Strong bounds on required resources for quantum channels by local operations and classical communication

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

(Received 14 June 2019; published 21 October 2019)

Given a protocol $\mathcal{P}$ that implements multipartite quantum channel $\mathcal{E}$ by repeated rounds of local operations and classical communication (LOCC), we construct an alternate LOCC protocol for $\mathcal{E}$ in no more rounds than $\mathcal{P}$ and no more than a fixed, constant number of outcomes for each local measurement, the same constant number for every party and every round. We then obtain another upper bound on the number of outcomes that, under certain conditions, improves on the first. The latter bound shows that for LOCC channels that are extreme points of the convex set of all quantum channels, the parties can restrict the number of outcomes in their individual local measurements to no more than the square of their local Hilbert space dimension, d_α, suggesting a possible link between the required resources for LOCC and the convex structure of the set of all quantum channels. Our bounds on the number of outcomes indicating the need for only constant resources per round, independent of the number of rounds r including when that number is infinite, are a stark contrast to the exponential r dependence in the only previously published bound of which we are aware. If a lower bound is known on the number of product operators needed to represent the channel, we obtain a lower bound on the number of rounds required to implement the given channel by LOCC. Finally, we show that when the quantum channel is not required but only that a given task be implemented deterministically, then no more than d_α^2 outcomes are needed for each local measurement by party α.

DOI: 10.1103/PhysRevA.100.042324

I. INTRODUCTION

Economics is the study of how people use scarce resources to produce commodities for later consumption. Scientists designing experiments, as well as those who use their discoveries in everyday life, must take economics into account. These considerations have recently spawned studies of quantum resource theories [1–3], an outgrowth of quantum information science [4], which aim to quantify the costs of implementing exciting applications such as quantum teleportation [5] and quantum computing [6–8] under constraints imposed by circumstances. Entanglement [9], a fascinating property found in multipartite quantum systems involving an unusual and extremely strong type of correlation between the parts of these systems, was the first example of such a resource theory. An example of constraints imposed is the recognition that entanglement cannot be created by local operations on constituent subsystems, even when supplemented by classical communication between the acting parties, a paradigm known as LOCC [10], which plays an important role in many aspects of quantum information processing, including distributed quantum computing [11], entanglement distillation [12] and manipulation [13,14], local distinguishability of quantum states [15], local cloning [16,17], and various quantum cryptographic protocols, such as secret sharing [18]. Under the constraint of LOCC, which may arise due to spatial separation between constituent parts of a larger system, any entanglement must be supplied in advance and is therefore a valuable resource, whereas local operations and classical communication are each viewed as free. In reality, however, LOCC itself comes at a cost. Classical communication channels must be available to carry information from one party to another, those parties must have the means to make complex local measurements, and they must have the time available to implement the possibly numerous rounds of measuring and sharing information that may be needed.

The number of rounds needed for LOCC has received a fair amount of attention over recent years [19], showing that there are circumstances when a single round is as good as many [20] whereas, in other cases, two or more rounds [21], possibly even an infinite number [22], are necessary. In this paper, we consider a different resource for LOCC, a property that has heretofore received little attention: the complexity of making measurements and the corresponding amount of classical communication that must be exchanged between the parties at each round, both of which are determined by the number of outcomes in individual local measurements. Generalized measurements on system $\mathcal{S}$ can be performed by introducing an ancillary system $\mathcal{S}_a$ of dimension equal to the number of outcomes, interacting $\mathcal{S}_a$ with $\mathcal{S}$, and then performing a (projective) measurement on $\mathcal{S}_a$. As recently shown in [23], the interaction between $\mathcal{S}_a$ and $\mathcal{S}$ requires a time scaling as the squared dimension of the combined system $\mathcal{S}_a \otimes \mathcal{S}$. In addition, the ability to distinguish among the various outcomes of the measurement—which may, for example, be made using a Stern-Gerlach [24,25] type of apparatus—requires a level of spatial resolution that will also scale as the dimension of $\mathcal{S}_a$. Thus resource requirements increase with the number of outcomes of the desired measurement

*cohensm52@gmail.com

on $\mathcal{S}$. The question of the number of outcomes necessary at each round has been previously addressed for the case of finite-round LOCC protocols, in the context of showing that the set of all such protocols is compact [26]. It was shown there that if quantum channel $\mathcal{E}$ acts on a multipartite system of overall dimension D and can be implemented by an LOCC protocol consisting of a total of r rounds, then there exists an r-round protocol for $\mathcal{E}$ such that at round l there are no more than $D^{4(r-l+1)}$ outcomes in any local measurement [26]. This result was important in that, prior to this work, there was every possibility that "intermediate measurements with an unbounded number of outcomes" could be necessary at any point during the protocol [26]. The result scales poorly with r, however, and leaves open the possibility that an unbounded number of outcomes continue to be necessary within infinite-round protocols. Below, we obtain upper bounds on the required number of outcomes at each round which are (1) independent of r (and of l), (2) never greater than D^4, and (3) applicable to both finite- and infinite-round protocols, strongly bounding the required resources for LOCC. Depending on certain parameters, these bounds can be surprisingly small.

Our upper bounds on the number of outcomes in local measurements can have important practical applications, examples of which have already been mentioned above. If, as had been believed prior to the present results, a protocol had required any given party to make measurements at different rounds with widely differing numbers of outcomes, they would have needed to either use different measuring apparatuses for different measurements or else use a single apparatus capable of measurements with a larger number of outcomes than necessary. The latter option would require larger ancillae and thus more space and more time [23] to implement than would at times be necessary, whereas the former option would obviously be more costly in a variety of ways. Therefore, the ability to limit the required number of outcomes at every round throughout the protocol can represent a significant savings in resources. It should also be mentioned that our upper bounds can be useful in simplifying the design of protocols [27], making them more computationally tractable by reducing the number of outcomes that one must search for at each round.

Recently, we learned that Leung, Winter, and Yu [28] have obtained results related to our own. They have also shown how to "compress" an LOCC protocol to one that has a limited number of outcomes for each local measurement, and their compression will often yield a tighter bound than ours, but the reverse situation can also hold. Their main results apply to protocols aimed at achieving certain tasks, whereas our compression works for all protocols while preserving the desired quantum channel. A result applicable for channels is also obtained in Ref. [28] but requires that the parties have access to shared randomness, without which the desired channel cannot be recovered using their approach. In contrast, our results are "pure" in the sense that we limit resources without the parties needing to replace that resource with another. In addition, the compression of individual measurements for that particular result in Ref. [28] requires consideration of later rounds, whereas our compression is simple: each local measurement is compressed by considering that measurement alone, and nothing else.

The rest of the paper is organized as follows. In Sec. II, we review the mathematics needed to describe quantum channels and LOCC, and then we prove Theorem 1 and Lemma 1, each of which will be used in obtaining our main results. In Sec. III, we present our main results in the form of two theorems and two corollaries, which concern the number of outcomes needed in individual local measurements utilized within LOCC protocols implementing a given quantum channel. Finally, in Sec. IV, we discuss our results and then prove an additional theorem concerning execution of any task deterministically by LOCC, for conditions under which implementation of a specific quantum channel is not of concern.

II. MATHEMATICAL TOOLS

We consider the evolution, $\mathcal{E}$, of a multipartite quantum system interacting with an environment, viewed as a noisy quantum channel [29,30] mapping initial quantum state ρ, an operator on Hilbert space $\mathcal{H}$ of dimension D, to state $\mathcal{E}(\rho)$. The channel $\mathcal{E}$ may be represented in terms of a set of Kraus operators [31,32], K_i, as

$$\mathcal{E}(\rho) = \sum_{i=1}^{N} K_i \rho K_i^\dagger, \tag{1}$$

with

$$\sum_{i=1}^{N} K_i^\dagger K_i = I_{\mathcal{H}}, \tag{2}$$

where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$. This collection of Kraus operators is referred to as a Kraus representation of $\mathcal{E}$ and such representations are not unique. Without loss of generality, we assume that set $\{K_i\}$ is a minimal set, in the sense that no smaller set of Kraus operators represents $\mathcal{E}$. The Kraus rank κ of $\mathcal{E}$ is defined as the size of this minimal set, so $N = \kappa$, where $1 \leqslant \kappa \leqslant D^2$. Any other set of Kraus operators, $\{K'_j\}_{j=1}^{N'}$, describes the same channel as the original set if and only if there exists [4] an isometry V, $V^\dagger V = I_\kappa$ with I_κ the $\kappa \times \kappa$ identity matrix, such that for each $j = 1, \ldots, N'$,

$$K'_j = \sum_{i=1}^{\kappa} V_{ji} K_i. \tag{3}$$

We consider quantum channels implemented by LOCC protocols. An LOCC protocol involves one party making a measurement, informing the other parties of her outcome, after which, according to a preapproved plan, one of the other parties performs the next measurement, and so on. Since each local measurement involves a number of possible outcomes, the entire process is commonly represented as a rooted tree, $\mathcal{L}$, the children of any given node representing the set of outcomes of the local measurement made at that stage in the protocol. We associate with each node $n \in \mathcal{L}$ the accumulated action of all the parties up to that stage in the protocol, which may be represented by a Kraus operator $\hat{K}_n$, or more conveniently for our purposes, the corresponding POVM element, $E_n = \hat{K}_n^\dagger \hat{K}_n \geqslant 0$. Since each measurement in an LOCC protocol is local, being performed by a single party while all the other parties do nothing, E_n is a tensor product operator, of the form $A \otimes B \otimes \cdots$. The root node

represents the situation before the parties have done anything, so is labeled by—and we will say, is equal to—the identity operator on the full Hilbert space, $\mathcal{I}_{\mathcal{H}}$. A branch starts at the root and stretches via an edge from each node on that branch to one of its children, either continuing without end or else terminating at what is known as a leaf node. As we have discussed elsewhere [27], if the tree $\mathcal{L}$ represents an LOCC protocol (finite or infinite), which implements the set of Kraus operators $\{K'_j\}$, then E_n is equal to a positive linear combination of the set of operators, $\{K'^{\dagger}_j K'_j\}$, and each leaf node l is proportional to one of the $K'^{\dagger}_j K'_j$ with positive constant of proportionality, say $c^{(l)}_j$. That $\mathcal{L}$ implements $\{K'_j\}$ means that the sum of coefficients $c^{(l)}_j$ over all those leaf nodes corresponding to the same j is equal to unity, which we represent (somewhat loosely) as $\sum_{l\in j} c^{(l)}_j = 1$. This is necessary so that the Kraus representation implemented by $\mathcal{L}$ includes each K'_j precisely, rather than $\sqrt{\hat{c}_j}K'_j$ for some constant $\hat{c}_j \neq 1$. Then, if this tree $\mathcal{L}$ implements quantum channel $\mathcal{E}$, we see using Eq. (3) that

$$E_n = \sum_{j=1}^{N'} c^{(n)}_j K'^{\dagger}_j K'_j = \sum_{i,i'=1}^{\kappa} \left[\sum_{j=1}^{N'} V^*_{ji} c^{(n)}_j V_{ji'} \right] K^{\dagger}_i K_{i'}$$
$$= \sum_{i,i'=1}^{\kappa} C^{(n)}_{ii'} K^{\dagger}_i K_{i'}, \tag{4}$$

with $c^{(n)}_j \geqslant 0$ for all j, n and $C^{(n)}_{ii'} := \sum_{j=1}^{N'} V^*_{ji} c^{(n)}_j V_{ji'}$. Since V is an isometry, $C^{(n)}$ is a positive semidefinite matrix, $C^{(n)} \geqslant 0$. We note that the matrix $C^{(n)}$ encodes information about the weights of those final outcomes of the protocol that are descended from node n, through the eigenvalues $c^{(n)}_j$, as well as information about precisely what those final outcomes K'_j are through the isometry V that diagonalizes $C^{(n)}$. Note also that if l is a leaf node, then as pointed out above, $E_l = c^{(l)}_J K'^{\dagger}_J K'_J$ for some fixed J (no summation). This implies that the rank of matrix $C^{(l)}$ is equal to unity for each leaf node in the tree, and given that $C^{(l)} \geqslant 0$, we have that $C^{(l)} = \vec{v}_l \vec{v}_l{}^{\dagger}$ at each leaf node, with $(\vec{v}_l)_i = \sqrt{c^{(l)}_J} V^*_{Ji}$. Index J depends on l with a possibly one-to-many relationship (many leaf nodes implementing the same Kraus operator), and as noted above Eq. (4), $\sum_{l\in J} c^{(l)}_J = 1$. The associated Kraus operator at leaf node l is then $K''_l = \sqrt{c^{(l)}_J} K'_J = \sqrt{c^{(l)}_J} \sum_i V_{Ji} K_i$.

The main tool for our arguments will be the following theorem. It provides a necessary and sufficient condition for a tree graph to represent an LOCC protocol implementing quantum channel $\mathcal{E}$, with each node in the tree labeled by a positive semidefinite $\kappa \times \kappa$ matrix $C^{(n)}$.

Theorem 1. Quantum channel $\mathcal{E}$, represented by the (minimal) set of Kraus operators $\{K_i\}_{i=1}^{\kappa}$, can be implemented by LOCC if and only if there exists a tree graph $\mathcal{L}$ satisfying all of the following conditions.

(1) For each node $n \in \mathcal{L}$ and its associated $\kappa \times \kappa$ matrix $C^{(n)} \geqslant 0$, $E_n = \sum_{i,i'} C^{(n)}_{ii'} K^{\dagger}_i K_{i'}$ is a product operator.

(2) The root node is labeled by matrix $C^{(0)} = I_\kappa$, so that $\sum_{i,i'} C^{(0)}_{ii'} K^{\dagger}_i K_{i'} = I_{\mathcal{H}}$.

(3) For each node n and operator E_n, the collection of its child nodes, s, with operators E_s, satisfy $\sum_{s\in \text{siblings}} E_s = E_n$.

(4) Each node n along with each of its child nodes, $s \in$ siblings, correspond to positive semidefinite product operators E_n and E_s that differ in only one party's local operator, that being the same party for all of them. For example, if it is party A, all sibling nodes are of the form $E_s = \sum_{i,i'} C^{(s)}_{ii'} K^{\dagger}_i K_{i'} = \mathcal{A}^{(s)} \otimes \bar{\mathcal{A}}$ with parent $E_n = \mathcal{A}^{(n)} \otimes \bar{\mathcal{A}}$, where $\bar{\mathcal{A}}$ is a positive semidefinite operator that acts, and is a tensor product, on all parties other than A (the same operator for all of these nodes), and by the preceding item (1), $\sum_{s\in \text{siblings}} \mathcal{A}^{(s)} = \mathcal{A}^{(n)}$.

(5) (a) For every leaf node l, $C^{(l)} = \vec{v}_l \vec{v}_l{}^{\dagger}$, and so has rank equal to one; (b) for any infinite-round protocol, the condition of the preceding item [5(a)] is satisfied asymptotically.

(6) (a) The sum of all leaf nodes in any finite-round protocol is equal to the root node: $\sum_l C^{(l)} = C^{(0)} = I_\kappa$; (b) for any infinite-round protocol, the condition of the preceding item [6(a)] is satisfied asymptotically.

Proof. Item (1) is just the well-known condition that LOCC protocols can only implement product operators. Item (2) just says that at the beginning of the protocol, no party has done anything yet. Item (3) is just the condition that each local measurement is complete, in the sense that the probabilities of all outcomes of any given measurement must sum to unity.[1] Item (4) is the condition that the parties take turns making measurements, only one party measuring at any given time. Item [5(a)] is necessary and sufficient that the collection of final outcomes of the protocol constitute an implementation of the channel $\mathcal{E}$, a conclusion that follows from the discussion after Eq. (4).

For item [6(a)], consider the set of leaf nodes l in any finite protocol $\mathcal{P}$. By assumption $\mathcal{P}$ implements $\mathcal{E}$, or in other words, a Kraus representation $\{K'_j\}$ of $\mathcal{E}$. As discussed in the paragraph following Eq. (4), we have that $(v_l)_i = \sqrt{c^{(l)}_j} V^*_{ji}$ with $\sum_{l\in j} c^{(l)}_j = 1$. Thus $(\sum_l \vec{v}_l \vec{v}^{\dagger}_l)_{ii'} = \sum_j \sum_{l\in j} c^{(l)}_j V^*_{ji} V_{ji'} = \delta_{ii'}$ and it then follows that $\sum_l \vec{v}_l \vec{v}^{\dagger}_l = I_\kappa$, proving the claim.

Items [5(b)] and [6(b)] require a bit more explanation. In discussing an infinite-round protocol, we envision a sequence of finite-round protocols, $\{\mathcal{P}_m\}$, with each $\mathcal{P}_m$ implementing quantum channel $\mathcal{E}_m$ in m rounds, and $\mathcal{P}_m$ differs from $\mathcal{P}_{m-1}$ only by the addition of an mth round. If the set of Kraus operators implemented by $\mathcal{P}_m$ is $\mathbf{K}_m = \{K^{(m)}_j\}_j$, then $\mathbf{K}_m$ is a Kraus representation of $\mathcal{E}_m$. By saying that an infinite-round protocol implements channel $\mathcal{E}$, we mean $\lim_{m\to\infty} \mathcal{E}_m = \mathcal{E}$. One can then show (using the diamond norm for quantum channels) that this latter statement is equivalent to having $K^{(m)}_j = \sum_i V^{(m)}_{ji} K_i + O(\epsilon)$ for each j, where $\mathbf{K} = \{K_i\}_i$ is a (minimal) Kraus representation of $\mathcal{E}$, $V^{(m)}$ is an isometry, and

[1] Note that when the set $\{K^{\dagger}_i K_j\}$ is linearly independent, then Eq. (4) implies that also $\sum_{s\in \text{siblings}} C^{(s)} = C^{(n)}$. If, on the other hand, that set is linearly dependent, the latter conclusion does not immediately follow. For any finite protocol we can construct a set of matrices $C^{(n)}$ for each n such that it does hold, simply by working backward from the leaf nodes. It is not clear to us, however, that there is a straightforward way to take the limit to infinite rounds, but we will not need this condition to obtain our results.

$\epsilon \to 0$ when $m \to \infty$. Therefore, in this limit, the protocol implements a set of Kraus operators that are related to those in **K** through an isometry, which, according to the discussion following Eq. (4), implies item [5(b)] directly. In addition, item [6(b)] follows immediately from item [6(a)]: since the latter holds for each finite protocol $\mathcal{P}_m$, it also holds in the limit. ■

Our main results will be direct consequences of the following lemma.

Lemma 1. If multipartite quantum channel $\mathcal{E}$ can be implemented by LOCC in r rounds, where r may be infinite, then there exists an LOCC implementation of $\mathcal{E}$ using no more than r rounds such that, for each local measurement, the collection of matrices $\{C^{(s)}\}$ corresponding to the outcomes of that measurement (these outcomes indexed by s) is a linearly independent set.

Proof. Suppose tree $\mathcal{L}$ represents a protocol that implements the desired channel $\mathcal{E}$. Let us consider node $n \in \mathcal{L}$, and assume matrices $C^{(s)}$ associated with its children collectively form a linearly dependent set. We will give a constructive argument showing that the number of these children can be reduced by unity. This will prove the lemma, since we can continue this process for as long as the children remain dependent.

Since $C^{(s)} \geqslant 0$, linear dependence implies the existence of a vanishing real linear combination of these matrices. By a judicious choice of s_1, there then exist coefficients q_s such that

$$C^{(s_1)} = \sum_{s \neq s_1} q_s C^{(s)}, \tag{5}$$

with $|q_s| \leqslant 1$ and the sum is over all siblings of s_1. This means that if we omit node s_1, along with all of its descendants (including those that extend to infinity along infinite branches), and replace each sibling of s_1 by $C^{(s)} \to (1 + q_s)C^{(s)}$, then the sum of the remaining children of node n is still equal to $C^{(n)}$, as required. In addition, this procedure cannot increase the number of rounds. Note that, since $1 + q_s \geqslant 0$, these replacement matrices continue to be positive semidefinite. Therefore, this new local measurement is still a valid one at this stage of the protocol. Nonetheless, there remain two questions that need be considered before we are done. First, do the descendants of those remaining children continue to constitute a valid protocol? They do not, as they were, but they can easily be altered to become valid, by replacing every node, t, descendant from child node s, by $C^{(t)} \to (1 + q_s)C^{(t)}$. By doing so, every set of children of a given node continues to satisfy the conditions of Theorem 1; in particular, conditions (1) and (3) of that theorem, that the nodes correspond to positive semidefinite product operators that sum to their parent, are still satisfied.

This demonstrates that, following omission of s_1 and all its descendants, we are still left with a valid LOCC protocol. However, it remains to be shown that this new protocol continues to implement the same, desired quantum channel $\mathcal{E}$. To see that it does, let us start by considering a finite-round protocol $\mathcal{P}$. The leaf nodes remaining after trimming this tree are a subset of the same leaf nodes that were in the original protocol, though some have been modified as just described. As noted above, see the paragraph following Eq. (4), each remaining leaf node l is $C^{(l)} = \vec{v}_l \vec{v}_l{}^\dagger$ with $(\vec{v}_l)_i = \sqrt{\tilde{c}_J^{(l)}} V_{Ji}^*$ for some fixed index J, which depends on l ($\tilde{c}_J^{(l)}$ is a product of $c_J^{(l)}$ and possibly a factor of $1 + q_s$). Furthermore, by construction this collection of leaf nodes continues to satisfy conditions (2) and (6) of Theorem 1; that is, since the root node is unchanged in our procedure,

$$\sum_l C^{(l)} = C^{(0)} = I_\kappa, \tag{6}$$

and summation here is over all leaf nodes remaining in the pruned tree. By looking at matrix elements of this expression, this yields

$$\sum_l v_{lj} v_{li}^* = \delta_{ij}. \tag{7}$$

We see that the pruned tree implements the collection of Kraus operators [see the discussion following Eq. (4)]

$$K_l'' = \sum_{j=1}^{\kappa} v_{lj} K_j, \tag{8}$$

where, according to Eq. (7), the collection of matrix elements v_{lj} constitute an isometry.[2] By the isometric freedom in operator-sum representations of quantum channels, we thus see that this modified protocol, which uses no more rounds than the original protocol, implements a valid set of Kraus operators for the desired channel $\mathcal{E}$. This completes the proof for finite-round protocols.

For infinite-round protocols, recall the discussion in the last paragraph of the proof of Theorem 1, where we introduced a sequence of finite-round protocols $\mathcal{P}_m$, each implementing channel $\mathcal{E}_m$, respectively. Then, simply notice that we have just proved that each (finite-round) $\mathcal{P}_m$ continues to implement the same channel $\mathcal{E}_m$ as it did before being pruned. Since the original sequence of protocols implemented $\mathcal{E}$ in the limit to begin with, we know that $\lim_{m\to\infty} \mathcal{E}_m = \mathcal{E}$. Therefore, the limiting infinite-round protocol continues to implement $\mathcal{E}$ after being pruned. This completes the proof. ■

III. MAIN RESULTS

Recall from earlier discussion that matrices $C^{(s)} \geqslant 0$ are of size $\kappa \times \kappa$, implying there can be no more than κ^2 of these matrices in any linearly independent set. Therefore, the next theorem follows immediately from Lemma 1.

Theorem 2. If multipartite quantum channel $\mathcal{E}$ can be implemented by LOCC in r rounds, where r may be infinite, then there exists an LOCC implementation of $\mathcal{E}$ using no more than r rounds such that no local measurement in the protocol has more than κ^2 outcomes.

[2]What we have effectively done here is to delete a subset of rows in the original isometry V, scaling each remaining row by some non-negative factor. We have also essentially proven that, for every isometry V that corresponds to an LOCC protocol containing intermediate measurements involving sets of linearly "dependent children," what remains after this process of deletions and rescalings is still an isometry.

If a channel is LOCC in a finite number of rounds, r, then after reducing the protocol as described in the proof of Lemma 1, there will be no more than κ^{2r} leaf nodes in the tree representing the resulting protocol. Since each Kraus operator in the Kraus representation implemented by this finite-round protocol must be a leaf node, we have that $N_p \leqslant \kappa^{2r}$, where N_p is the minimum number of operators in any Kraus representation of $\mathcal{E}$. Therefore, the following corollary is a direct consequence of Theorem 2.

Corollary 1. If the smallest Kraus representation of quantum channel $\mathcal{E}$ by product Kraus operators has at least N_p members, then the number of rounds, r, required to implement $\mathcal{E}$ by LOCC is lower bounded as $r \geqslant \log N_p / \log \kappa^2$.

If $N_p < \kappa^2$, the bound in this corollary is trivial and provides no information. On the other hand, for $N_p \gg \kappa^2$ the bound provides useful guidance as to the difficulty of implementing the given channel by LOCC, including that, in the limit as $N_p \to \infty$, we have that the channel cannot be implemented by finite-round LOCC. It should be noted, however, that determining N_p is likely not a simple task.

Theorem 2 applies in complete generality to all quantum channels, and depends only on the Kraus rank κ of the given channel. The upper bound on the number of outcomes needed in intermediate measurements is independent of the size of the Kraus representation actually implemented, and it is even independent of the size, N_p, of the smallest possible product Kraus representation. It is thus seen to be a strong result, indicating a significant constraint on required resources, especially when κ is small. It turns out, however, that this result can often be strengthened, in some cases considerably. This stronger result is stated in the following theorem, where we denote as χ the dimension of the subspace spanned by the set of operators $\{K_i^\dagger K_j\}_{i,j=1}^{\kappa}$, and it is not difficult to show that χ is a characteristic property of the channel, being independent of the chosen Kraus representation.

Theorem 3. If multipartite quantum channel $\mathcal{E}$ has Kraus rank κ and can be implemented by LOCC in r rounds, where r may be infinite, then there exists an LOCC implementation of $\mathcal{E}$ using no more than r rounds such that no local measurement in the protocol has more than $d_\alpha^2 + \kappa^2 - \chi$ outcomes, for each party α (d_α is the dimension of the Hilbert space describing the states of party α's subsystem).

Proof. If $\chi \leqslant d_\alpha^2$, then the bound of Theorem 2 already implies the desired result, so assume $\chi > d_\alpha^2$. Let us consider a measurement by Alice (party A) consisting of N_A outcomes $\mathcal{A}_s \otimes \bar{\mathcal{A}}$, where $\bar{\mathcal{A}}$ is an operator acting on the composite of all subsystems other than A, this operator being the same for all outcomes because only Alice is measuring; see item (4) of Theorem 1. Each outcome is associated with a matrix $C^{(s)}$, so by Lemma 1, proof of this theorem will follow from showing that no more than $d_A^2 + \kappa^2 - \chi$ of these matrices can be linearly independent. Let us write

$$C^{(s)} = \sum_{t=1}^{\kappa^2} M_{st} Q^{(t)}, \tag{9}$$

where the $Q^{(t)}$ constitute an orthonormal basis of the space of $\kappa \times \kappa$ matrices, $\mathrm{Tr}(Q^{(t)\dagger} Q^{(t')}) = \delta_{tt'}$, and we also choose these basis elements such that they correspond to the $\kappa^2 - \chi$ (independent) linear dependencies of the $K_i^\dagger K_j$; that is,

$$0 = \sum_{i,j=1}^{\kappa} Q_{ij}^{(t)} K_i^\dagger K_j, \tag{10}$$

when $t > \chi$. Then we can write the outcomes of Alice's measurement as

$$\begin{aligned} \mathcal{A}_s \otimes \bar{\mathcal{A}} &= \sum_{i,j=1}^{\kappa} C_{ij}^{(s)} K_i^\dagger K_j = \sum_{t=1}^{\kappa^2} M_{st} \sum_{i,j=1}^{\kappa} Q_{ij}^{(t)} K_i^\dagger K_j \\ &= \sum_{t=1}^{\chi} M_{st} \mathcal{K}^{(t)}, \end{aligned} \tag{11}$$

with $\mathcal{K}^{(t)} := \sum_{ij} Q_{ij}^{(t)} K_i^\dagger K_j$, and we have used Eq. (10) to reduce the sum to just χ terms in the final expression. Note that orthogonality of the $Q^{(t)}$ matrices ensures that operators $\mathcal{K}^{(t)}$ are linearly independent for $t = 1, \ldots, \chi$ because otherwise there would be additional dependencies among the $K_i^\dagger K_j$, contrary to assumption.

Since $\chi \leqslant \kappa^2$, if the number of outcomes satisfies $N_A \leqslant d_A^2$, then $N_A \leqslant d_A^2 + \kappa^2 - \chi$, which is what we are trying to prove. Therefore, we only need consider the case that $N_A > d_A^2$. So suppose there are $N_A > d_A^2$ outcomes $\mathcal{A}_s \otimes \bar{\mathcal{A}}$, $s = 1, \ldots, N_A$. Then since with $\bar{\mathcal{A}}$ fixed, no more than d_A^2 of these can be linearly independent, there must exist $N_A - d_A^2$ linearly independent vectors $\vec{\lambda}^{(p)}$ in N_A dimensions having elements $\lambda_s^{(p)}$ not all zero such that

$$0 = \sum_{s=1}^{N_A} \lambda_s^{(p)*} \mathcal{A}_s \otimes \bar{\mathcal{A}} = \sum_{t=1}^{\chi} \sum_{s=1}^{N_A} \lambda_s^{(p)*} M_{st} \mathcal{K}^{(t)}, \tag{12}$$

for $p = 1, \ldots, N_A - d_A^2$. By the linear independence of the $\mathcal{K}^{(t)}$ that appear in this expression, this implies that

$$\sum_{s=1}^{N_A} \lambda_s^{(p)*} M_{st} = 0, \tag{13}$$

for all $t \leqslant \chi$. This means that the first χ columns of matrix M, consisting of matrix elements M_{st}, are each orthogonal to the $(N_A - d_A^2)$-dimensional subspace spanned by the collection of vectors $\vec{\lambda}^{(p)}$. Since these first χ columns of M are N_A dimensional, there can be no more than d_A^2 of them in any linearly independent subset. There are $\kappa^2 - \chi$ remaining columns in M, so the rank of M cannot exceed $d_A^2 + \kappa^2 - \chi$. This implies that the entire collection of columns of M span a subspace of dimension no more than $d_A^2 + \kappa^2 - \chi$. Therefore, if $N_A \geqslant d_A^2 + \kappa^2 - \chi$, there exists a nonzero N_A-dimensional vector $\vec{\lambda}'$, elements λ_s', orthogonal to every column of M. That is, $\sum_s \lambda_s'^* M_{st} = 0$ for all t. Multiplying Eq. (9) by $\lambda_s'^*$ and summing over s, we immediately see that the $C^{(s)}$ are linearly dependent, and we reach the conclusion that no more than $d_A^2 + \kappa^2 - \chi$ of the $C^{(s)}$ can be linearly independent. Since the same argument holds for any of the parties, and by reference to Lemma 1, this completes the proof. ∎

Finally, we note that channel $\mathcal{E}$ is an extreme point of the convex set of all quantum channels if and only if $\chi = \kappa^2$ [33]. This leads us to the following corollary as an immediate consequence of Theorem 3, suggesting a possible connection

between the required resources for LOCC and the convex structure of the set of all quantum channels.

Corollary 2. If $\mathcal{E}$ is an extreme point of the set of all quantum channels and can be implemented by LOCC in r rounds, where r may be infinite, then it can be implemented by an LOCC protocol using no more than r rounds in which, for each party α, no more than d_α^2 outcomes are used in each local measurement by that party in the entire sequence of rounds of the protocol.

IV. CONCLUSIONS

In summary, we have derived strong upper bounds on the number of outcomes that each intermediate measurement need have in any LOCC protocol implementing a quantum channel $\mathcal{E}$, no matter how many rounds are involved, including if the number of rounds is infinite. These bounds are presented in Theorems 2 and 3, and they are independent of the round number and of the total number of rounds. These theorems bound the resources required for LOCC without the need to replace them with resources of a different type. They lead directly to Corollary 1, which provides a lower bound on the number of rounds needed to implement $\mathcal{E}$ if a lower bound on the number of product operators in any product Kraus representation of $\mathcal{E}$ is known, and Corollary 2, which suggests a possible link between the convex structure of the set of quantum channels and the resources needed to implement those channels by LOCC. It is perhaps worth pointing out that Theorem 2 (and thus Corollary 1), which depends only on the Kraus rank κ of $\mathcal{E}$, provides a bound that is independent of the way the parties are partitioned. That is, for example, if two or more of the original parties are able to merge together to act as one, κ, and therefore this bound, remains unchanged. Note also that χ is independent of partitioning, as well. Therefore, merging (or splitting) the parties only changes the bound in Theorem 3 by changing the local dimensions d_α.

We would like to make clear that the crucial step in achieving these results is the representation of LOCC protocols in terms of the $\kappa \times \kappa$ matrices $C^{(n)}$, introduced in [27] and described here in Eq. (4). It is these matrices that have allowed us to show that our tree-pruning procedure, described in the proof of the critical Lemma 1 where all sets of sibling nodes are reduced to linearly independent sets of these $C^{(n)}$ matrices, leaves the quantum channel implemented by the protocol unchanged; see the argument leading to Eqs. (7) and (8). One might try to prune these trees differently, in ways that leave sets of sibling nodes linearly independent when viewing these nodes as positive semidefinite operators E_n, or even as Kraus operators, but such efforts appear to be doomed to failure. In the case of labeling by E_n, one can easily prune in this way such that the tree remains a valid LOCC protocol, but it will not generally implement the same channel as the unpruned tree. For example, suppose in the original protocol for $\mathcal{E}$ there is a terminal measurement (every outcome corresponding to a leaf node) where the collection of sibling operators E_s obeys a single linear dependency, but the collection of matrices $C^{(s)}$—which have rank equal to unity according to item (5) of Theorem 1—is linearly independent. Then, in eliminating one of the E_s (say E_{s_1}, with s_1 one of the original leaf nodes) to end up with a linearly independent set of the remaining E_s, the remaining $C^{(s)}$ matrices will be replaced by new matrices that are positive linear combinations of two of the original $C^{(s)}$ matrices; specifically, $C^{(s)} + q_s C^{(s_1)}$ (see the proof of Lemma 1). Since $C^{(s)}$ and $C^{(s_1)}$ are linearly independent, rank-1, positive semidefinite matrices, such linear combinations cannot themselves have rank equal to unity and thus, again according to item (5) of Theorem 1, the resulting LOCC protocol no longer implements the original channel $\mathcal{E}$. Of course, this raises the question of whether it may be possible to improve on these bounds, or if our bounds may themselves be tight for the implementation of a given quantum channel (without the availability of sufficient shared randomness [28]). We are presently unable to provide an intelligent guess as to which of these possibilities is more likely, but it is certainly a question that deserves further study.

Notice that pruning in a way that leaves sibling E_s operators linearly independent fails only because of the need to retain the rank-1 condition on leaves of the tree in order to preserve implementation of the same channel $\mathcal{E}$. It may be that we do not need to implement a given channel but instead only care about accomplishing a given task. Consider, then, a "deterministic" LOCC protocol, by which we mean that every leaf in the tree is successful in completing a given task, and for each infinite branch (if any), successful completion of the task is approached asymptotically. Examples include deterministic local state transformation [13,14] and deterministic local cloning [16,17]. Since every branch in such protocols is successful, we may prune these trees to leave sibling E_s operators linearly independent such that the resulting tree—whose branches are a subset of those in the original protocol—also represents a deterministic protocol for the given task. Since each local measurement (for example, by Alice) produces sibling E_s operators of the form $\mathcal{A}_s \otimes \overline{\mathcal{A}}$ with $\overline{\mathcal{A}}$ the same for all these children, and since the $\mathcal{A}_s$ operate on a space of dimension d_A, no more than d_A^2 of these E_s operators can be linearly independent. We have thus proved, and will end with, the following theorem.

Theorem 4. Suppose we have an LOCC protocol that deterministically implements a given task in r rounds, where r may be infinite. Then there exists an LOCC protocol that also deterministically implements the given task using no more than r rounds, and such that no local measurement in the protocol has more than d_α^2 outcomes for each party α.

ACKNOWLEDGMENTS

We wish to thank D. Leung, B. Kraus, and C. Spee for helpful discussions.

[1] M. Horodecki and J. Oppenheim, (Quantumness in the context of) resource theories, Int. J. Mod. Phys. B **27**, 1345019 (2013).

[2] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[3] F. G. S. L. Brandão and G. Gour, Reversible Framework for Quantum Resource Theories, Phys. Rev. Lett. **115**, 070503 (2015).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[5] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State Via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **70**, 1895 (1993).

[6] P. Benioff, The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by turing machines, J. Stat. Phys. **22**, 563 (1980).

[7] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Phys. **21**, 467 (1982).

[8] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. R. Soc. London A **400**, 97 (1985).

[9] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[10] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

[11] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Distributed quantum computation over noisy channels, Phys. Rev. A **59**, 4249 (1999).

[12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation Via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[13] M. A. Nielsen, Conditions for a Class of Entanglement Transformations, Phys. Rev. Lett. **83**, 436 (1999).

[14] C. Spee, J. I. de Vicente, D. Sauerwein, and B. Kraus, Entangled Pure State Transformations Via Local Operations Assisted by Finitely Many Rounds of Classical Communication, Phys. Rev. Lett. **118**, 040503 (2017).

[15] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States, Phys. Rev. Lett. **85**, 4972 (2000).

[16] F. Anselmi, A. Chefles, and M. B. Plenio, Local copying of orthogonal entangled quantum states, New J. Phys. **6**, 164 (2004).

[17] V. Gheorghiu, L. Yu, and S. M. Cohen, Local cloning of entangled states, Phys. Rev. A **82**, 022313 (2010).

[18] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[19] E. Chitambar and M.-H. Hsieh, Round complexity in the local transformations of quantum and classical states, Nat. Commun. **8**, 2086 (2017).

[20] H.-K. Lo and S. Popescu, Concentrating entanglement by local actions: beyond mean values, Phys. Rev. A **63**, 022301 (2001).

[21] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[22] E. Chitambar, Local Quantum Transformations Requiring Infinite Rounds of Classical Communication, Phys. Rev. Lett. **107**, 190502 (2011).

[23] S. Lloyd and R. Maity, Efficient implementation of unitary transformations, arXiv:1901.03431v1.

[24] W. Gerlach and O. Stern, Der experimentelle nachweis des magnetischen moments des silberatoms, Z. Phys. **8**, 110 (1922).

[25] W. Gerlach and O. Stern, Der experimentelle nachweis der richtungsquantelung, Z. Phys. **9**, 349 (1922).

[26] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328**, 303 (2014).

[27] S. M. Cohen, General Approach to Quantum Channel Impossibility by Local Operations and Classical Communication, Phys. Rev. Lett. **118**, 020501 (2017).

[28] D. Leung, A. Winter, and N. Yu, LOCC protocols with bounded width per round optimize convex functions, arXiv:1904.10985 [quant-ph].

[29] S. Lloyd, Capacity of the noisy quantum channel, Phys. Rev. A **55**, 1613 (1997).

[30] B. Schumacher, Sending entanglement through noisy quantum channels, Phys. Rev. A **54**, 2614 (1996).

[31] K. Kraus, *States, Effects, and Operations* (Spring-Verlag, Berlin, 1983).

[32] K. Kraus, General state changes in quantum theory, Ann. Phys. (NY) **64**, 311 (1971).

[33] M.-D. Choi, Completely positive linear maps on complex matrices, Lin. Alg. Appl. **10**, 285 (1975).