1}\exp\left(\pi i\{-[j+k_s+q_{b,s}+(r_s \bmod 2)/2]^2+[k_s+q_{b,s}+(r_s \bmod 2)/2]^2\}/r_s\right)\\&=\frac{1}{\sqrt{N}}\prod_{s=1}^{\eta}\left[\left(\sum_{j=0}^{r_s-1}\exp\{-\pi i[j+k_s+q_{b,s}+(r_s \bmod 2)/2]^2/r_s\}\right)\exp\{\pi i[k_s+q_{b,s}+(r_s \bmod 2)/2]^2/r_s\}\right]\\&=\frac{\alpha}{\sqrt{N}}\prod_{s=1}^{\eta}\exp\{\pi i[k_s+q_{b,s}+(r_s \bmod 2)/2]^2/r_s\}\end{aligned} \tag{C7}$$

where α is a constant independent of k and q. In deriving the last line above, we have used $(r+j)^2\equiv j^2 (\mathrm{mod}\ 2r)$ for even r, and $(r+j+1/2)^2\equiv(j+1/2)^2 (\mathrm{mod}\ 2r)$ for odd r, which make the substitution $j+k_s+q_{b,s}\to j$ possible, and obtained $\alpha=\prod_{s=1}^{\eta}\alpha_s$, where $\alpha_s=\sum_{j=0}^{r_s-1}\exp\{-\pi i[j+(r_s \bmod 2)/2]^2/r_s\}$.

Define the local operators M_A and M_B on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively as follows:

$$M_A=\sum_{k=0}^{N-1}\zeta_{k0}^{-1}P_k^A, \qquad M_B=\zeta_{00}\sum_{b=0}^{d_B-1}\zeta_{0b}^{-1}|b\rangle\langle b|, \tag{C8}$$

From the unitarity of $\mathcal{W}$, ζ_{kb} is always a phase factor with magnitude 1, hence M_A and M_B are unitary operators. Then for $|k\rangle$ chosen arbitrarily from the eigenstates of P_k^A, we have

$$\begin{aligned}(M_A\otimes M_B)\mathcal{W}|k\rangle|b\rangle&=(M_A\otimes M_B)\zeta_{kb}|k\rangle|b\rangle\\&=\zeta_{00}\zeta_{kb}\zeta_{k0}^{-1}\zeta_{0b}^{-1}|k\rangle|b\rangle\\&=\left[\prod_{s=1}^{\eta}\exp(2\pi i k_s q_{b,s}/r_s)\right]|k\rangle|b\rangle\\&=\sum_{k=0}^{N-1}P_k^A\otimes V_k^B|k\rangle|b\rangle\\&=\mathcal{U}|k\rangle|b\rangle\end{aligned} \tag{C9}$$

where we have used (C7) to derive the third line, and used (C2) to derive the fourth line. Since P_k^A are of finite rank, there exist a finite collection of states of the form $|k\rangle|b\rangle$ to make a complete basis of $\mathcal{H}_{AB}$. The actions of $(M_A\otimes M_B)\mathcal{W}$ and $\mathcal{U}$ are the same on all states in a complete basis, hence they must be identical operators. Therefore $\mathcal{U}$ is equivalent to $\mathcal{W}$ under local unitaries.

Using the algorithm in Sec. III B, it can be verified

that the choice of coefficients $c(f)$ given above (which can be viewed as the choice in Example 6 generalized to the non-cyclic Abelian groups) satisfies the requirements for the fast protocol. Hence the double-group protocol for $\mathcal{W}$ is fast.

The proof above can basically be applied to the case that $\{V_k^B\}$ form a subset of a representation. In general some P_k^A do not occur in the expressions for $Q(f)$ and M_A; those P_k^A can be safely removed because $Q(f)$ and M_A are block-diagonal, where the blocks are determined from the support of the P_k^A's. The coefficients $c(f)$ are still the same as above, so the protocol is still fast. Hence the proof still works. □

[1] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio. Phys. Rev. A **62**, 052317 (2000).

[2] B. Reznik, Y. Aharonov and B. Groisman. Phys. Rev. A **65**, 032312 (2002).

[3] L. Yu, R. B. Griffiths, and S. M. Cohen. Phys. Rev. A **81**, 062315 (2010).

[4] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Phys. Rev. A **59**, 4249 (1999).

[5] A. Yimsiriwattana, S. J. Lomonaco Jr. AMS Contemporary Mathematics, Volume **381**, 131-147 (2005). e-print arXiv:quant-ph/0402148v3.

[6] A. Yimsiriwattana, S. J. Lomonaco Jr. Proc. SPIE **5436**, 360 (2004). e-print arXiv:quant-ph/0403146v2.

[7] R. Van Meter, K. Nemoto, W. J. Munro. IEEE Transactions on Computers, **56**(12), 1643–1653, Dec. 2007. e-print arXiv:quant-ph/0701043v1.

[8] A. Kent, W. J. Munro, T. P. Spiller. Phys. Rev. A **84**, 012326 (2011).

[9] A. Kent, R. Beausoleil, W. Munro and T. Spiller, Tagging Systems US patent US20067075438 (2006).

[10] H. K. Lau, H. K. Lo. Phys. Rev. A **83**, 012322 (2011).

[11] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, C. Schaffner. e-print arXiv:1009.2490v4 [quant-ph]. in *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*, Vol. 6841 (2011) p. 423.

[12] B. Groisman and B. Reznik. Phys. Rev. A **71**, 032322 (2005).

[13] G.-F. Dang and H. Fan. e-print arXiv:0711.3714v2 [quant-ph].

[14] S. Beigi, R. Koenig. e-print arXiv:1101.1065v3 [quant-ph].

[15] L. Vaidman. Phys. Rev. Lett. **90**, 010402 (2003).

[16] B. Groisman and B. Reznik. Phys. Rev. A **66**, 022110 (2002).

[17] S. R. Clark, A. J. Connor, D. Jaksch, S. Popescu. New J. Phys. **12**, 083034 (2010).

[18] J. Tyson, J. Phys. A: Math. Gen. **36**, 10101-10114 (2003).

[19] http://en.wikipedia.org/wiki/Representation_theory_of_finite_groups. Retrieved on 8/24/2011.

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

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

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

[23] J. Zhang, J. Vala, S. Sastry, K. B. Whaley. Phys. Rev. Lett. **93**, 020502 (2004).

[24] Shoon Kyung Kim, *Group Theoretical Methods and Applications to Molecules and Crystals*, Cambridge University Press, 1999.