# All Unitaries Having Operator Schmidt Rank 2 are Controlled Unitaries 

Scott M. Cohen<br>Portland State University<br>Li Yu

# Let us know how access to this document benefits you. 

Follow this and additional works at: http://pdxscholar.library.pdx.edu/phy_fac
Part of the Physics Commons

## Citation Details

Cohen, S. M., \& Li, Y. (2013). All unitaries having operator Schmidt rank 2 are controlled unitaries. Physical Review A: Atomic, Molecular \& Optical Physics, 87(2-A), 022329-1-022329-6.

# All unitaries having operator Schmidt rank 2 are controlled unitaries 

Scott M. Cohen*<br>Department of Physics, Portland State University, Portland, Oregon 97201, USA

Li Yu
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543 (Received 9 December 2012; published 20 February 2013)


#### Abstract

We prove that every unitary acting on any multipartite system and having operator Schmidt rank equal to 2 can be diagonalized by local unitaries. This then implies that every such multipartite unitary is locally equivalent to a controlled unitary with every party but one controlling a set of unitaries on the last party. We also prove that any bipartite unitary of Schmidt rank 2 is locally equivalent to a controlled unitary where either party can be chosen as the control, and at least one party can control with two terms, which implies that each such unitary can be implemented using local operations and classical communication (LOCC) and a maximally entangled state on two qubits. These results hold regardless of the dimensions of the systems on which the unitary acts.


DOI: 10.1103/PhysRevA.87.022329
PACS number(s): 03.67.Ac

## I. INTRODUCTION

Unitary gates are essential for quantum information processing, hence it is important to find simple ways to implement them. In this paper we consider unitaries acting on $P$ systems, where $P \geqslant 2 .{ }^{1}$ Generally, methods for implementing a given unitary are discussed in two different scenarios: local and nonlocal. In the local scenario, the given unitary acting on $P$ systems is decomposed as a product of simpler unitaries, each of which may act on any number of systems. In the nonlocal scenario, many different parties at remote locations could share some ancillary quantum state that may be entangled, and they do local operations and classical communication (LOCC) to implement the desired unitary. This paper is developed for the nonlocal scenario, but it applies to gate decomposition in the local scenario as well; see the remarks in the conclusion.

A common approach is to express unitaries using a sum of product operators:

$$
\begin{equation*}
\mathcal{U}=\sum_{j} A_{j} \otimes B_{j} \otimes C_{j} \otimes \cdots \otimes R_{j} \tag{1}
\end{equation*}
$$

where $A_{j}, B_{j}$, etc. are local operators on the respective parties. A simple expansion would help us find ways to implement $\mathcal{U}$, but to judge what is a simple expansion there are at least two different criteria. The first is to use a numeric measure: for example, the Schmidt rank [1], defined as the smallest possible number of product operators that can be summed to obtain $\mathcal{U}$. The second is to see whether the local operators in the expansion are simple. A set of mutually orthogonal projectors would qualify under this criterion. If the expansion on one party involves only such projectors, then $\mathcal{U}$ is a controlled unitary. Another simple type of local operators is discussed in Ref. [2]. In this paper we find a connection between the two criteria: all Schmidt rank-2 multipartite unitaries are equivalent

[^0]to controlled unitaries under local unitaries. The result of the bipartite case is slightly stronger, see Theorem 6 below. Our result can be viewed as a structure theorem for the class of Schmidt rank-2 nonlocal unitaries. It characterizes what these unitaries are in terms of product-operator expansions. Since we have solved the simplest nontrivial case of Schmidt rank 2, the next goal would be to characterize nonlocal unitaries of higher Schmidt rank. The forms of expansions in Ref. [2] may help toward this goal.

Amongst the various types of nonlocal unitaries, controlled unitaries are in some ways most easily understood. In the bipartite case, they are one of the few classes of unitaries for which their capacity to create entanglement between the parts is relatively well understood [3], and significant progress has been made toward understanding their entanglement cost; that is, the amount of entanglement that is required to implement them without bringing the various parts together in a single laboratory [4,5]. (The result of [5] also applies to some other classes of unitaries not yet completely characterized.) Controlled unitaries also play an important role in quantum information theory, being one constituent in commonly used gate sets that are universal [6] for quantum computation [7], as well as being instrumental in the creation of graph states and cluster states [8], which find wide use in quantum communication protocols [9] and quantum computation.

Perhaps the simplest controlled unitary is the controlled NOT on two qubits $A$ and $B$,

$$
\begin{equation*}
\mathcal{U}_{\mathrm{CNOT}}=|0\rangle_{A}\langle 0| \otimes I^{(B)}+|1\rangle_{A}\langle 1| \otimes \sigma_{x}^{(B)}, \tag{2}
\end{equation*}
$$

where $I^{(B)}$ is the identity operator and $\sigma_{x}^{(B)}=|0\rangle_{B}\langle 1|+$ $|1\rangle_{B}\langle 0|$ is the usual Pauli operator, both acting on system $B$. If system $A$ starts out in the $|0\rangle_{A}$ state, the state of the full $A B$ system is unchanged, whereas if the initial state of $A$ is $|1\rangle_{A}$, that system is unchanged, but the $B$ system is "flipped." This notion is generalized to provide a definition of a controlled unitary, one for which if the input state of one system is a state in a given orthogonal basis, say the standard basis $\left\{|j\rangle_{A}\right\}$ as in the previous example, then that state is unchanged and unitary $W_{j}$ is performed on the remaining system, which may itself
be multipartite,

$$
\begin{equation*}
\mathcal{U}=\sum_{j=1}^{d_{A}}|j\rangle_{A}\langle j| \otimes W_{j} \tag{3}
\end{equation*}
$$

Since it is easy for the controlling party to perform local unitaries on her system both before and after the action of $\mathcal{U}$, we want to allow for this possibility. Then, every unitary $\mathcal{U}$ for which there exist local unitaries $U^{(A)}, V^{(A)}$ such that

$$
\begin{equation*}
\left(U^{(A)} \otimes I^{(B)}\right) \mathcal{U}\left(V^{(A) \dagger} \otimes I^{(B)}\right)=\sum_{j=1}^{d_{A}}|j\rangle_{A}\langle j| \otimes W_{j} \tag{4}
\end{equation*}
$$

will be referred to as "locally equivalent" to a controlled unitary with party $A$ controlling. This definition can be generalized in an obvious way to the case where multiple parties are controlling when $\mathcal{U}$ acts on three or more parties, but we will require that the controlling parties each control locally, such as in

$$
\begin{equation*}
\mathcal{U}=\sum_{j, k}|j\rangle_{A}\langle j| \otimes|k\rangle_{B}\langle k| \otimes W_{j k} . \tag{5}
\end{equation*}
$$

We will refer to a unitary acting on $P$ parties as "fully controlled" if $P-1$ of the parties can act as controls. Our main result is the following theorem:

Theorem 1. Every nonlocal unitary having Schmidt rank equal to 2 is locally equivalent to (i) a fully controlled unitary, and to (ii) a diagonal unitary.

Note that (i) and (ii) are generally inequivalent without the Schmidt rank-2 assumption. The statement (ii) implies (i) with complete generality according to Lemma 2 below, but not the other way around. For the special case of two qubits, however, (i) and (ii) are each equivalent to the unitary having Schmidt rank 2, and therefore are equivalent to each other. The result (i) for two qubits was previously obtained in Ref. [10].

In the next section, we provide a series of results that are then used in Sec. II B to prove Theorem 1. Then, in Sec. III and for a unitary of any Schmidt rank operating on any number of parties, we provide a sufficient condition for when that unitary is locally equivalent to a controlled unitary, a condition that also tells us which party or parties can act as a control.

## II. MAIN RESULTS

In this section we prove the result that every nonlocal unitary of Schmidt rank equal to 2 is locally equivalent to a controlled unitary. We start out by proving a series of results that are then used to prove our main theorem.

## A. Preliminaries

We begin with the following lemma:
Lemma 2. A nonlocal unitary $\mathcal{U}=\sum_{j} A_{j} \otimes B_{j}$, here written in a Schmidt expansion across the $A \mid B$ cut with $B$ itself possibly a multipartite system, is locally equivalent to a controlled unitary with party $A$ controlling if and only if the set of operators $\left\{A_{j}\right\}$ has a simultaneous singular value decomposition.

Proof. By saying that a set of operators $\left\{A_{j}\right\}$ has a "simultaneous singular value decomposition," we mean every operator in that set can be diagonalized by the same pair
of unitaries, $U^{(A)}$ and $V^{(A)}$. In other words, $U^{(A)} A_{j} V^{(A) \dagger}$ is diagonal for every $j$. To prove the "if" part of this lemma, write $U^{(A)} A_{j} V^{(A) \dagger}=\sum_{k=1}^{d_{A}} a_{j k}|k\rangle_{A}\langle k|$, from which we have that

$$
\begin{align*}
& \left(U^{(A)} \otimes I^{(B)}\right) \mathcal{U}\left(V^{(A) \dagger} \otimes I^{(B)}\right) \\
& \quad=\sum_{j} U^{(A)} A_{j} V^{(A) \dagger} \otimes B_{j}=\sum_{j} \sum_{k=1}^{d_{A}} a_{j k}|k\rangle_{A}\langle k| \otimes B_{j} \\
& \quad=\sum_{k=1}^{d_{A}}|k\rangle_{A}\langle k| \otimes\left(\sum_{j} a_{j k} B_{j}\right), \tag{6}
\end{align*}
$$

which indeed shows that this is a controlled unitary with $A$ controlling.

To prove the converse, if $\mathcal{U}$ is locally equivalent to a controlled unitary with $A$ controlling, then $\exists U^{(A)}, V^{(A)}$ unitaries such that

$$
\begin{equation*}
\left(U^{(A)} \otimes I^{(B)}\right) \mathcal{U}\left(V^{(A) \dagger} \otimes I^{(B)}\right)=\sum_{k=1}^{d_{A}}|k\rangle_{A}\langle k| \otimes W_{k} \tag{7}
\end{equation*}
$$

If $\mathcal{U}=\sum_{j} A_{j} \otimes B_{j}$ is a Schmidt expansion, then the $\left\{B_{j}\right\}$ satisfy $\operatorname{Tr}\left(B_{l}^{\dagger} B_{j}\right)=\delta_{j l}$, which implies from

$$
\begin{equation*}
\sum_{j} U^{(A)} A_{j} V^{(A) \dagger} \otimes B_{j}=\sum_{k=1}^{d_{A}}|k\rangle_{A}\langle k| \otimes W_{k}, \tag{8}
\end{equation*}
$$

that for each $l$,

$$
\begin{equation*}
U^{(A)} A_{l} V^{(A) \dagger}=\sum_{k=1}^{d_{A}} b_{l k}|k\rangle_{A}\langle k|, \tag{9}
\end{equation*}
$$

where $b_{l k}=\operatorname{Tr}\left(B_{l}^{\dagger} W_{k}\right)$. This completes the proof.
The next lemma will also be useful.
Lemma 3. Given $r$ maps $\left\{R_{i}\right\}$ from input space $\mathcal{H}_{\text {in }}$ to output space $\mathcal{H}_{\text {out }}$ such that the set of $r^{2}$ operators $\left\{R_{i}^{\dagger} R_{j}\right\}$ spans a two-dimensional space containing the identity operator $I$, then there exist unitaries $U, V$ such that $U R_{i} V^{\dagger}$ is diagonal for every $i$.

The proof is given in the Appendix.
We will also use a result from Ref. [11] that tells us when a sum of product operators can be equal to a product operator. This will be of use here, since we will be considering expansions of nonlocal unitary $\mathcal{U}$ in terms of product operators, so that the unitary condition, $I=\mathcal{U}^{i} \mathcal{U}$, will appear as a sum of product operators that is equal to the product operator, $I$.

Theorem 4. [11] Given a set of product operators acting on two parties, $\left\{\mathcal{M}_{k}=M_{k}^{(1)} \otimes M_{k}^{(2)}\right\}_{k=1}^{N}$, if there exists a set of nonzero coefficients, $\left\{c_{k}\right\}$, such that the linear combination $\mathcal{S}=\sum_{k=1}^{N} c_{k} \mathcal{M}_{k}$ has Schmidt rank $r_{s}=1$ and so is also a product operator, then

$$
\begin{equation*}
\delta_{1}+\delta_{2} \leqslant N+1 \tag{10}
\end{equation*}
$$

where $\delta_{\alpha}$ is the dimension of the space spanned by operators $\left\{M_{k}^{(\alpha)}\right\}_{k=1}^{N}$.

The connection between this theorem and Lemma 3 is seen by considering $k$ as the composite index $(i, j)$, and $M_{k}^{(\alpha)}=R_{i}^{(\alpha) \dagger} R_{j}^{(\alpha)}$. Since our aim is to analyze nonlocal unitaries, we will consider the case where $\mathcal{S}$ in this theorem is
the identity operator so that with $\mathcal{U}=\sum_{i} R_{i}^{(1)} \otimes \cdots \otimes R_{i}^{(P)}$, $\left\{\mathcal{M}_{k}\right\}$ provides a product expansion of $\mathcal{U}^{\dagger} \mathcal{U}=I$.

We need one more lemma in order to prove our main theorem. This result is well known, but if the reader is interested in seeing a short proof, it can be found in Ref. [11].

Lemma 5. If operators $\left\{M_{j}^{(\alpha)}\right\}_{j=1}^{N}$ span a space of dimension $\delta_{\alpha}$, then with $M_{j}^{(\beta)} \neq 0 \forall j(\beta \neq \alpha)$, operators $\left\{M_{j}^{(\alpha)} \otimes\right.$ $\left.M_{j}^{(\beta)}\right\}_{j=1}^{N}$ span a space of dimension no less than $\delta_{\alpha}$.

## B. Proof of Theorem 1

The proof of Theorem 1 follows directly from the results of the previous section. A unitary of Schmidt rank 2 acting on $P$ parties can be written

$$
\begin{align*}
\mathcal{U}= & M_{1}^{(1)} \otimes M_{1}^{(2)} \otimes \cdots \otimes M_{1}^{(P)} \\
& +M_{2}^{(1)} \otimes M_{2}^{(2)} \otimes \cdots \otimes M_{2}^{(P)} \tag{11}
\end{align*}
$$

with $M_{j}^{(\alpha)}$ an operator acting on party $\alpha$, and $\mathcal{U}$ will satisfy

$$
\begin{align*}
I & =\mathcal{U}^{\dagger} \mathcal{U} \\
& =\sum_{i, j=1}^{2} M_{i}^{(1)^{\dagger}} M_{j}^{(1)} \otimes M_{i}^{(2)^{\dagger}} M_{j}^{(2)} \otimes \cdots \otimes M_{i}^{(P)^{\dagger}} M_{j}^{(P)} \tag{12}
\end{align*}
$$

Let us first discuss the case that no terms on the right-hand side of Eq. (12) vanish. Then this expression is a sum of four product operators equal to a product operator, so that by Theorem 4, it must be that for any bipartite split $A \mid B$ of the $P$ parties, the spans of the corresponding operators on the two sides satisfy $\delta_{A}+\delta_{B} \leqslant 5$. This implies that no more than one party's set of operators $\left\{M_{i}^{(\alpha)^{\dagger}} M_{j}^{(\alpha)}\right\}$ can span a space of dimension exceeding two. This can be seen as follows: suppose parties $\alpha$ and $\beta$ each have spans of dimension at least three. Consider a bipartite split where party $\alpha$ is in part $A$ and $\beta$ is in part $B$. By Lemma $5, \delta_{A} \geqslant 3$ and $\delta_{B} \geqslant 3$, contradicting the above-stated requirement from Theorem 4 that the sum of these cannot exceed 5. Hence, for all parties but one, the spans have dimension no greater than two. If for a given party $\alpha, \delta_{\alpha}=1$, we must have $M_{1}^{(\alpha)} \propto M_{2}^{(\alpha)}$, and both these operators must be proportional to the same unitary. In this case, party $\alpha$ can just perform that unitary, which is uncorrelated to the actions on the other parties, and party $\alpha$ need not be considered further in the analysis. Then, we can just start over by considering a "reduced" $\mathcal{U}$ that only operates on the remaining parties. Alternatively, one may view party $\alpha$ as controlling, with the unitary that acts on the remaining parties being independent of the input on $\alpha$. If, on the other hand, $\delta_{\alpha}=2$, then by Lemma 3, there exist unitaries $U^{(\alpha)}, V^{(\alpha)}$ acting on party $\alpha$ such that $U^{(\alpha)} M_{1}^{(\alpha)} V^{(\alpha) \dagger}$ and $U^{(\alpha)} M_{2}^{(\alpha)} V^{(\alpha) \dagger}$ are both diagonal, and this is true for every $\alpha$ for which $\delta_{\alpha}=2$. This is seen by partially tracing out all parties but one in Eq. (12), revealing that the spans of operators $\left\{M_{i}^{(\alpha)^{\dagger}} M_{j}^{(\alpha)}\right\}$ contain the identity operator, and then the conditions of Lemma 3 are met for each party having $\delta_{\alpha}=2$. Hence for all parties but one, there exist local unitaries to diagonalize the $M_{j}^{(\alpha)}$ operators on that party. For each such party, there exists a set of orthogonal projectors such that the two diagonalized $M_{j}^{(\alpha)}$ are linear combinations of these projectors; see the proof of Lemma 2. Hence, all
parties but one can act as controls simultaneously; that is, $\mathcal{U}$ is "fully controlled." In the expansion of $\mathcal{U}$ using these projectors on $P-1$ parties, the operators on the remaining party are unitaries, and since $\mathcal{U}$ is of Schmidt rank 2, these unitaries span a space of dimension two. Denote by $V_{1}$ and $V_{2}$ two of these unitaries that form a basis of this space. These become $I$ and $V_{1}^{\dagger} V_{2}$ when $\mathcal{U}$ is multiplied by $V_{1}^{\dagger}$ on that party. Then, $V_{1}^{\dagger} V_{2}$ can be diagonalized under a unitary similarity transform, which does not alter the identity $I$, hence $I$ and $V_{1}^{\dagger} V_{2}$ can be diagonalized simultaneously. Therefore, all the local operators (unitaries) in the expansion of $\mathcal{U}$ on that last party can be simultaneously diagonalized, since they are all linear combinations of $V_{1}$ and $V_{2}$. Therefore $\mathcal{U}$ is locally equivalent to a diagonal unitary. This completes the proof of our main theorem for the case that there are no vanishing terms in Eq. (12).

The remaining case is that some terms in Eq. (12) vanish, which only happens if for one party, say the first, $M_{1}^{(1) \dagger} M_{2}^{(1)}=0=M_{2}^{(1) \dagger} M_{1}^{(1)}$. If the corresponding operator products vanished for more than one party, then with Lemma 5, Eq. (12) could not satisfy Theorem 4. This is because for a bipartite split $A \mid B$ with $A$ including only party 1 and $B$ being all the rest, we have $\delta_{A}=2$ (because $M_{1}^{(1) \dagger} M_{1}^{(1)}$ and $M_{2}^{(1) \dagger} M_{2}^{(1)}$ cannot be proportional to each other while summing to the identity when $M_{1}^{(1) \dagger} M_{2}^{(1)}=0$ ) implying from Theorem 4 that $\delta_{B} \leqslant N+1-\delta_{A}=1$, as $N=2$. Therefore, when $M_{1}^{(1) \dagger} M_{2}^{(1)}=0=M_{2}^{(1) \dagger} M_{1}^{(1)}, M_{j}^{(\alpha)}$ is proportional to a unitary for $j=1,2$ and $\alpha \neq 1$, and

$$
\begin{align*}
\left(I^{(1)}\right. & \left.\otimes M_{1}^{(2) \dagger} \otimes M_{1}^{(3) \dagger} \cdots \otimes M_{1}^{(P) \dagger}\right) \mathcal{U} \\
= & c M_{1}^{(1)} \otimes I^{(2)} \otimes \cdots \otimes I^{(P)} \\
\quad & +M_{2}^{(1)} \otimes M_{1}^{(2) \dagger} M_{2}^{(2)} \otimes \cdots \otimes M_{1}^{(P) \dagger} M_{2}^{(P)} \tag{13}
\end{align*}
$$

for some constant $c$. Since $M_{1}^{(\alpha) \dagger} M_{2}^{(\alpha)}$ is proportional to a unitary for every $\alpha \neq 1$, we can find unitaries $U^{(\alpha)}$ such that $U^{(\alpha)} M_{1}^{(\alpha) \dagger} M_{2}^{(\alpha)} U^{(\alpha) \dagger}$ is diagonal $\forall \alpha \neq 1$. Then, by Lemma 2, all other parties can control the first, and the argument at the end of the last paragraph for $\mathcal{U}$ being locally equivalent to a diagonal unitary still applies, completing the proof of Theorem 1.

## C. The bipartite case

We will now show the following:
Theorem 6. Any bipartite unitary of Schmidt rank 2 is locally equivalent to a controlled unitary where either party can be chosen as the control, and at least one party can control with two terms.

For example, if the first party controls with two terms, then up to local unitaries

$$
\begin{equation*}
\mathcal{U}=P_{1} \otimes W_{1}+P_{2} \otimes W_{2} \tag{14}
\end{equation*}
$$

where $P_{1}$ and $P_{2}$ are orthogonal projectors.
Proof. Given Theorem 1, it only remains to prove the claims that either party can control and that one of them can control with two terms. Assuming Theorem 1 shows that it is the first
party that can control, then

$$
\begin{equation*}
\left(U^{(1)} \otimes I^{(2)}\right) \mathcal{U}\left(V^{(1) \dagger} \otimes I^{(2)}\right)=\sum_{k=1}^{d_{1}}|k\rangle\langle k| \otimes W_{k} \tag{15}
\end{equation*}
$$

Since $\mathcal{U}$ has Schmidt rank 2, it must be that the span of unitaries $\left\{W_{k}\right\}_{k=1}^{d_{1}}$ has dimension exactly equal to 2 . Choose ordering of the standard basis states on the first party's space such that $W_{1}, W_{2}$ are linearly independent. Then,

$$
\begin{equation*}
W_{k}=\mu_{k 1} W_{1}+\mu_{k 2} W_{2} \tag{16}
\end{equation*}
$$

Inserting this into Eq. (15), we find

$$
\begin{align*}
\left(U^{(1)} \otimes I^{(2)}\right) \mathcal{U}\left(V^{(1) \dagger} \otimes I^{(2)}\right) & =\sum_{k=1}^{d_{1}}|k\rangle_{1}\langle k| \otimes \sum_{j=1}^{2} \mu_{k j} W_{j} \\
& =\sum_{j=1}^{2}\left(\sum_{k=1}^{d_{1}} \mu_{k j}|k\rangle_{1}\langle k|\right) \otimes W_{j} \\
& :=\sum_{j=1}^{2} A_{j} \otimes W_{j} . \tag{17}
\end{align*}
$$

Since $W_{k}$ is unitary so that $W_{k}^{\dagger} W_{k}=I^{(2)}$, then from Eq. (16) we find that for every $k$,

$$
\begin{align*}
0= & \mu_{k 1} \mu_{k 2}^{*} I^{(2)}-\left(1-\left|\mu_{k 1}\right|^{2}-\left|\mu_{k 2}\right|^{2}\right) W_{1}^{\dagger} W_{2} \\
& +\mu_{k 1}^{*} \mu_{k 2}\left(W_{1}^{\dagger} W_{2}\right)^{2} . \tag{18}
\end{align*}
$$

First let us assume that the coefficients in this quadratic equation for unitary $W_{1}^{\dagger} W_{2}$ do not all vanish. Then when diagonalized, it becomes a quadratic equation for the eigenvalues of this unitary. Since all eigenvalues satisfy the same quadratic equation, which has exactly two distinct solutions, this means that $W_{1}^{\dagger} W_{2}$ has exactly two distinct eigenvalues (which is why the quadratic equation cannot have only one distinct solution, since $W_{1}^{\dagger} W_{2} \not \propto I^{(2)}$ ), and then with $P_{1}, P_{2}$ orthogonal projectors onto the degenerate subspaces of $W_{1}^{\dagger} W_{2}$, thus providing a decomposition of the identity on the second party's space, $I^{(2)}=P_{1}+P_{2}$, we have

$$
\begin{equation*}
W_{1}^{\dagger} W_{2}=\lambda_{1} P_{1}+\lambda_{2} P_{2} \tag{19}
\end{equation*}
$$

and

$$
\begin{align*}
& \left(U^{(1)} \otimes W_{1}^{\dagger}\right) \mathcal{U}\left(V^{(1) \dagger} \otimes I^{(2)}\right) \\
& \quad=A_{1} \otimes\left(P_{1}+P_{2}\right)+A_{2} \otimes\left(\lambda_{1} P_{1}+\lambda_{2} P_{2}\right) \\
& \quad=Q_{1} \otimes P_{1}+Q_{2} \otimes P_{2}, \tag{20}
\end{align*}
$$

with $Q_{j}=\left(A_{1}+\lambda_{j} A_{2}\right)$ unitaries. Therefore, either party can control, and the second party can control with two terms.

We still need to consider the case that all coefficients in the quadratic (18) vanish. Then for each $k$, either $\mu_{k 1}=0$ and $\left|\mu_{k 2}\right|=1$ or $\mu_{k 2}=0$ and $\left|\mu_{k 1}\right|=1$. In either case, we can multiply Eq. (17) by the diagonal unitary $D=\sum_{k} \mu_{k m}^{*}|k\rangle_{1}\langle k|$, with $m=1$ or 2 chosen so that each diagonal element is
nonzero, to obtain

$$
\begin{align*}
& \left(D U^{(1)} \otimes I^{(2)}\right) \mathcal{U}\left(V^{(1) \dagger} \otimes I^{(2)}\right) \\
& \quad=\sum_{j=1}^{2}\left(\sum_{k=1}^{d_{1}}\left|\mu_{k j}\right|^{2}|k\rangle_{1}\langle k|\right) \otimes W_{j}=P_{1} \otimes W_{1}+P_{2} \otimes W_{2} . \tag{21}
\end{align*}
$$

In this case, the first party can control with two terms. Multiplying this expression on the left by $I^{(1)} \otimes W_{1}^{\dagger}$ and then performing a unitary similarity transformation on the second party to diagonalize $W_{1}^{\dagger} W_{2}$, we see by Lemma 2 that the second party can also control, completing the proof.

Theorem 6 has the following corollary:
Corollary 7. Any Schmidt rank-2 bipartite unitary can be implemented using a maximally entangled state on two qubits and LOCC.

We omit the proof because this corollary follows directly from the results of Ref. [2], which also provides a simple protocol. Let us just offer a remark on whether this entanglement cost of 1 ebit is optimal: while it is shown in Ref. [5] that it is impossible to deterministically implement any Schmidt rank-2 bipartite unitary using a Schmidt rank-2 partially entangled state and LOCC, it may be possible by using a partially entangled state of Schmidt rank greater than 2 with less than 1 ebit of entanglement, see the example in Ref. [5]. Hence the optimal entanglement cost is not always 1 ebit.

## III. DISCUSSION: UNITARIES OF HIGHER SCHMIDT RANK

It is not difficult to find unitaries that are not controlled, and one need only go to Schmidt rank-3 to find simple examples. One such example, which acts on three parties, is

$$
\begin{equation*}
\mathcal{U}=\frac{1}{\sqrt{3}}(I \otimes I \otimes I+i X \otimes X \otimes X+i Z \otimes Z \otimes Z) \tag{22}
\end{equation*}
$$

where $X$ and $Z$ are Hermitian unitaries that anticommute with one another: $X Z+Z X=0$. For such operators, no unitaries $U, V$ exist such that $U V^{\dagger}, U X V^{\dagger}, U Z V^{\dagger}$ are all diagonal (because this would require that $V^{\dagger} U$ commutes with both $X$ and $Z$, and that $U X V^{\dagger}$ commutes with $U Z V^{\dagger}$; together these commutation relations imply that $X$ commutes with $Z$ ). A common example of operators satisfying these conditions is the usual Pauli operators $\sigma_{x}, \sigma_{z}$. Another well-known example, this time on a bipartite system and having Schmidt rank of 4, is the SWAP operator on two qubits,

$$
\begin{equation*}
\mathcal{U}=\frac{1}{2}\left(I \otimes I+\sigma_{x} \otimes \sigma_{x}+\sigma_{y} \otimes \sigma_{y}+\sigma_{z} \otimes \sigma_{z}\right) \tag{23}
\end{equation*}
$$

Of course, it is certainly also possible for unitaries of higher Schmidt rank to be controlled unitaries. Following the arguments presented in the previous sections, we can give a sufficient condition that any given unitary is locally equivalent to a controlled unitary. Write unitary $\mathcal{U}$ as a sum of product operators,

$$
\begin{equation*}
\mathcal{U}=\sum_{j=1}^{N} M_{j}^{(1)} \otimes M_{j}^{(2)} \otimes \cdots \otimes M_{j}^{(P)}, \tag{24}
\end{equation*}
$$

so that

$$
\begin{align*}
I & =\mathcal{U}^{\dagger} \mathcal{U} \\
& =\sum_{i, j=1}^{N} M_{i}^{(1) \dagger} M_{j}^{(1)} \otimes M_{i}^{(2) \dagger} M_{j}^{(2)} \otimes \cdots \otimes M_{i}^{(P) \dagger} M_{j}^{(P)} \tag{25}
\end{align*}
$$

If for any given $\alpha$, operators $\left\{M_{i}^{(\alpha) \dagger} M_{j}^{(\alpha)}\right\}$ span a twodimensional space, Lemma 3 tells us that $\left\{M_{i}^{(\alpha)}\right\}_{j=1}^{N}$ can all be simultaneously diagonalized by local unitaries $U^{(\alpha)}, V^{(\alpha)}$. By Lemma 2, we then have that each such party can act as a control for this unitary. Therefore, the following theorem holds:

Theorem 8. Given nonlocal unitary $\mathcal{U}=\sum M_{j}^{(1)} \otimes \cdots \otimes$ $M_{j}^{(P)}$ acting on $P$ parties and having any Schmidt rank, if for any given $\alpha$, operators $\left\{M_{i}^{(\alpha) \dagger} M_{j}^{(\alpha)}\right\}$ span a two-dimensional space, that party can act as a control for $\mathcal{U}$, and this is true for every such party.

## IV. CONCLUSIONS

We have shown that every nonlocal multipartite unitary having Schmidt rank equal to 2 is locally equivalent to a fully controlled unitary with all parties but one acting as a control. In the bipartite case we get a stronger result: any bipartite unitary of Schmidt rank 2 is locally equivalent to a controlled unitary where either party can be chosen as the control, and at least one party can control with two terms, which implies that such unitary can be implemented using LOCC and a maximally entangled state on two qubits. We also provided a sufficient condition for when a nonlocal unitary on any number of parties is locally equivalent to a controlled unitary, and this condition allows one to identify which, if any, parties can act as controls.

As mentioned in the Introduction, our main results can be applied to the gate decomposition (quantum circuit design) of unitaries that act on several systems in the same laboratory. For example, the bipartite result would imply that any unitary acting on systems $A$ and $B$ with Schmidt rank 2 can be expressed as $\mathcal{U}=\left(U_{1}^{(A)} \otimes U_{1}^{(B)}\right) Q\left(U_{2}^{(A)} \otimes U_{2}^{(B)}\right)$, where $U_{j}^{(A)}$ and $U_{j}^{(B)}$ are local unitaries on $A$ or $B$, and $Q$ is a controlled unitary.

A natural extension of the work presented in this paper on unitaries of Schmidt rank-2 would be to characterize higher Schmidt rank nonlocal unitaries in terms of product operator expansions, beginning with multipartite unitaries of small Schmidt rank. Such studies may help us better understand the entanglement cost of implementing nonlocal unitaries using LOCC protocols.

## ACKNOWLEDGMENTS

S.C. was supported in part by the National Science Foundation through Grant No. PHY-1205931. L. Yu was
supported by the National Research Foundation and Ministry of Education in Singapore.

## APPENDIX: PROOF OF LEMMA 3

Since the identity operator lies in the two-dimensional span of operators $\left\{R_{i}^{\dagger} R_{j}\right\}$, there exist indices $K, L$ such that for all $i, j, R_{i}^{\dagger} R_{j}$ lies in the span of $\left\{I, R_{K}^{\dagger} R_{L}\right\}$. In particular, we can write

$$
\begin{equation*}
R_{i}^{\dagger} R_{L}=\mu_{i} I+v_{i} R_{K}^{\dagger} R_{L} \forall i \tag{A1}
\end{equation*}
$$

Suppose we fix $K$ and seek $L$ such that $\exists i$ for which $\mu_{i} \neq 0$. If this is impossible, then

$$
\begin{equation*}
R_{i}^{\dagger} R_{j}=\hat{v}_{i j} R_{K}^{\dagger} R_{j} \forall i, j \tag{A2}
\end{equation*}
$$

However, this means

$$
\begin{equation*}
I=\sum_{i, j} \alpha_{i j} R_{i}^{\dagger} R_{j}=R_{K}^{\dagger} \sum_{i, j} \alpha_{i j} \hat{v}_{i j} R_{j}, \tag{A3}
\end{equation*}
$$

which implies that $R_{K}$ is full rank, and then with $j=K$ in (A2), we have that every $R_{i}$ is proportional to $R_{K}$. This is impossible given that $\left\{R_{i}^{\dagger} R_{j}\right\}$ spans a two-dimensional space, so for each $K$ there exists a choice of $L$ such that $\mu_{i} \neq 0$ for at least one $i$ in (A1), and we immediately see that $R_{L}$ is full rank. Hence $R_{L}^{-1}$ exists, and from (A1) we have

$$
\begin{equation*}
R_{i}^{\dagger}=\mu_{i} R_{L}^{-1}+v_{i} R_{K}^{\dagger} \forall i \tag{A4}
\end{equation*}
$$

Setting $i=L$ and choosing unitaries $U, V$ such that $U R_{L} V^{\dagger}$ is diagonal, we see that $U R_{K} V^{\dagger}$ is also diagonal, unless $\nu_{L}=0$. If $v_{L} \neq 0$, then by (A4), $U R_{i} V^{\dagger}$ is diagonal for all $i$, and we are finished.

Suppose now that there is no choice of $K, L$ such that $v_{L} \neq 0$. Then $\exists L$ such that $v_{L}=0$, and this implies that $R_{L}=$ $\sqrt{\mu_{L}} W_{L}$ with $W_{L}$ unitary and $\mu_{L} \neq 0$. Then, from (A1)

$$
\begin{equation*}
\sqrt{\mu_{L}} R_{i}^{\dagger} W_{L}=\mu_{i} I+v_{i} \sqrt{\mu_{L}} R_{K}^{\dagger} W_{L} \forall i, \tag{A5}
\end{equation*}
$$

and if $R_{K}$ is proportional to a unitary, we can choose unitary $V$ such that $V R_{K}^{\dagger} W_{L} V^{\dagger}$ is diagonal, in which case $V R_{i}^{\dagger} W_{L} V^{\dagger}$ is diagonal $\forall i$ and choosing $U=V W_{L}^{\dagger}$, we are done.

Finally, consider the case that there is no choice of $K, L$ such that $v_{L} \neq 0$ and $R_{K}$ is not proportional to a unitary. Then, $R_{K}^{\dagger} R_{K}$ is not proportional to the identity operator, and we can write

$$
\begin{equation*}
R_{i}^{\dagger} R_{j}=\mu_{i j} I+v_{i j} R_{K}^{\dagger} R_{K} \forall i, j \tag{A6}
\end{equation*}
$$

We still have $L$ such that $R_{L}=\sqrt{\mu_{L}} W_{L}$, as above. Then,

$$
\begin{equation*}
\sqrt{\mu_{L}} R_{i}^{\dagger} W_{L}=\mu_{i L} I+v_{i L} R_{K}^{\dagger} R_{K} \forall i . \tag{A7}
\end{equation*}
$$

Choosing unitary $V$ so that $V R_{K}^{\dagger} R_{K} V^{\dagger}$ is diagonal, we then have that $V W_{L}^{\dagger} R_{i} V^{\dagger}$ is diagonal $\forall i$. Choosing $U=V W_{L}^{\dagger}$ completes the proof.
[1] J. Tyson, J. Phys. A: Math. Gen. 36, 10101 (2003).
[2] L. Yu, R. B. Griffiths, and S. M. Cohen, Phys. Rev. A 81, 062315 (2010).
[3] X. Wang, B. C. Sanders, and D. W. Berry, Phys. Rev. A 67, 042323 (2003).
[4] A. Soeda, P. S. Turner, and M. Murao, Phys. Rev. Lett. 107, 180501 (2011).
[5] D. Stahlke and R. B. Griffiths, Phys. Rev. A 84, 032316 (2011).
[6] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A 52, 3457 (1995).
[7] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, UK, 2000).
[8] D. Schlingemann, Quantum Inf. Comp. 3(5), 431 (2003).
[9] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984 (IEEE, New York, 1984), pp. 175-179.
[10] S. Balakrishnan and R. Sankaranarayanan, Quantum Inf. Process. 10, 449 (2011).
[11] S. M. Cohen, arXiv:1210.0644v3 [quant-ph].


[^0]:    *cohensm52@gmail.com
    ${ }^{1}$ We assume that the dimension of the Hilbert space of each system remains unchanged after the action of the unitary.

