Local cloning of entangled states

Vlad Gheorghiu,[1,*] Li Yu,[1,†] and Scott M. Cohen[1,2,‡]
[1]*Department of Physics, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA*
[2]*Department of Physics, Duquesne University, Pittsburgh, Pennsylvania 15282, USA*
(Received 7 May 2010; published 11 August 2010)

We investigate the conditions under which a set $\mathcal{S}$ of pure bipartite quantum states on a $D \times D$ system can be locally cloned deterministically by separable operations, when at least one of the states is full Schmidt rank. We allow for the possibility of cloning using a resource state that is less than maximally entangled. Our results include that: (i) all states in $\mathcal{S}$ must be full Schmidt rank and equally entangled under the G-concurrence measure, and (ii) the set $\mathcal{S}$ can be extended to a larger clonable set generated by a finite group G of order $|G| = N$, the number of states in the larger set. It is then shown that any local cloning apparatus is capable of cloning a number of states that divides D exactly. We provide a complete solution for two central problems in local cloning, giving necessary and sufficient conditions for (i) when a set of maximally entangled states can be locally cloned, valid for all D; and (ii) local cloning of entangled qubit states with nonvanishing entanglement. In both of these cases, we show that a maximally entangled resource is necessary and sufficient, and the states must be related to each other by local unitary "shift" operations. These shifts are determined by the group structure, so need not be simple cyclic permutations. Assuming this shifted form and partially entangled states, then in $D = 3$ we show that a maximally entangled resource is again necessary and sufficient, while for higher-dimensional systems, we find that the resource state must be strictly more entangled than the states in $\mathcal{S}$. All of our necessary conditions for separable operations are also necessary conditions for local operations and classical communication (LOCC), since the latter is a proper subset of the former. In fact, all our results hold for LOCC, as our sufficient conditions are demonstrated for LOCC, directly.

DOI: 10.1103/PhysRevA.82.022313 PACS number(s): 03.67.Mn

I. INTRODUCTION

As summarized by the "no-cloning" theorem of [1], any set of quantum states can be deterministically cloned if and only if the states in the set are mutually orthogonal. When the set consists of bipartite entangled states, and the cloning is restricted to local operations and classical communication (LOCC), the problem becomes much more difficult, and further restrictions have to be imposed. The mere orthogonality of the states no longer implies that they can be (locally) cloned.

The local cloning protocol of a set of bipartite entangled states $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ is schematically represented as

$$|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab} \longrightarrow |\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}, \quad \forall i, \tag{1}$$

where the letters A,a label Alice's systems and B,b label Bob's systems. Both parties are assumed to have access to ancillary qudits and may share a classical communication channel, so that in principle any LOCC operation can be performed. The state $|\phi\rangle$ is shared in advance between the parties, and it plays the role of a "blank state" on which the copy of $|\psi_i\rangle$ is to be imprinted.

The local cloning problem has recently received a great deal of attention [2–6], and was partially extended to tripartite systems in [7]. The question addressed in all previous work was which sets of states $\mathcal{S}$ can be locally cloned (by LOCC) using a given blank state $|\phi\rangle$.

Note that if one can use LOCC to transform $|\phi\rangle$ into three maximally entangled states of sufficient Schmidt rank, then the local cloning of any set of bipartite orthogonal entangled states becomes trivially possible, using teleportation: Alice uses one maximally entangled state to teleport her part of $|\psi_i\rangle$ to Bob, who then distinguishes it (i.e., learns i), and next communicates the result back to Alice. Now both Alice and Bob know which state was fed into the local cloning machine. Finally, they transform deterministically the two remaining maximally entangled states into $|\psi_i\rangle \otimes |\psi_i\rangle$ by LOCC, which is always possible, according to [8].

Another possible scenario that uses only two entangled blank states involves using LOCC to deterministically distinguish which state $|\psi_i\rangle$ was fed into the local cloning machine, which can always be done if there are only two states in the set $\mathcal{S}$ [9]. Then, knowing the state, one can deterministically transform the two blank states into $|\psi_i\rangle \otimes |\psi_i\rangle$ (by LOCC). In this case, one needs at least two maximally entangled resource states, one for each of the two copies that must now be created, since in general the entanglement of the original state will have been destroyed in the process of distinguishing the states [10].

One might hope, however, that local cloning can be performed using even less entanglement. As first shown in [2], this hope is sometimes correct. Any two (and not more) two-qubit Bell states can be locally cloned using only one two-qubit maximally entangled state.

This result was further extended in [3] and [4], which considered local cloning of maximally entangled states on higher-dimensional $D \times D$ systems using a maximally entangled resource of Schmidt rank D. First, necessary and sufficient conditions for the local cloning of two maximally entangled states were provided in [3], which also proved that for $D = 2$ (qubits) or $D = 3$ (qutrits) any pair of maximally entangled states can be locally cloned with a maximally entangled blank state. Whenever D is not prime the authors

*vgheorgh@andrew.cmu.edu
†liy@andrew.cmu.edu
‡cohensm@duq.edu

showed that there always exist pairs of maximally entangled states that cannot be locally cloned with a maximally entangled blank state. A generalization to more than two states but prime D was given in [4], which showed that a set of D maximally entangled states can be locally cloned using a maximally entangled resource if and only if the states in the set are locally (cyclically) shifted,

$$|\psi_i\rangle = \frac{1}{\sqrt{D}} \sum_{r=0}^{D-1} |r\rangle^A |r \oplus i\rangle^B, \tag{2}$$

where the $\oplus$ symbol denotes addition modulo D.

Kay and Ericsson [5] extended the above results to the LOCC cloning of full Schmidt rank partially entangled states using a maximally entangled blank state. They presented an explicit protocol for the local cloning of a set of $D \times D$ cyclically shifted partially entangled states,

$$|\psi_i\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r} |r\rangle^A |r \oplus i\rangle^B, \tag{3}$$

and asserted that (3) is also a necessary condition for such cloning; the states to be cloned must be of this form. Unfortunately, the proof is not correct,[1] and therefore finding necessary conditions when the states are partially entangled remains an open problem.

In this paper, we consider a set $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ of full Schmidt rank qudit (of arbitrary dimension) partially entangled states. Actually, we will begin by considering sets $\mathcal{S}$ in which only one state is required to be full Schmidt rank, and then we will see that in fact, all states in $\mathcal{S}$ must be full rank. Previous work assumed the blank state $|\phi\rangle$ to be maximally entangled, but in the present article we do not impose any *a priori* assumptions on $|\phi\rangle$ and find that its Schmidt rank must be at least that of the states in $\mathcal{S}$. Furthermore, we do not restrict to LOCC cloning, but allow for the more general class of separable operations—all the necessary conditions we find for separable operations will also be necessary for LOCC since the latter is a (proper) subset of the former [11].

The remainder of the paper is organized as follows. In the next section we give a preliminary discussion and define some terms that will be used. Then, in Sec. III, we turn to the characterization of clonable sets of states, where we show that $|\phi\rangle$ and all states in $\mathcal{S}$ must be full Schmidt rank, provide additional necessary conditions on $\mathcal{S}$, and then prove the group structure of these sets. From this group structure, it is then shown that the number of states in $\mathcal{S}$ must divide D exactly, and this is followed by a proof of a necessary ("group-shifted") condition on the local cloning of a set of $D \times D$ maximally entangled states. Then, in Sec. IV, we further consider group-shifted sets, now allowed to be not maximally entangled, showing that a maximally entangled blank state is sufficient by giving an LOCC protocol that clones these states. This demonstrates that the necessary condition found in the previous section for cloning maximally entangled states is also sufficient for LOCC cloning. In Sec. V, we provide necessary conditions on the minimum entanglement in the blank. In addition, we obtain necessary and sufficient conditions for local cloning of any set when $D = 2$ (entangled qubits), and for any group-shifted set for $D = 3$ (entangled qutrits); in both these cases we find that the blank state must be maximally entangled, even when the states to be cloned are not. For higher dimensions with these group-shifted sets, we also show that the blank must have strictly more entanglement than the states to be cloned. Finally, Sec. VI provides concluding remarks as well as some open questions. Longer proofs are presented in the appendixes.

II. PRELIMINARY REMARKS AND DEFINITIONS

A separable operation Λ on a bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$ is a transformation that can be written as

$$\rho' = \Lambda(\rho) = \sum_{m=0}^{M-1} (A_m \otimes B_m) \rho (A_m \otimes B_m)^\dagger, \tag{4}$$

where ρ is an initial density operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The Kraus operators are arbitrary product operators satisfying the closure condition,

$$\sum_{m=0}^{M-1} A_m^\dagger A_m \otimes B_m^\dagger B_m = I_A \otimes I_B, \tag{5}$$

with I_A and I_B the identity operators. The extension to multipartite systems is obvious, but here we will only consider the bipartite case. To avoid technical issues the sums in (4) and (5), as well as the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$, are assumed to be finite.

The local cloning protocol is described as follows. Suppose Alice and Bob are two spatially separated parties, each holding a pair of quantum systems of dimension D, with Alice's systems described by a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_a$ and Bob's by $\mathcal{H}_B \otimes \mathcal{H}_b$. Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ be a set of orthogonal bipartite entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $|\phi\rangle^{ab} \in \mathcal{H}_a \otimes \mathcal{H}_b$ be another bipartite entangled state that plays the role of a resource, which we call the blank state, and is shared in advance between Alice and Bob. Their goal is to implement

[1]The matter was discussed with Kay [23]. The fact that the argument is not correct can be observed after a careful reading of the paragraph following Eq. (3) in [5]. The authors claim that the local cloning of partially entangled states is equivalent to the cloning of maximally entangled states, but this statement is incorrect, because the authors implicitly modified the Kraus operators that defined the local cloning i.e., changed A_k to $A'_k = A_k M_0$, where M_0, (defined in Eq. (3) of [5]), is the operator that transforms the maximally entangled state $(1/\sqrt{D}) \sum_{r=0}^{D-1} |r\rangle^A |r\rangle^B$ to the partially entangled state $|\psi_0\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r} |r\rangle^A |r\rangle^B$. The new Kraus operators do not satisfy the closure condition anymore (necessary for a deterministic transformation), since $\sum_k {A'_k}^\dagger A'_k \otimes {B_k}^\dagger B_k = \sum_k M_0^\dagger (A_k^\dagger A_k) M_0 \otimes {B_k}^\dagger B_k = M_0^\dagger M_0 \otimes I \neq I \otimes I$, because M_0 is not a unitary operator (unless $|\psi_0\rangle$ is maximally entangled, case excluded).

Another way of seeing that the argument is not correct is to observe that, if the B_k operator performs the cloning of a maximally entangled state using a maximally entangled blank, as it is claimed, then B_k must be proportional to a unitary operator (see Theorem 1 (iii) of [16] and Sec. 3.1 of [3]). It then follows that the closure condition for the Kraus operators is not satisfied, with A_k as defined in Eq. (3) of [5].

deterministically (i.e., with probability one) the transformation,

$$|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab} \longrightarrow |\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}, \quad \forall i = 0 \cdots N-1, \tag{6}$$

by a bipartite separable operation. Alice and Bob know exactly the states that belong to the set $\mathcal{S}$ and also know the blank state $|\phi\rangle^{ab}$, but they do not know which state will be fed to the local cloning machine described by (6)—the machine has to work equally well for all states in $\mathcal{S}$! Note that local cloning is defined up to local unitaries (i.e., a set $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ can be locally cloned if and only if the set $\mathcal{S}' = \{U^A \otimes V^B |\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ can be locally cloned), where U^A and V^B are local unitaries. This is true because local unitaries can always be implemented deterministically at the beginning or at the end of the cloning operation.

The Schmidt coefficients of $|\psi_i\rangle^{AB}$ are labeled by $\lambda_r^{(i)}$ and by convention are sorted in decreasing order, with $\lambda_0^{(i)} \geqslant \lambda_1^{(i)} \geqslant \cdots \geqslant \lambda_{D-1}^{(i)}$ and $\sum_{r=0}^{D-1} \lambda_r^{(i)} = 1$, for all $i = 0 \ldots N-1$, and the Schmidt coefficients of $|\phi\rangle^{ab}$ are labeled by γ_r, with $\gamma_0 \geqslant \gamma_1 \cdots \geqslant \gamma_{D-1}$ and $\sum_{r=0}^{D-1} \gamma_r = 1$. To remind the reader that the components of a vector $\vec{\lambda}$ are arranged in decreasing order we use the notation $\vec{\lambda}^{\downarrow}$.

The Schmidt rank of a bipartite state is the number of its nonzero Schmidt coefficients. We say that a state of a $D \times D$ dimensional system has full Schmidt rank if its Schmidt rank is equal to D.

We use the concept of majorization, which is a partial ordering on D-dimensional real vectors. More precisely, if $\vec{x} = (x_0, \ldots, x_{D-1})$ and $\vec{y} = (y_0, \ldots, y_{D-1})$ are two real D-dimensional vectors, we say that $\vec{x}$ is majorized by $\vec{y}$ and write $\vec{x} \prec \vec{y}$ if and only if $\sum_{j=0}^{k} x_j^{\downarrow} \leqslant \sum_{j=0}^{k} y_j^{\downarrow}$ holds for all $k = 0, \ldots, D-1$, with equality when $k = D-1$.

For two $D \times D$ bipartite pure states $|\chi\rangle$ and $|\eta\rangle$, we use the shorthand notation $|\chi\rangle \prec |\eta\rangle$ to denote the fact that the vector of Schmidt coefficients of $|\chi\rangle$ is majorized by the vector of Schmidt coefficients of $|\eta\rangle$. See [8] or Chapter 12.5 of [12] for more details about majorization.

The entanglement of a $D \times D$ bipartite pure state $|\chi\rangle$ can be quantified by various entanglement measures,[2] the ones used extensively in this paper being the *entropy of entanglement*,

$$E(|\chi\rangle) = -\sum_{r=0}^{D-1} \lambda_r \log_D \lambda_r, \tag{7}$$

and the *G-concurrence* [13],

$$C_G(|\chi\rangle) = D \left(\prod_{r=0}^{D-1} \lambda_r \right)^{1/D}, \tag{8}$$

where λ_r denotes the rth Schmidt coefficient of $|\chi\rangle$. The base D in the logarithm in (7) as well as the prefactor D in (8) appear for normalization purposes, so that the entropy of entanglement as well as the G-concurrence of a maximally entangled state are both 1, regardless of the dimension.

[2]Often called entanglement monotones (i.e., nonincreasing under LOCC).

III. CHARACTERIZING SETS OF CLONABLE STATES

A. Preliminary analysis

Mathematically, the local cloning problem can be formulated in terms of a separable transformation on a set of pure input states $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$, using a blank state $|\phi\rangle^{ab}$.

If a set of states $\mathcal{S}$ can be locally cloned using the blank state $|\phi\rangle^{ab}$, then there must exist a bipartite separable operation Λ for which

$$\Lambda(|\psi_i\rangle\langle\psi_i|^{AB} \otimes |\phi\rangle\langle\phi|^{ab}) = |\psi_i\rangle\langle\psi_i|^{AB} \otimes |\psi_i\rangle\langle\psi_i|^{AB}, \quad \forall i = 0 \cdots N-1 \tag{9}$$

(note here that an overall phase factor in the definition of the individual states is of no significance). Since Λ is separable, it can be represented by a set of product Kraus operators,

$$\sum_{m=0}^{M-1} (A_m \otimes B_m)(|\psi_i\rangle\langle\psi_i|^{AB} \otimes |\phi\rangle\langle\phi|^{ab})(A_m \otimes B_m)^{\dagger} = |\psi_i\rangle\langle\psi_i|^{AB} \otimes |\psi_i\rangle\langle\psi_i|^{AB}, \quad \forall i = 0 \cdots N-1, \tag{10}$$

where operators A_m act on $\mathcal{H}_A \otimes \mathcal{H}_a$, and B_m on $\mathcal{H}_B \otimes \mathcal{H}_b$. The above equation is equivalent to

$$A_m \otimes B_m(|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab}) = \sqrt{p_{mi}} e^{i\varphi_{mi}} (|\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}), \quad \forall i = 0 \cdots N-1, \quad \forall m = 0 \cdots M-1, \tag{11}$$

where $e^{i\varphi_{mi}}$ is a complex phase that may depend on m and i, and p_{mi} are probabilities for which

$$\sum_{m=0}^{M-1} p_{mi} = 1, \quad \forall i = 0 \cdots N-1. \tag{12}$$

By map-state duality in the computational basis[3] [14–17] one can rewrite (11) as

$$A_m(\psi_i \otimes \phi) B_m^T = \sqrt{p_{mi}} e^{i\varphi_{mi}} \psi_i \otimes \psi_i, \ \forall i,m, \tag{13}$$

where ψ_i and ϕ are now operators obtained from the corresponding kets by turning a ket into a bra, and B_m^T is the transpose of B_m.

The superscripts in (13) that label the Hilbert spaces have been dropped for clarity, since now one can regard everything as abstract linear operators, or matrices in the computational basis. Although map-state duality is basis dependent, our results will not depend on the choice of a specific basis.

We now state our first result characterizing sets of states $\mathcal{S}$ that can be locally cloned.

Theorem 1. Rank of states in $\mathcal{S}$. Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ be a set of bipartite orthogonal states on $\mathcal{H}_A \otimes \mathcal{H}_B$ with one state, say $|\psi_0\rangle$, having full Schmidt rank. If the local cloning of $\mathcal{S}$ is

[3]As an example of map-state duality, a bipartite state $|\chi\rangle^{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, $|\chi\rangle^{AB} = \sum c_{ij} |i\rangle^A |j\rangle^B$, is transformed into a map $\chi : \mathcal{H}_B \longrightarrow \mathcal{H}_A$, $\chi = \sum c_{ij} |i\rangle^A \langle j|^B$. Note that the rank of the operator χ is the Schmidt rank of $|\chi\rangle^{AB}$, and the squares of the singular values of χ (or, equivalently, the eigenvalues of $\chi\chi^{\dagger}$) are the Schmidt coefficients of $|\chi\rangle^{AB}$. For more details about map-state duality, see Sec. II of [16].

possible by a separable operation using a blank state $|\phi\rangle$, then $|\phi\rangle$ and all states in $\mathcal{S}$ must be full rank.

Proof. This result follows directly from (13). Given that $|\psi_0\rangle$ has full Schmidt rank, then ψ_0 is a full rank operator. Since the rank of a tensor product is the product of ranks, $\psi_0 \otimes \psi_0$ is a full rank operator. From (12), there must be an m such that $p_{m0} > 0$, then for this m and for $i = 0$ the right-hand side of (13) is a full rank operator, thus the left-hand side is also full rank. Then, since a product of operators cannot have rank exceeding that of any of the individual operators in the product, $\psi_0 \otimes \phi$ is full rank, as are A_m and B_m^T for this m. $\psi_0 \otimes \phi$ being full rank implies that ϕ is full rank. Now for $\forall i \neq 0$, the left-hand side of (13) has rank $D \times \mathrm{rank}(\psi_i)$ as multiplying by the full rank operators A_m and B_m^T do not change the rank. In addition, $D \times \mathrm{rank}(\psi_i)$ is always non-zero, as $\mathrm{rank}(\psi_i) \geqslant 1$, thus $p_{mi} \neq 0$ for this m, otherwise the right-hand side of (13) would have zero rank. Then the right-hand side of (13) is of rank $[\mathrm{rank}(\psi_i)]^2$, so $\mathrm{rank}(\psi_i) = D$, $\forall i$, and we are done. ■

In this paper, we are considering sets $\mathcal{S}$ in which at least one state is full rank. Therefore, by this theorem, we may instead restrict to sets in which every state is full rank, and we will do so throughout the remainder of the paper.

As just argued in the proof of the previous theorem, for m such that $p_{m0} > 0$, all operators in (13) are full rank, hence invertible. From now on we will only consider those m such that $p_{m0} > 0$. Now take the inverse of (13), replace i by j, and right multiply (13) by it to obtain

$$A_m\left(\psi_i \psi_j^{-1} \otimes I\right) A_m^{-1} = \sqrt{\frac{p_{mi}}{p_{mj}}} e^{\mathrm{i}(\varphi_{mi} - \varphi_{mj})} \left(\psi_i \psi_j^{-1} \otimes \psi_i \psi_j^{-1}\right). \tag{14}$$

Define

$$T_{ij}^{(m)} = \sqrt{\frac{p_{mi}}{p_{mj}}} e^{\mathrm{i}(\varphi_{mi} - \varphi_{mj})} \psi_i \psi_j^{-1}, \tag{15}$$

for those m for which $p_{m0} > 0$. Then (14) can be written more compactly as

$$A_m\left(T_{ij}^{(m)} \otimes I\right) A_m^{-1} = T_{ij}^{(m)} \otimes T_{ij}^{(m)}. \tag{16}$$

Since for every i, ψ_i is full rank, we see that $\det(\psi_i) \neq 0$, so $\det(T_{ij}^{(m)})$ is also nonvanishing. Thus, taking the determinant on both sides of (16) yields

$$\det\left(T_{ij}^{(m)}\right)^D = 1, \tag{17}$$

where we have used the fact that $\det(A \otimes B) = \det(A)^M \det(B)^N$, for A and B being $N \times N$ and $M \times M$ matrices, respectively. Recalling the definition of $T_{ij}^{(m)}$ in (15), this condition becomes

$$1 = \left(\frac{p_{mi}}{p_{mj}}\right)^{D/2} \left|\frac{\det(\psi_i)}{\det(\psi_j)}\right|, \tag{18}$$

or

$$p_{mj} = p_{mi} \left|\frac{\det(\psi_i)}{\det(\psi_j)}\right|^{2/D}. \tag{19}$$

Summing (19) over m yields

$$|\det(\psi_i)| = |\det(\psi_j)|, \tag{20}$$

implying

$$p_{mi} = p_{mj}, \tag{21}$$

hence, these determinants and probabilities are independent of the input state. As a consequence, we may write $T_{ij}^{(m)}$ in the simpler form,

$$T_{ij}^{(m)} = e^{\mathrm{i}(\varphi_{mi} - \varphi_{mj})} \psi_i \psi_j^{-1}. \tag{22}$$

Observation. The fact that $p_{mi} = p_m$, independent of i, implies that the cloning apparatus provides no information whatsoever about which state was input to that apparatus, nor can any such information "leak" to an external environment that might be used to implement the local cloning separable operation. This is not without interest, since it rules out the possibility of local cloning by locally distinguishing while preserving entanglement [10]. This result turns out to be valid in the much more general setting of one-to-one transformation of full Schmidt rank pure-state ensembles by separable operations, but a discussion of these broader implications will be presented in a future publication.

We can now provide additional conditions that must hold in order for $\mathcal{S}$ to be a set of states that can be locally cloned by separable operations. These are stated in the following theorem, which holds under completely general conditions, applicable for any N and D.

Theorem 2. Necessary conditions. Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab} \in \mathcal{H}_a \otimes \mathcal{H}_b$ is possible by a separable operation, then the following must hold:

(i) All states in $\mathcal{S}$ are equally entangled with respect to the G-concurrence measure,

$$C_G(|\psi_i\rangle^{AB}) = C_G(|\psi_j\rangle^{AB}), \forall i, j. \tag{23}$$

(ii) Any two states in $\mathcal{S}$ must either share the same set of Schmidt coefficients or be incomparable under majorization.

(iii) $$\mathrm{Spec}\left(T_{ij}^{(m)} \otimes I\right) = \mathrm{Spec}\left(T_{ij}^{(m)} \otimes T_{ij}^{(m)}\right), \forall i, j, \tag{24}$$

where $\mathrm{Spec}(\cdot)$ denotes the spectrum of its argument and $T_{ij}^{(m)}$ is defined as in (22).

Proof. Proof of (i). This follows at once from (20), the definition (8) of G-concurrence, and the fact that for any state $|\chi\rangle$ the product of its Schmidt coefficients is equal to $|\det(\chi)|^2$.

Proof of (ii). The proof follows from Theorem 1 (ii) and (iii) of [16] which states that any two bipartite states $|\chi\rangle$ and $|\eta\rangle$ that are comparable under majorization (i.e., $|\chi\rangle \prec |\eta\rangle$ or $|\eta\rangle \prec |\chi\rangle$) and have equal G-concurrence must share the same set of Schmidt coefficients.

Proof of (iii). The proof follows at once from (16). ■

B. Characterization of clonable sets in terms of finite groups

We next show that to any set $\mathcal{S}$ of states that can all be cloned by the same apparatus, there can be associated a finite group, and the set is essentially generated by this group.

Theorem 3. Group structure of $\mathcal{S}$. Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. If the local cloning of $\mathcal{S}$ is possible by a separable operation, then the set $\mathcal{S}$ can be extended to a larger set

such that $\{T_{ij}^{(m)}\}$ of (22) for fixed j,m constitutes an ordinary representation of a finite group, G. Since the states in $\mathcal{S}$ are related as $e^{i\varphi_{mi}}|\psi_i\rangle = e^{i\varphi_{mj}}(T_{ij}^{(m)} \otimes I_B)|\psi_j\rangle$, then the larger set, with $N = |G|$ members, is generated by the action of the group G on any individual state in the set.

Proof. The starting point of the proof is to multiply (16) on the left of (13) (with index k) to obtain

$$A_m\left(T_{ij}^{(m)}\psi_k \otimes \phi\right)B_m^T = \sqrt{p_m}e^{i\varphi_{mk}}T_{ij}^{(m)}\psi_k \otimes T_{ij}^{(m)}\psi_k. \tag{25}$$

Using (22) this becomes

$$\begin{aligned} &A_m\left(\psi_i\psi_j^{-1}\psi_k \otimes \phi\right)B_m^T \\ &\quad = \sqrt{p_m}e^{i(\varphi_{mi}-\varphi_{mj}+\varphi_{mk})}\psi_i\psi_j^{-1}\psi_k \otimes \psi_i\psi_j^{-1}\psi_k, \end{aligned} \tag{26}$$

which by map-state duality implies that the state $|\psi_i\psi_j^{-1}\psi_k\rangle$ is cloned by the same apparatus as all the states in the original set $\mathcal{S}$. Therefore, $|\psi_i\psi_j^{-1}\psi_k\rangle$—which, by considering the version of (26) that corresponds to states [as in (11)], taking the squared norm of both sides and summing over m, is seen to be normalized—must either (i) be orthogonal to the entire set $\mathcal{S}$, or (ii) be equal to one of those original states up to an overall phase factor. If this state is orthogonal to $\mathcal{S}$, then $\mathcal{S}$ can be extended by including this state as one of its members. So assume $\mathcal{S}$ has been extended to its maximal size (since we are working in finite dimensions, this size will be finite), and then we can conclude that for every i,j,k,

$$\psi_i\psi_j^{-1}\psi_k = e^{i(\varphi_{ml}-\varphi_{mi}+\varphi_{mj}-\varphi_{mk})}\psi_l, \tag{27}$$

for some l, where the phase in the above expression has been determined by comparing (26) to (13). Next multiply this latter expression on the right by $e^{-i\varphi_{mn}}\psi_n^{-1}$ to obtain

$$T_{ij}^{(m)}T_{kn}^{(m)} = T_{ln}^{(m)}. \tag{28}$$

Hence, the collection of $T_{ij}^{(m)}$ is closed under matrix multiplication, which is associative. In addition, $T_{ii}^{(m)} = I$ for every i and $T_{ij}^{(m)}T_{ji}^{(m)} = I$ for every i,j, so we see that the identity element and inverses are present, which concludes the proof that the set $\{T_{ij}^{(m)}\}$ with fixed m form a representation of a group, G. Now, the number of index pairs (i,j) is N^2, where N is the number of states in $\mathcal{S}$. However, we will now show that in fact the order $|G|$ of this group is equal to N and not N^2.

Setting $n = j$ in (28), we have

$$T_{ij}^{(m)}T_{kj}^{(m)} = T_{lj}^{(m)}, \tag{29}$$

so the product is closed even when the second index is constrained to be the same. If we set $l = j$, we see that with $T_{jj}^{(m)} = I$, then for each i there exists k such that $T_{kj}^{(m)} = (T_{ij}^{(m)})^{-1}$. Hence, for every fixed j the set $\mathcal{T}_j = \{T_{ij}^{(m)}\}$ also is a representation of G. Similarly, one can show the same holds if instead it is the first index that is held fixed. Note now that by multiplying (28) on the right by $(T_{kn}^{(m)})^{-1}$, and given that (28) holds for any i,j,k,n, we see that for every i,j, T_{ij} is a member of the group formed by the T_{kn} for fixed n. That is, the group of the T_{kn} for fixed n contains all elements T_{ij}.

Could two or more of the $T_{ij}^{(m)}$ be equal, for fixed j? We will now show this is not the case by demonstrating the linearly independence of the set $\mathcal{T}_j$. Indeed,

$$\begin{aligned} 0 &= \sum_{k=0}^{N-1} c_k T_{kj}^{(m)} = \sum_{k=0}^{N-1} c_k e^{i(\varphi_{mk}-\varphi_{mj})}\psi_k\psi_j^{-1} \\ \iff 0 &= \sum_{k=0}^{N-1} c_k e^{i\varphi_{mk}}\psi_k. \end{aligned} \tag{30}$$

However, the ψ_k are mutually orthogonal, $\mathrm{Tr}(\psi_k^\dagger\psi_j) = \delta_{jk}$, so this can only be satisfied if all the c_k vanish, implying that $\mathcal{T}_j$ is linearly independent, and hence, that $|G| = N$: the (maximal) number of states in $\mathcal{S}$ is equal to the order of G.

For the remainder of the paper, we will use labels f,g,h instead of i,j,k, where the former represent elements of the group G; the group multiplication is denoted as fg, with e the identity element. For example, instead of ψ_0 we will now write ψ_e, and in place of $T_{j0}^{(m)}$ we will simply write $T_f^{(m)}$.

We may now utilize the powerful tools of group theory to study sets $\mathcal{S}$ of clonable states, obtaining a very strong constraint on how many states any given apparatus can possibly clone. Any group G is characterized by its irreducible representations, which we denote as $\Gamma^{(\alpha)}(f), f \in G$, and any representation of G may be decomposed into a direct sum of irreducible representations with a given irreducible representation $\Gamma^{(\alpha)}(f)$ appearing some number n_α times in that sum. In general, a given representation may have $n_\alpha = 0$ for some α, but since here our representation is linearly independent, we know that every irreducible representation must appear at least once [18].

We can use character theory [19] to calculate n_α. Defining characters as $\chi(T_f^{(m)}) = \mathrm{Tr}(T_f^{(m)})$ and $\chi^{(\alpha)}(f) = \mathrm{Tr}[\Gamma^{(\alpha)}(f)]$, we have that

$$n_\alpha = \frac{1}{|G|}\sum_{f\in G}\chi^{(\alpha)}(f)^*\chi\left(T_f^{(m)}\right). \tag{31}$$

However, by taking the trace of (16) and recalling that the trace of a tensor product is equal to the product of the traces, we see that $\chi(T_f^{(m)})$ is equal to either 0 or D. Since every invertible representation of a finite group is equivalent to a unitary representation, the eigenvalues of our representation matrices $T_f^{(m)}$ all have magnitude one. Hence $\chi(T_f^{(m)}) = D$ if and only if all eigenvalues of $T_f^{(m)}$ are equal to 1, in which case we have that $T_f^{(m)} = I$ because $T_f^{(m)}$ is similar to a unitary matrix and therefore diagonalizable. However, $T_f^{(m)} = I$ is equivalent to $f = e$, since $T_f^{(m)} = e^{i(\varphi_{mf}-\varphi_{me})}\psi_f\psi_e^{-1}$. Hence, we may conclude that $\chi(T_f^{(m)})$ vanishes except when $f = e$, in which case $\chi(T_e^{(m)}) = D$.

$$n_\alpha = \frac{Dd_\alpha}{|G|}, \tag{32}$$

where $d_\alpha = \chi^{(\alpha)}(e)$ is the dimension of the α^{th} irreducible representation. Since for every ordinary representation of a finite group there is always the trivial irreducible representation of all ones, $\Gamma^{(t)}(f) = 1$, $\forall f \in G$, where this irreducible representation has dimension $d_t = 1$, we have immediately

that $n_t = D/|G|$ is an integer, implying that $N = |G|$ divides D. Thus,

Theorem 4. Number of clonable states. If an apparatus can locally clone more than one state on a $D \times D$ system, where at least one (and therefore all; see Theorem 1) of these states has full Schmidt rank, then that apparatus can in fact clone a number of states that divides D exactly. In particular, if D is prime, then any such apparatus can clone exactly D states, no more and no less.

Now we see from (32) that n_α is an integer multiple of d_α. If $|G| = D$ so that $n_\alpha = d_\alpha$, we have what is known as the regular representation of G. Otherwise, our representation is a direct sum of an integer number $n_t = D/|G|$ of copies of the regular representation. As is well known, there is always a choice of basis in which the matrices in a *unitary* regular representation appear as permutation matrices $L(f)$, with each row (column) having only a single nonzero entry equal to one. In this basis, denoted as $\{|g\rangle\}_{g\in G}$, we have that $L(f)|g\rangle = |fg\rangle$. The representation $L(f)$ is called the *left regular representation*. One can as well use the *right regular representation* $R(f)$ with $R(f)|g\rangle = |gf^{-1}\rangle$, but without loss of generality in the rest of the paper we restrict only to $L(f)$, since for finite groups the right and left regular representations are equivalent [20].

In our case the representation will generally not be unitary, so when $|G| = D$ we will have that

$$T_f^{(m)} = SL(f)S^{-1}, \tag{33}$$

for some invertible matrix S.

In the remainder of the paper we restrict consideration to $|G| = D$ (or, equivalently, to $n_t = 1$), and note that all results obtained in the remainder of the paper are valid (with small modifications) also when $|G| < D$. However, the notation becomes a bit cumbersome, so we defer detailed discussion about the $|G| < D$ case to Appendix B.

C. Form of the clonable states when all are maximally entangled

It was shown in [3] that when at least one of the states in $\mathcal{S}$ is maximally entangled, then all states in $\mathcal{S}$ must also be maximally entangled. In this section, we consider such sets, in which case the $T_f^{(m)}$ must all be unitary. This follows directly from the fact that when ψ_e is proportional to the identity then ψ_f is proportional to $T_f^{(m)}$, and also that $|\psi_f\rangle$ is maximally entangled if and only if ψ_f is proportional to a unitary.

We have seen that when $N = D$, then $T_f^{(m)} = SL(f)S^{-1}$ for some invertible S, and $L(f)$ is the permutation form of the regular representation of group G. However, we have

Lemma 5. Unitary equivalence. For any two unitary representations T_f and $L(f)$ of a finite group G, which are equivalent in the sense that $T_f = SL(f)S^{-1}$ for some invertible matrix S, then these two representations are also equivalent by a unitary similarity transformation, $T_f = WL(f)W^\dagger$, with W unitary.

A proof of this lemma is given in Chapter 3.3 of [21], and we provide an alternative proof in Appendix A1.

What this lemma tells us is that ψ_f is proportional to $WL(f)\psi_e W^\dagger$ (since by local unitaries, ψ_e can be made proportional to the identity, we will assume here that this is the case, and then ψ_e commutes with $W^\dagger$), or

$$|\psi_f\rangle = c_f[WL(f)\otimes W^*]\sum_{g\in G}|g\rangle^A|g\rangle^B$$
$$= \frac{1}{\sqrt{D}}(W\otimes W^*)\sum_{g\in G}|fg\rangle^A|g\rangle^B, \tag{34}$$

where W^* is the complex conjugate of W, the states $\{|g\rangle\}_{g\in G}$ are some orthonormal basis, $\langle g|h\rangle = \delta_{g,h}$, and we have omitted an unimportant overall phase (from c_f, of magnitude $D^{-1/2}$) in the last line. Note that up to unimportant local unitaries and relabeling of group elements, the set of states (34) can be written either as

$$|\psi_f\rangle = \frac{1}{\sqrt{D}}\sum_{g\in G}|fg\rangle^A|g\rangle^B, \tag{35}$$

or

$$|\psi_f\rangle = \frac{1}{\sqrt{D}}\sum_{g\in G}|g\rangle^A|fg\rangle^B. \tag{36}$$

The states above are of a form that we will refer to as "group-shifted."

In Sec. IV, we provide an explicit LOCC protocol that accomplishes cloning of such shifted sets of states. Thus, we have:

Theorem 6. Maximally entangled states. A set of maximally entangled states on a $D \times D$ system can be cloned by LOCC if and only if there exists a choice of Schmidt bases shared by those states such that they have a group-shifted form, as in (35) or (36).

This extends the result of [4], which applied only for prime D.

Additionally, we remark that in our protocol presented in Sec. IV, there is no need for classical communication (the measurement M_r and the additional corrections Q_r appearing in that protocol can be omitted when the states to be cloned are maximally entangled). This result was first proven in [3], where it was shown that the Kraus operators implementing the cloning of maximally entangled states have to be proportional to unitary operators. A completely different proof of this fact was later provided in [16], in which it was shown that a separable operation that maps a pure state to another pure state, both sharing the same set of Schmidt coefficients, must have its Kraus operators proportional to unitaries; in our case $|\psi_f\rangle\otimes|\phi\rangle$ and $|\psi_f\rangle\otimes|\psi_f\rangle$ do share the same set of Schmidt coefficients, since they are maximally entangled. We here have another simple proof of this result, since we have proved in Theorem 6 that a set of maximally entangled states must be group-shifted in order that they can be cloned, and since our protocol in Sec. IV clones any set that is group-shifted without using communication.

D. Form of the clonable states when $D = 2$ (qubits)

Here, we restrict our attention to local cloning of qubit entangled states, $D = 2$. As D is prime, we know from Theorem 3 that exactly two states can be cloned, $\mathcal{S} = \{|\psi_e\rangle^{AB}, |\psi_g\rangle^{AB}\}$. Both are assumed to be entangled (nonproduct), but not maximally entangled.

Since there is only one independent Schmidt coefficient for a two-qubit state, any two such states are comparable under majorization, and then from part (ii) of Theorem 2 it follows at once that these states have to share the same set of Schmidt coefficients. This is already a surprising result, implicitly assumed (but not proved) in recent work on local cloning of qubit states [6]. We can actually prove a stronger condition: not only do the states have to share the same set of Schmidt coefficients, but they must also share the same Schmidt basis and be of a shifted form, as summarized by the following theorem.

Theorem 7. Entangled qubits. Let $\mathcal{S} = \{|\psi_e\rangle^{AB}, |\psi_g\rangle^{AB}\}$ be a set of two orthogonal two-qubit entangled states and let λ be the largest Schmidt coefficient of $|\psi_e\rangle^{AB}$, assumed to satisfy $1/2 < \lambda < 1$. If the local cloning of $\mathcal{S}$ using a two-qubit entangled blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then, up to local unitaries (that is, the same local unitaries acting on both states), the states must either be of the form,

$$\begin{aligned} |\psi_e\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B, \\ |\psi_g\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|1\rangle^B + \sqrt{1-\lambda}|1\rangle^A|0\rangle^B, \end{aligned} \tag{37}$$

or

$$\begin{aligned} |\psi_e\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B, \\ |\psi_g\rangle^{AB} &= \sqrt{\lambda}|1\rangle^A|0\rangle^B + \sqrt{1-\lambda}|0\rangle^A|1\rangle^B. \end{aligned} \tag{38}$$

Note that a relative phase $e^{i\vartheta}$ may be introduced into $|\psi_g\rangle$, without altering $|\psi_e\rangle$, by Alice and Bob doing local unitaries on systems A and B, $U^{A,B} = |0\rangle\langle 0| + e^{\pm i\vartheta/2}|1\rangle\langle 1|$ (one of them chooses the upper sign; the other does the lower, which accomplishes the task up to an unimportant overall phase). Therefore, the theorem allows cloning of states with these phases.

Proof. First note that without loss of generality one can always assume that the first state $|\psi_e\rangle^{AB}$ is already in Schmidt form,

$$|\psi_e\rangle^{AB} = \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B, \tag{39}$$

since this can be done by a local unitary map $U^A \otimes V^B$. Therefore, the operators ψ_e and ψ_g obtained by map-state duality can be assumed to have the form,

$$\psi_e = \begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \tag{40}$$

$$\psi_g = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}, \tag{41}$$

where λ is the largest Schmidt coefficient of $|\psi_e\rangle^{AB}$ and a_{ij} are complex numbers with $\sum |a_{ij}|^2 = 1$, which is equivalent to the requirement that $|\psi_g\rangle$ be normalized.

Orthogonality between these two states implies that

$$0 = \sqrt{\lambda}a_{00} + \sqrt{1-\lambda}a_{11}. \tag{42}$$

Since the only group of order 2 is cyclic with elements e, g and $g^2 = e$, we have from Theorem 3 that $(T_g^{(m)})^2 = SL(g)^2 S^{-1} = I$. Thus, we require

$$\left(\psi_g \psi_e^{-1}\right)^2 = \begin{pmatrix} e^{i\vartheta} & 0 \\ 0 & e^{i\vartheta} \end{pmatrix}, \tag{43}$$

where the factor of $e^{i\vartheta}$ arises from the phases that appear in the definition of $T_g^{(m)}$; see (22). Thus, (43) implies

$$\frac{a_{00}^2}{\lambda} = \frac{a_{11}^2}{1-\lambda} = e^{i\vartheta} - \frac{a_{01}a_{10}}{\sqrt{\lambda(1-\lambda)}}, \tag{44}$$

and either (i) $a_{00}\sqrt{1-\lambda} = -a_{11}\sqrt{\lambda}$; or (ii) $a_{01} = 0 = a_{10}$. The condition that ψ_g be normalized in the latter case (ii), along with (42) and (44), can only be satisfied if $\lambda = 1/2$, a case we are not considering here. The former case (i) along with (42) implies that $a_{00} = 0 = a_{11}$ (again, assuming $\lambda \neq 1/2$). This concludes the proof, since it implies that $|\psi_g\rangle^{AB}$ has to have either the form (37) or the form (38), up to an unimportant global phase.

Now one can immediately see that one of the families of states considered in [6], of the form $|\psi_e\rangle = \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B$ and $|\psi_g\rangle = \sqrt{1-\lambda}|0\rangle^A|0\rangle^B - \sqrt{\lambda}|1\rangle^A|1\rangle^B$ cannot be locally cloned with a blank state of Schmidt rank 2, unless they are maximally entangled (case already studied in [3]).

IV. LOCAL CLONING OF GROUP-SHIFTED STATES: EXPLICIT PROTOCOL USING A MAXIMALLY ENTANGLED BLANK STATE

Consider now a set of group-shifted partially entangled states $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, where the dimension of both Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is equal to D,

$$|\psi_f\rangle^{AB} = \sum_{g\in G} \sqrt{\lambda_g}|g\rangle^A|fg\rangle^B, \tag{45}$$

and we remind the reader that throughout this section we restrict to the $|G| = D$ case (see Appendix B for the $|G| < D$ case). The reader should also note that we are here using the form (36), where the shift is on the B side, rather than the form (35), which was used throughout Sec. III with the shift on the A side.

In the following we present a protocol that locally clones $\mathcal{S}$ using a maximally entangled blank state of Schmidt rank D. Our protocol, which works for any group G, is a direct generalization of the one presented for the special case of a cyclic group in [5].

Theorem 8. Group-shifted states. Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by (45). The local cloning of $\mathcal{S}$ is always possible using a maximally entangled blank state $|\phi\rangle^{ab}$ of Schmidt rank D.

Proof. Without loss of generality the maximally entangled blank state can be written as

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}} \sum_{h\in G} |h\rangle^a|h\rangle^b. \tag{46}$$

The local cloning protocol is summarized below and the quantum circuit is displayed in Fig. 1.

(1) Starting with $|\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab}$, both Alice and Bob apply the "controlled-group" unitary,

$$\sum_{g\in G} |g\rangle\langle g| \otimes P_g, \quad \text{with} \quad P_g = \sum_{h\in G} |gh\rangle\langle h|, \tag{47}$$

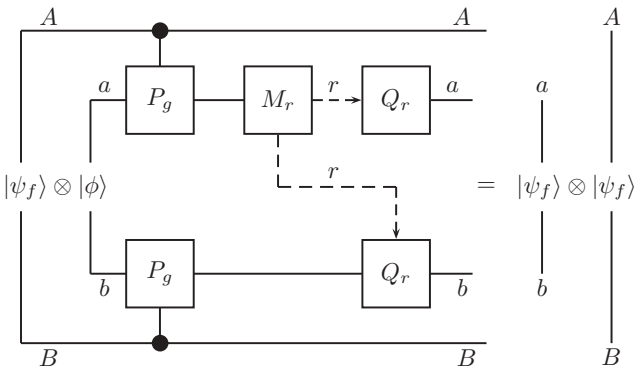

FIG. 1. Circuit diagram for the local cloning of group-shifted states with a maximally entangled blank state. There is no need to perform the measurement M_r and the corrections Q_r whenever the states to be cloned are maximally entangled.

where the permutation P_g acts on system a (b) and is controlled by system A (B), to obtain

$$\sum_{g\in G}\sqrt{\lambda_g}|g\rangle^A|fg\rangle^B\frac{1}{\sqrt{D}}\sum_{h\in G}|gh\rangle^a|fgh\rangle^b = \sum_{g\in G}\sqrt{\lambda_g}|g\rangle^A|fg\rangle^B\frac{1}{\sqrt{D}}\sum_{h\in G}|h\rangle^a|fh\rangle^b. \quad (48)$$

(2) Next, Alice performs a generalized measurement on system a with Kraus operators,

$$M_r=\sum_{h\in G}\sqrt{\lambda_{hr}}|h\rangle\langle h|, \quad \sum_{r\in G}M_r{}^\dagger M_r=I, \quad (49)$$

and communicates the result r to Bob. Conditioned on the result r, the output state is

$$\sum_{g\in G}\sqrt{\lambda_g}|g\rangle^A|fg\rangle^B\sum_{h\in G}\sqrt{\lambda_{hr}}|h\rangle^a|fh\rangle^b. \quad (50)$$

(3) Both Alice and Bob apply the unitary correction,

$$Q_r=\sum_{h\in G}|hr\rangle\langle h|, \quad (51)$$

on systems a and b, respectively, to obtain

$$\sum_{g\in G}\sqrt{\lambda_g}|g\rangle^A|fg\rangle^B\sum_{h\in G}\sqrt{\lambda_{hr}}|hr\rangle^a|fhr\rangle^b = \sum_{g\in G}\sqrt{\lambda_g}|g\rangle^A|fg\rangle^B\sum_{h\in G}\sqrt{\lambda_h}|h\rangle^a|fh\rangle^b = |\psi_f\rangle^{AB}\otimes|\psi_f\rangle^{ab}, \quad (52)$$

which is the desired output.

Note that from symmetry considerations, states of the form $\sum_{g\in G}\sqrt{\lambda_g}|fg\rangle^A|g\rangle^B$ (with the term fg appearing now on Alice's side instead of Bob's side) can also be locally cloned, by interchanging the roles of Alice and Bob in the protocol (e.g., performing the measurement M_r on system b instead of a), then sending the result back to a. Therefore, in the following, when discussing group-shifted states, we will restrict to the states of the form (45).

V. LOCAL CLONING OF GROUP-SHIFTED STATES: MINIMUM ENTANGLEMENT OF THE BLANK

Here again, we restrict for simplicity to the $|G|=D$ case, and discuss the extension of the results for $|G|<D$ in Appendix B.

A. Necessary conditions for arbitrary D

We now turn our attention to the task of characterizing the blank state, which essentially amounts to determining the amount of entanglement it must have in order for the local cloning to be possible. We first give a very general lower bound as:

Theorem 9. Minimum entanglement of the blank. Let $\mathcal{S}=\{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A\otimes\mathcal{H}_B$. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}\in\mathcal{H}_a\otimes\mathcal{H}_b$ is possible by a separable operation, then it must be that

$$\mathrm{Ent}(|\phi\rangle^{ab})\geqslant\max_{f\in G}\mathrm{Ent}(|\psi_f\rangle^{AB}), \quad (53)$$

where $\mathrm{Ent}(\cdot)$ denotes any pure-state entanglement measure.

Proof. We recently proved in [17] that any pure-state entanglement monotone is nonincreasing on average under the general class of separable operations. The theorem follows directly, since otherwise the local cloning machine increases entanglement across the Aa/Bb cut. ■

Providing a more detailed lower bound appears to be difficult, in general, but turns out to be possible in the special case of group-shifted states.

Consider again the set of D group-shifted entangled states (45), and allow for arbitrary phases, $\vartheta_{f,g}$,

$$|\psi_f\rangle^{AB}=\sum_{g\in G}\sqrt{\lambda_g}e^{i\vartheta_{f,g}}|g\rangle^A|fg\rangle^B. \quad (54)$$

Without loss of generality, the blank state $|\phi\rangle^{ab}$ can be written as

$$|\phi\rangle^{ab}=\sum_{h\in G}\sqrt{\gamma_h}|h\rangle^a|h\rangle^b, \quad (55)$$

where γ_h are its Schmidt coefficients, $\sum_{h\in G}\gamma_h=1$.

All states in $\mathcal{S}$ have the same Schmidt coefficients, and hence the same entanglement. As shown above, the local cloning of the above set of states is possible using a maximally entangled blank state when all phases $e^{i\vartheta_{f,g}}$ are chosen to be 1, but it is not yet known if one can accomplish this task using less entanglement. One might hope that the local cloning of $\mathcal{S}$ is possible using a blank state having the same entanglement as each of the states in $\mathcal{S}$, which could be regarded as an "optimal" local cloning. However, we prove below that such an optimal local cloning is impossible with these states. Indeed, we find a sizable gap between the entanglement needed in the blank state and the entanglement of the states of $\mathcal{S}$. For $D=2$ and $D=3$, we prove that a maximally entangled blank state is *always* necessary.

In the rest of this section we will use the *rearrangement inequality* (see Chapter X of [22]), which states that

$$x_ny_1+\cdots+x_1y_n\leqslant x_{\sigma(1)}y_1+\cdots+x_{\sigma(n)}y_n\leqslant x_1y_1+\cdots+x_ny_n, \quad (56)$$

for every choice of real numbers $x_1 \leqslant \cdots \leqslant x_n$ and $y_1 \leqslant \cdots \leqslant y_n$ and every permutation $x_{\sigma(1)}, \ldots, x_{\sigma(n)}$ of $x_1, \ldots, x_n$.

The following lemma is the most important technical result of this section (note that in the statement of this result, we will use $\overline{g}$ for inverses g^{-1} of elements in the group G, which will make the notation somewhat more readable).

Lemma 10. Majorization conditions. Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of D group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by (54) and considered to be not maximally entangled. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then

(i) The majorization condition,

$$\vec{\alpha} \prec \vec{\beta}, \tag{57}$$

must hold. Here, $\vec{\alpha}$ and $\vec{\beta}$ are vectors with D^2 components indexed by elements $g,h \in G$,

$$\alpha_{g,h} = \gamma_h \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}, \quad \beta_{g,h} = \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}\lambda_{fh}, \tag{58}$$

and $\{\mu_f\}_{f\in G}$ is an arbitrary set of non-negative real coefficients that satisfy $\sum_f \mu_f = 1$.

(ii) The smallest Schmidt coefficient $\gamma_{\min}$ of the blank state has to satisfy

$$\gamma_{\min} \geqslant \max_{\{\mu_f\}} \frac{\min_{g,h\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}\lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}}. \tag{59}$$

(iii) In particular, a good choice of $\{\mu_f\}$ is given by

$$\mu_f = \frac{\eta}{\lambda_{\overline{f}}}, \quad \text{with } \eta^{-1} = \sum_{g\in G} 1/\lambda_g, \tag{60}$$

for which (59) becomes

$$\gamma_{\min} \geqslant \frac{1}{D} \min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}\lambda_{fh}. \tag{61}$$

The majorization relation (57) restricts the possible allowed Schmidt coefficients for the blank state and can easily be checked numerically, but an analytic expression is difficult to find, since there is no simple way of ordering (58). That is why parts (ii) and (iii) of the lemma have their importance, since they focus only on the smallest Schmidt coefficient of the blank state. In particular, the bound (iii) is crucial in deriving the necessity of a maximally entangled blank state for the local cloning of qubit and group-shifted qutrit states.

The proof of the lemma is rather technical and is presented in Appendix A 2. However, the main idea of the proof consists of adding an ancillary system $\mathcal{H}_E$ of dimension D on Alice's side and then considering a superposition $\sum_{f\in G} \sqrt{\mu_f}|\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab} \otimes |f\rangle^E$ that will be mapped by the deterministic separable operation to an ensemble $\{p_m, |\Psi_{m,\text{out}}\rangle^{AaBbE}\}$, with $|\Psi_{m,\text{out}}\rangle^{AaBbE} = \sum_{f\in G} e^{i\varphi_{mf}} \sqrt{\mu_f}|\psi_f\rangle^{AB} \otimes |\psi_f\rangle^{ab} \otimes |f\rangle^E$, and we have used the fact discovered above that $p_{mf} = p_m$, independent of f. The average Schmidt vector of the output ensemble over the AaE/Bb cut has to majorize the input Schmidt vector (see [17]) and this yields (i). Parts (ii) and (iii) are direct implications of (i).

B. Qubits and qutrits

When $D = 2$ or $D = 3$, one can easily show that the minimum in (61) is exactly one, and therefore:

Theorem 11. Necessity of maximally entangled blank. The following must hold.

(i) A maximally entangled state of Schmidt rank 2 is the minimum required resource for the local cloning of two entangled qubit states.

(ii) A maximally entangled state of Schmidt rank 3 is the minimum required resource for the local cloning of three group-shifted entangled qutrit states.

The proof of both (i) and (ii) follows easily from Lemma 10 (iii), by applying the rearrangement inequality to (61), and is presented in Appendix A 3.

When $D = 2$, or when $D = 3$ and all phases $e^{i\vartheta_{f,g}} = 1$, an explicit protocol for cloning these states exists [5] (alternatively, see the proof of our Theorem 8), and therefore Theorem 11 becomes a necessary and sufficient condition for the local cloning of such states. In particular, together with Theorem 7, it provides a complete solution to the problem of local cloning when $D = 2$.

C. $D > 3$: finite gap in the necessary entanglement

For $D > 3$, preliminary numerical studies indicate that the minimum (61) in Lemma 10 (iii) is often equal to one, with few exceptions. It might be the case that a better choice of $\{\mu_f\}$ in (59) of Lemma 10 (ii) may provide the $1/D$ lower bound, but we were unable to prove this.

However, for any set of group-shifted states, we can prove that there is a rather sizable gap between the entanglement needed in the blank state and the entanglement of the states of $\mathcal{S}$, as stated by the following theorem.

Theorem 12. Finite gap. Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of D group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by (54) and considered to be not maximally entangled. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then the entanglement of the blank state has to be strictly greater than the entanglement of the states in $\mathcal{S}$, often by a wide margin. Specifically,

$$E(|\phi\rangle^{ab}) \geqslant H(\{q_r\}) > E(|\psi_f\rangle^{AB}), \quad \forall f \in G, \tag{62}$$

where $E(\cdot)$ denotes the entropy of entanglement and $H(\{q_r\})$ is the Shannon entropy of the probability distribution $\{q_r\}$, $q_r := \sum_{f\in G} \lambda_f \lambda_{fr}$, $\sum_{r\in G} q_r = 1$.

The proof follows by setting $\mu_f = 1/D$ in Lemma 10 (i), but is rather long and is presented in Appendix A 4.

VI. CONCLUSION AND OPEN QUESTIONS

We have investigated the problem of local cloning of a set $\mathcal{S}$ of bipartite $D \times D$ entangled states by separable operations, at least one of which is full Schmidt rank. We proved that all states in $\mathcal{S}$ must be full rank and that the maximal set of clonable states must be generated by a finite group G of order N, the number of states in this maximal set, and then we showed that N has to divide D exactly. We further proved that all states in $\mathcal{S}$ must be equally entangled with respect to the G-concurrence measure, and this implied that any two states

in $\mathcal{S}$ must either share the same set of Schmidt coefficients or otherwise be incomparable under majorization.

We have completely solved two important problems in local cloning. For $D = 2$ (entangled qubits), we proved that no more than two states can be locally cloned, and that these states must be locally shifted. We showed that a two-qubit maximally entangled state is a necessary and sufficient resource for such a cloning. In addition, we provided necessary and sufficient conditions when the states are maximally entangled, valid for any dimension D, showing that the states must be group-shifted, and then we also provided an LOCC protocol that clones such a set of states.

We have studied in detail the local cloning of partially entangled group-shifted states and provided an explicit protocol for local cloning of such states with a maximally entangled resource. For $D = 3$ (entangled qutrits) we showed that a maximally entangled blank state is also necessary and sufficient, whereas for $D > 3$ we proved that the blank state has to be strictly more entangled than any state in $\mathcal{S}$, often by a sizable amount.

The necessary form of the clonable states for $D > 2$ remains an open problem. One might guess that the states have to be of a group-shifted form, but a proof of such a claim is not presently available. Although we proved the necessity of a maximally entangled resource for the $D = 2$ case and for group-shifted states in the $D = 3$ case, in higher dimensions it is still not clear if a maximally entangled state of Schmidt rank D is always necessary. Finally, it would be of interest to investigate the local cloning of less than full Schmidt rank states, a problem that is likely to bring in additional complications, such as the possibility of first distinguishing amongst the states in $\mathcal{S}$ while preserving the states intact [10], and then once the state is known, the cloning becomes straightforward with a blank state having Schmidt coefficients that are majorized by those of each of the states in $\mathcal{S}$ [8,17].

ACKNOWLEDGMENTS

The research described here received support from the National Science Foundation through Grant No. PHY-0757251. S.M.C. has also been supported by a grant from the Research Corporation.

APPENDIX A: MATHEMATICAL PROOFS

1. Proof of Lemma 5

Consider the singular value decomposition of S, $S = V\mathcal{D}U$ with $\mathcal{D}$ diagonal and positive definite, and V and U unitary operators. Using this expression for S in $T_f = SL(f)S^{-1}$ shows that

$$V^\dagger T_f V = \mathcal{D}(UL(f)U^\dagger)\mathcal{D}^{-1}, \tag{A1}$$

or with $\tilde{T}_f = V^\dagger T_f V$ and $\tilde{L}(f) = UL(f)U^\dagger$,

$$\tilde{T}_f\mathcal{D} = \mathcal{D}\tilde{L}(f). \tag{A2}$$

Left-multiply (or right-multiply) each side of this equation with the respective adjoint ($\mathcal{D}^\dagger\tilde{T}_f^\dagger$ and $\tilde{L}(f)^\dagger\mathcal{D}^\dagger$), and using the fact that $\tilde{T}_f$ and $\tilde{L}(f)$ are both unitary, we have that $\tilde{T}_f$ and $\tilde{L}(f)$ each commutes with $\mathcal{D}^\dagger\mathcal{D} = \mathcal{D}^2$. That is,

$$\begin{aligned}\mathcal{D}_i^2[\tilde{T}_f]_{ij} &= [\tilde{T}_f]_{ij}\mathcal{D}_j^2,\\ \mathcal{D}_i^2[\tilde{L}(f)]_{ij} &= [\tilde{L}(f)]_{ij}\mathcal{D}_j^2,\end{aligned} \tag{A3}$$

from which we conclude that when $\mathcal{D}_i \neq \mathcal{D}_j$, $[\tilde{T}_f]_{ij} = 0 = [\tilde{L}(f)]_{ij}$. By a judicious choice of U and V, we may arrange for $\mathcal{D}$ to be a direct sum of scalar matrices (some may be one-dimensional). That is, $\mathcal{D} = \oplus_\nu \alpha_\nu I_\nu$, and then we see that T_f and $L(f)$ share the same block-diagonal structure, with blocks corresponding to this direct sum decomposition of $\mathcal{D}$.

We also have directly from (A2) that

$$[\tilde{T}_f]_{ij}\mathcal{D}_j = \mathcal{D}_i[\tilde{L}(f)]_{ij}. \tag{A4}$$

Therefore, when $\mathcal{D}_j = \mathcal{D}_i$, $[\tilde{T}_f]_{ij} = [\tilde{L}(f)]_{ij}$, and we see that the blocks of $\tilde{T}_f$ are identical to those of $\tilde{L}(f)$. In other words, we have shown that $\tilde{T}_f = \tilde{L}(f)$ or, equivalently, $T_f = WL(f)W^\dagger$ with $W = VU$, completing the proof.

2. Proof of Lemma 10

Proof of (i). Let us introduce an ancillary system $\mathcal{H}_E$ of dimension D on Alice's side and construct the superposition,

$$|\Psi_{\text{in}}\rangle^{ABabE} := \sum_{f\in G}\sqrt{\mu_f}|\psi_f\rangle^{AB}\otimes|\phi\rangle^{ab}\otimes|f\rangle^E, \tag{A5}$$

with $\{\mu_f\}_{f\in G}$ an arbitrary set of non-negative real coefficients that satisfy $\sum_f \mu_f = 1$. The proof is based on the fact that if $|\psi_f\rangle^{AB}\otimes|\phi\rangle^{ab}$ is deterministically mapped to $e^{i\varphi_{mf}}|\psi_f\rangle^{AB}\otimes|\psi_f\rangle^{ab}$ [see (11)], then $|\Psi_{\text{in}}\rangle^{ABabE}$ will be deterministically mapped to an ensemble $\{p_m, |\Psi_{m,\text{out}}\rangle^{AaBbE}\}$, where

$$|\Psi_{m,\text{out}}\rangle^{AaBbE} = \sum_{f\in G} e^{i\varphi_{mf}}\sqrt{\mu_f}|\psi_f\rangle^{AB}\otimes|\psi_f\rangle^{ab}\otimes|f\rangle^E. \tag{A6}$$

Note that this conclusion rests crucially on the fact, discovered in the main text, that $p_{mf} = p_m$, independent of f.

Let us now write $|\Psi_{\text{in}}\rangle^{ABabE}$ in Schmidt form over the AaE/Bb cut. One has (again we use $\overline{f} = f^{-1}$)

$$\begin{aligned}&|\Psi_{\text{in}}\rangle^{ABabE}\\ &= \sum_{f\in G}\sqrt{\mu_f}\left(\sum_{g,h\in G} e^{i\vartheta_{f,g}}\sqrt{\lambda_g\gamma_h}|g\rangle^A|fg\rangle^B|h\rangle^a|h\rangle^b\right)|f\rangle^E\\ &= \sum_{f,g,h\in G} e^{i\vartheta_{f,g}}\sqrt{\mu_f\lambda_g\gamma_h}|g\rangle^A|h\rangle^a|f\rangle^E\otimes|fg\rangle^B|h\rangle^b\\ &= \sum_{g,h\in G}\left(\sum_{f\in G} e^{i\vartheta_{f,\overline{f}g}}\sqrt{\mu_f\lambda_{\overline{f}g}\gamma_h}|\overline{f}g\rangle^A|f\rangle^E\right)|h\rangle^a\otimes|g\rangle^B|h\rangle^b\\ &= \sum_{g,h\in G}\left(\sum_{f\in G} e^{i\vartheta_{\overline{f},fg}}\sqrt{\mu_{\overline{f}}\lambda_{fg}\gamma_h}|fg\rangle^A|\overline{f}\rangle^E\right)|h\rangle^a\otimes|g\rangle^B|h\rangle^b,\end{aligned} \tag{A7}$$

where we used the group property of G and replaced g by $\overline{f}g$ and summation over f by summation over $\overline{f}$ where

necessary. The states on the AaE system are orthogonal for different pairs of g,h, and therefore (A7) represents a Schmidt decomposition, with Schmidt coefficients $\alpha_{g,h}$ given by the squared norm of the states on the AaE system,

$$\alpha_{g,h} = \gamma_h \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}. \tag{A8}$$

A similar calculation yields for the Schmidt coefficients $\beta_{g,h}$ of $|\Psi_{m,\mathrm{out}}\rangle^{ABabE}$ the expression,

$$\beta_{g,h} = \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg} \lambda_{fh}, \tag{A9}$$

independent of m, which means that the average Schmidt vector of the output ensemble under the Aa/BbE cut is the same as the Schmidt vector of an individual state $|\Psi_{m,\mathrm{out}}\rangle^{ABabE}$.

We have proven in [17] that the average Schmidt vector of the output ensemble produced by a separable operation acting on a pure state has to majorize the input Schmidt vector, and this concludes (i).

Proof of (ii). The proof follows as a direct consequence of (i). A particular majorization inequality imposed by Lemma 10 (i) requires that the smallest Schmidt coefficients $\alpha_{\min}$ and $\beta_{\min}$ have to satisfy

$$\alpha_{\min} \geqslant \beta_{\min}, \tag{A10}$$

where α and β were defined in (A8) and (A9), respectively. This is equivalent to

$$\gamma_{\min} \geqslant \frac{\min_{g,h\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg} \lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}}. \tag{A11}$$

The above equation must hold regardless of which set of $\{\mu_f\}$ was chosen, hence, taking the maximum over all possible sets $\{\mu_f\}$ concludes the proof of (ii).

Proof of (iii). Inserting the expression (60) for $\{\mu_f\}$ in (A11) yields

$$\gamma_{\min} \geqslant \frac{\min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg} \lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}} \tag{A12}$$

$$= \frac{1}{D} \min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg} \lambda_{fh}, \tag{A13}$$

where (A13) follows from applying the rearrangement inequality to the denominator in (A12), which in this case reads as

$$\min_{g\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg} = \sum_{f\in G} \frac{1}{\lambda_f} \lambda_f = D. \tag{A14}$$

3. Proof of Theorem 11

Proof of (i). In this case the group G is the cyclic group of order 2, and we identify its group elements by $\{0,1\}$. We proved in Theorem 7 that the qubit states have to be locally shifted. The minimum in (61) of Lemma 10 (iii) becomes explicitly a minimum over four quantities that correspond to all possible pairings of g,h; a straightforward calculation shows that three out of these four quantities are equal to 1, except for $g = h = 1$, in which case the sum in (A13) equals $\lambda_1^2/\lambda_0 + \lambda_0^2/\lambda_1$. Order the λ's such that $\lambda_0 \geqslant \lambda_1$ and note that

$$\frac{1}{\lambda_0} \leqslant \frac{1}{\lambda_1}, \quad \text{and} \tag{A15}$$

$$\lambda_1^2 \leqslant \lambda_0^2. \tag{A16}$$

From the rearrangement inequality applied to (A15) and (A16) it follows that

$$\frac{\lambda_1^2}{\lambda_0} + \frac{\lambda_0^2}{\lambda_1} \geqslant \frac{\lambda_0^2}{\lambda_0} + \frac{\lambda_1^2}{\lambda_1} = 1, \tag{A17}$$

and hence the minimum in case (i) equals 1.

Proof of (ii). Now the group G is isomorphic to the cyclic group of order 3 and again we identify its elements by $\{0,1,2\}$. We order the λ's such that $\lambda_0 \geqslant \lambda_1 \geqslant \lambda_2$. The minimum in (A13) is now taken over nine possible pairs g,h. Again straightforward algebra shows that most expressions sum up to 1, except for the following three cases for which we show that the sum exceeds 1.

(1) $g = h = 1$, for which the sum in (A13) equals $\lambda_1^2/\lambda_0 + \lambda_2^2/\lambda_1 + \lambda_0^2/\lambda_2$;

(2) $g = h = 2$, for which the sum in (A13) equals $\lambda_2^2/\lambda_0 + \lambda_0^2/\lambda_1 + \lambda_1^2/\lambda_2$;

(3) $g = 1$, $h = 2$ or $g = 2$, $h = 1$, for which the sum in (A13) equals $\lambda_1\lambda_2/\lambda_0 + \lambda_2\lambda_0/\lambda_1 + \lambda_0\lambda_1/\lambda_2$.

Note first that

$$\frac{1}{\lambda_0} \leqslant \frac{1}{\lambda_1} \leqslant \frac{1}{\lambda_2}, \tag{A18}$$

$$\lambda_2{}^2 \leqslant \lambda_1{}^2 \leqslant \lambda_0{}^2, \quad \text{and} \tag{A19}$$

$$\lambda_1\lambda_2 \leqslant \lambda_2\lambda_0 \leqslant \lambda_0\lambda_1. \tag{A20}$$

From the rearrangement inequality applied to (A18) and (A19) it follows that

$$\frac{1}{\lambda_0}\lambda_1^2 + \frac{1}{\lambda_1}\lambda_2^2 + \frac{1}{\lambda_2}\lambda_0^2 \geqslant \frac{1}{\lambda_0}\lambda_0^2 + \frac{1}{\lambda_1}\lambda_1^2 + \frac{1}{\lambda_2}\lambda_2^2 = 1, \tag{A21}$$

which proves case 1, and

$$\frac{1}{\lambda_0}\lambda_2^2 + \frac{1}{\lambda_1}\lambda_0^2 + \frac{1}{\lambda_2}\lambda_1^2 \geqslant \frac{1}{\lambda_0}\lambda_0^2 + \frac{1}{\lambda_1}\lambda_1^2 + \frac{1}{\lambda_2}\lambda_2^2 = 1, \tag{A22}$$

which proves case 2.

Next apply the rearrangement inequality to (A18) and (A20) to get

$$\frac{1}{\lambda_0}(\lambda_1\lambda_2) + \frac{1}{\lambda_1}(\lambda_2\lambda_0) + \frac{1}{\lambda_2}(\lambda_0\lambda_1) \geqslant \frac{1}{\lambda_0}\lambda_0\lambda_1 + \frac{1}{\lambda_1}\lambda_1\lambda_2 + \frac{1}{\lambda_2}\lambda_0\lambda_2 = 1, \tag{A23}$$

and this proves case 3.

4. Proof of Theorem 12

By setting $\mu_f = 1/D$ in Lemma 10 (i), for all $f \in G$, the majorization relation (57) reads as

$$\frac{1}{D}\vec{\gamma} \times \vec{1} \prec \vec{\beta}, \tag{A24}$$

where $(1/D)\vec{\gamma} \times \vec{1}$ represents a D^2 component vector with components γ_h/D, each component repeated D times; here $\vec{\gamma}$ is the Schmidt vector of the blank state $|\phi\rangle^{ab}$. The D^2 components $\beta_{g,h}$ of $\vec{\beta}$ are given by

$$\beta_{g,h} = \frac{1}{D}\sum_{f\in G}\lambda_{fg}\lambda_{fh} = \frac{1}{D}\sum_{f\in G}\lambda_f\lambda_{f\bar{g}h}. \tag{A25}$$

Note that it is also the case that β has D components each repeated D times, so the majorization relation (A24) implies a majorization relation between two D-component vectors,

$$\vec{\gamma} \prec \vec{q}, \tag{A26}$$

where the rth component of $\vec{q}$ is given by

$$q_r := D\cdot\beta_{g,h}|_{\bar{g}h=r} = \sum_{f\in G}\lambda_f\lambda_{fr}. \tag{A27}$$

Note that both $\vec{\gamma}$ and $\vec{q}$ are normalized probability vectors. Since the Shannon entropy is a Schur-concave function, (A26) implies at once that

$$E(|\phi\rangle^{ab}) \geqslant H(\{q_r\}). \tag{A28}$$

We now show that the second inequality in (62) is strict. First we will prove that the ordered vector of probabilities $\vec{q}^{\downarrow}$, with components defined in (A27) and decreasing magnitudes of entries down its column, is majorized by $\vec{\lambda}^{\downarrow}$, the ordered vector of the λ_f,

$$\vec{q}^{\downarrow} \prec \vec{\lambda}^{\downarrow}. \tag{A29}$$

Since the Shannon entropy is not just Schur concave, but strictly Schur concave, this will imply at once that

$$H(\{q_r\}) \geqslant H(\{\lambda_f\}) = E(|\psi_f\rangle^{AB}), \quad \forall f \in G, \tag{A30}$$

with equality if and only if $\vec{q}^{\downarrow}$ equals $\vec{\lambda}^{\downarrow}$ (or, equivalently, if and only if the unordered vector $\vec{q}$ is the same as $\vec{\lambda}$ up to a permutation). One can see that $\vec{q}$ is not a permutation of $\vec{\lambda}$ unless all λ's are equal (case that we exclude). Hence, once we show the majorization condition (A29) holds, the proof will be complete.

We will actually show that $\vec{\lambda}^{\downarrow}$ majorizes every vector $\vec{q}$ of the q_r's no matter how $\vec{q}$ is ordered. Denote by S_n, with $|S_n| = n$ and $n = 1,\ldots,D-1$, the subset consisting of those elements $f \in G$ such that λ_f is one of the largest n of the λ's. Then, we need to show that for each n,

$$\sum_{g\in S_n}\lambda_g \geqslant \sum_{g\in S_n} q_{\sigma(g)} = \sum_{g\in S_n}\sum_{f\in G}\lambda_f\lambda_{f\sigma(g)}, \tag{A31}$$

where σ is an arbitrary permutation of the group elements. Since $\sum_f \lambda_f = 1$, this is equivalent to

$$\sum_{f\in G}\lambda_f\left[\sum_{g\in S_n}\lambda_g - \sum_{g\in S_n}\lambda_{f\sigma(g)}\right] \geqslant 0. \tag{A32}$$

However, given the way we have defined S_n, it is always true that the quantity in square brackets is non-negative. The reason is that the first term in this quantity is the sum of the n largest of the λ's. Therefore, the second term, which is also a sum of n of the λ's, cannot possibly be greater than the first. In fact, it is clear that for general sets of Schmidt coefficients $\{\lambda_f\}$, the quantity in square brackets will not be particularly small, implying that the gap between the required entanglement of the blank state and the entanglement of the states in $\mathcal{S}$ will be sizable. This ends the proof.

APPENDIX B: $|G| < D$ CASE

In the main body of the current paper, we restricted our consideration to the $|G| = D$ case. All of our results remain valid also when $|G| < D$, with minor modifications. Briefly, when $|G| < D$, $T_f^{(m)}$ is a direct sum of $n_t = D/|G|$ copies of $L(f)$, and the following theorems or lemmas have to be modified accordingly.

Theorem 6. Since Lemma 5 holds for any two unitary representations, it will hold when the regular representation $L(f)$ is replaced by a direct sum of a number of copies of $L(f)$. In this case, the maximally entangled group-shifted states (35) and (36) of Theorem 6 have the form,

$$|\psi_f\rangle^{AB} = \frac{1}{\sqrt{D}}\sum_{n=1}^{n_t}\sum_{g\in G}|fg,n\rangle^A|g,n\rangle^B, \tag{B1}$$

or

$$|\psi_f\rangle^{AB} = \frac{1}{\sqrt{D}}\sum_{n=1}^{n_t}\sum_{g\in G}|g,n\rangle^A|fg,n\rangle^B, \tag{B2}$$

respectively. Here, the states $\{|g,n\rangle\}_{g\in G,n=1,\ldots,n_t}$ are an orthonormal basis, $\langle g,n|h,m\rangle = \delta_{g,h}\delta_{n,m}$. The symbols $f,g \in G$ label the group elements and $m,n = 1,\ldots,n_t$ label the copies of the regular representation.

Theorem 8. When the family of partially entangled group-shifted states (45) is replaced by

$$|\psi_f\rangle^{AB} = \sum_{n=1}^{n_t}\sum_{g\in G}\sqrt{\lambda_{g,n}}|g,n\rangle^A|fg,n\rangle^B, \tag{B3}$$

and the maximally entangled blank state (46) is modified to

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}}\sum_{m=1}^{n_t}\sum_{h\in G}|h,m\rangle^a|h,m\rangle^b, \tag{B4}$$

the local cloning protocol of Theorem 8 continues to work, provided:

(1) The controlled-group unitary (47) is replaced by

$$\sum_{n=1}^{n_t}\sum_{g\in G}|g,n\rangle\langle g,n|\otimes P_g, \quad \text{with}$$
$$P_g = \sum_{m=1}^{n_t}\sum_{h\in G}|gh,m\rangle\langle h,m|. \tag{B5}$$

(2) The measurement (49) Alice performs is changed to

$$M_r = \sum_{m=1}^{n_t}\frac{1}{(\sum_{k\in G}\lambda_{k,m})^{1/2}}\sum_{h\in G}\sqrt{\lambda_{hr,m}}|h,m\rangle\langle h,m|, \tag{B6}$$

where the factor involving the sum over k is needed to ensure that this set of measurement operators corresponds to a complete measurement.

(3) Finally, the unitary correction (51) Alice and Bob perform is modified to

$$Q_r = \sum_{m=1}^{n_t} \sum_{h\in G} |hr,m\rangle\langle h,m|. \tag{B7}$$

Lemma 10. First the blank state has to be modified to

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}} \sum_{m=1}^{n_t} \sum_{h\in G} \sqrt{\gamma_{h,m}} |h,m\rangle^a |h,m\rangle^b. \tag{B8}$$

Next we follow the line of thought in Appendix A2. Even though there are only $|G| < D$ states in the clonable set $\mathcal{S}$, we still use a D-dimensional ancillary system $\mathcal{H}_E$ on Alice's side, with a basis now given by $\{|f,n\rangle^E\}_{f\in G, n=1,\ldots,n_t}$. Restricting to an ancillary system of dimension $|G|$ leads to unnecessary complications, since the rearrangement inequality can no longer be applied in part (ii) to obtain (iii).

We consider again an input superposition,

$$\sum_{n=1}^{n_t} \sum_{f\in G} \sqrt{\mu_{f,n}} |\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab} \otimes |f,n\rangle^E, \tag{B9}$$

and look at the Schmidt vector of the output ensemble produced by the separable operation acting on (B9), where $\{\mu_{f,n}\}$ is an arbitrary set of coefficients satisfying $\sum_{n=1}^{n_t} \sum_{f\in G} \mu_{f,s} = 1$. We then have:

(i) The majorization condition $\vec{\alpha} \prec \vec{\beta}$ corresponding to (57) holds, provided the vectors $\vec{\alpha}$ and $\vec{\beta}$ in (58) are redefined as

$$\begin{aligned} \alpha_{g,h}^{n,m} &= \gamma_{h,m} \sum_{s=1}^{n_t} \sum_{f\in G} \mu_{\overline{f},s} \lambda_{fg,n}, \\ \beta_{g,h}^{n,m} &= \sum_{s=1}^{n_t} \sum_{f\in G} \mu_{\overline{f},s} \lambda_{fg,n} \lambda_{fh,m}. \end{aligned} \tag{B10}$$

(ii) The smallest Schmidt coefficient $\gamma_{\min}$ of the blank has to satisfy

$$\gamma_{\min} \geqslant \max_{\{\mu_{f,s}\}} \frac{\min_{m,n} \min_{g,h\in G} \sum_{s=1}^{n_t} \sum_{f\in G} \mu_{\overline{f},s} \lambda_{fg,n} \lambda_{fh,m}}{\min_n \min_{g\in G} \sum_{s=1}^{n_t} \sum_{f\in G} \mu_{\overline{f},s} \lambda_{fg,n}}. \tag{B11}$$

(iii) A good choice of $\{\mu_{f,s}\}$ is given by $\mu_{f,s} = 1/\lambda_{\overline{f},s}$ [ignore the normalization, since $\mu_{f,s}$ appears both on the numerator and denominator of (B11)]. Then (B11) becomes

$$\gamma_{\min} \geqslant \frac{1}{|D|} \min_{m,n} \min_{g,h\in G} \sum_{s=1}^{n_t} \sum_{f\in G} \frac{1}{\lambda_{\overline{f},s}} \lambda_{fg,n} \lambda_{fh,m}. \tag{B12}$$

Theorem 12. Theorem 12 still provides a finite gap between the entanglement needed in the blank state and the entanglement of group-shifted states (B3). The proof follows the same ideas as before, by setting $\mu_{f,s} = 1/D$, for all $f \in G$ and $s = 1, \ldots, n_t$ in the majorization relation of the "modified" Lemma 10 (i) above.

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[2] S. Ghosh, G. Kar, and A. Roy, Phys. Rev. A **69**, 052312 (2004).
[3] F. Anselmi, A. Chefles, and M. B. Plenio, New J. Phys. **6**, 164 (2004).
[4] M. Owari and M. Hayashi, Phys. Rev. A **74**, 032108 (2006).
[5] A. Kay and M. Ericsson, Phys. Rev. A **73**, 012343 (2006).
[6] S. K. Choudhary, S. Kunkri, R. Rahaman, and A. Roy, Phys. Rev. A **76**, 052305 (2007).
[7] S. K. Choudhary, G. Kar, S. Kunkri, R. Rahaman, and A. Roy, Phys. Rev. A **76**, 062312 (2007).
[8] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[9] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[10] S. M. Cohen, Phys. Rev. A **75**, 052313 (2007).
[11] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th Ed. (Cambridge University Press, Cambridge, 2000).
[13] G. Gour, Phys. Rev. A **71**, 012318 (2005).
[14] K. Życzkowski and I. Bengtsson, Open Syst. Inf. Dyn. **11**, 3 (2004).
[15] R. B. Griffiths, S. Wu, L. Yu, and S. M. Cohen, Phys. Rev. A **73**, 052309 (2006).
[16] V. Gheorghiu and R. B. Griffiths, Phys. Rev. A **76**, 032310 (2007).
[17] V. Gheorghiu and R. B. Griffiths, Phys. Rev. A **78**, 020304 (2008).
[18] L. Yu, R. B. Griffiths, and S. M. Cohen, Phys. Rev. A **81**, 062315 (2010).
[19] M. Hamermesh, *Group Theory and Its Application to Physical Problems* (Dover Publications, Mineola, 1989).
[20] H. Michiel, *Encyclopaedia of Mathematics: Regular Representation* (Kluwer Academic Publishers, Dordrecht, 1995).
[21] Z.-Q. Ma, *Group Theory for Physicists* (World Scientific Publishing, Singapore, 2007).
[22] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities* (Cambridge University Press, Cambridge, 1999).
[23] A. Kay (private communication, 2006).