On quantum network coding

Avinash Jain,1,a) Massimo Franceschetti,1,b) and David A. Meyer2,c)

1Department of Electrical and Computer Engineering, University of California, San Diego, California, USA
2Department of Mathematics, University of California, San Diego, California, USA

(Received 9 March 2010; accepted 18 January 2011; published online 4 March 2011)

We study the problem of error-free multiple unicast over directed acyclic networks in a quantum setting. We provide a new information-theoretic proof of the known result that network coding does not achieve a larger quantum information flow than what can be achieved by routing for two-pair communication on the butterfly network. We then consider a k-pair multiple unicast problem and for all $k \geq 2$ we show that there exists a family of networks where quantum network coding achieves $k$-times larger quantum information flow than what can be achieved by routing. Finally, we specify a graph-theoretic sufficient condition for the quantum information flow of any multiple unicast problem to be bounded by the capacity of any sparsest multicut of the network. © 2011 American Institute of Physics. [doi:10.1063/1.3555801]

I. INTRODUCTION

The flow of commodities through a network is a well studied topic that started with the work of Ford and Fulkerson.1 More recently, the study of the flow of information through a network gained wide attention with the paper by Ahlswede et al.,2 which initiated the field of network coding. The main intuition of these authors was that, unlike commodities, information could be processed at intermediate nodes by performing coding operations on the received messages. They showed that such coding operations can significantly improve the information flow through the network.

In its original version, the problem studied was that of multicast, where each destination node requests all the messages generated by the source nodes. Later, multiple unicast problems, where given a set of source-destination pairs each source generates independent messages for a corresponding destination node, have also been studied; see, for example, Refs. 3 and 4. When only routing is allowed at the intermediate nodes, multiple unicast problems are also referred to as multimmodity flow problems.

The capacity improvements offered by network coding in transmission of classical information prompt a similar question for the handling of quantum information. Since the no-cloning theorem5 does not allow duplication of quantum information with fidelity 1, multicast in quantum networks is not a suitable question to ask when single copies of quantum states are available at the source nodes, while multiple destination nodes demand them with fidelity 1. For this reason, Shi and Soljanin6 have considered a variant in which each source node is equipped with the product of the copies of a quantum state and the objective is to recover at the destination nodes the single copies associated with each source.

In this paper, rather than multicast, we consider multiple unicast problems in which source-destination pairs want to communicate quantum states with fidelity 1. The first ones to study this problem were Hayashi et al.7 on the simple butterfly network with two-pair communication depicted in Fig. 1. In this network, the source–sink pairs are \{(1, 4), (3, 2)\} and the common edge (5, 6) can only transmit, at each network use, a single qubit from node 5 to node 6. They showed that
in a single use of the network, it is not possible to transmit two qubits without error, i.e., with fidelity of recovering the original qubits equal to 1. This contrasts with the well known result by which two classical bits can be transmitted in a single network use by the following network coding solution:

\[
\begin{aligned}
A' &= E' = A; \\
B' &= F' = B \\
C' &= A' \oplus B' \\
D' &= G' = C' \\
\end{aligned}
\]

The symbols in (1) refer to classical input bits which are binary random variables taking values in \(\mathbb{Z}_2\), while the number of primes refers to the order of the operation steps. The node operation \(\oplus\) denotes the XOR operation. The authors in Ref. 7 also showed that two qubits can be transmitted in a single use of the butterfly network with fidelity strictly greater than 1/2, though very close to 1/2. The extension of this second result to general graphs is considered in Ref. 8.

The results in Refs. 7 and 8 opened up a Pandora’s box of many unanswered questions as well. To start with, one may be interested in the quantum information flow over a large number of network uses, rather than in one-shot transmission. In this scenario, the quantity of interest is the quantum information flow per network use that can be achieved at a given fidelity. This question was considered by Leung et al. for communication at fidelity 1. They used results in quantum secret sharing to argue that on the butterfly network the total quantum information flow is bounded by what can be routed through the edge (5, 6).

One contribution of this paper is to provide an alternative information-theoretic proof of the above result. To do so, we develop a quantum information-theoretic framework for networks. This builds upon results on single channel communication in quantum information theory.

The works in Refs. 9 and 12 also show that by using external entanglement assistance and additional classical channels between certain nodes, there can be a coding advantage over routing on the butterfly network. Motivated by these works, a second contribution of this paper is to show that such an advantage can also occur in networks without any external assistance. To do so, for all \(k \geq 2\), we construct a \(k\)-pair example network, and show that in this case quantum network coding achieves \(k\)-times larger quantum information flow than what can be achieved via routing, with an entanglement assistance that is intrinsic to the topology of the network. Thus, as it has been shown in the classical setting in Refs. 3 and 4, even in a quantum setting without external entanglement assistance, the network coding advantage over routing can be arbitrarily large as \(k \to \infty\).

The different behaviors observed in the butterfly and in our example network naturally motivate the following question: is it possible to specify a graph-theoretic criterion which would demarcate the multiple unicast problems (and the corresponding networks) on which quantum network coding offers capacity benefits, from those where quantum network coding is not advantageous compared to routing? Finding such a criterion turns out to be hard. Even in the classical setting, only a weaker result is known, namely, the maximum routed flow in any multiple unicast problem is upper bounded.
by the capacity of any sparsest multicut that separates the source–target pairs of interest. On the other hand, the sparsest multicut capacity is generally not an upper bound on the maximum coded flow. In the quantum setting, we specify a necessary graph-theoretic property that must be satisfied for the quantum coded flow to exceed the sparsest multicut capacity. Accordingly, we call a network that satisfies this graph-theoretic property entanglement-supported. We show that when a network is not entanglement-supported, the quantum information flow, irrespective of the coding at intermediate nodes, is upper bounded by the sparsest multicut capacity. An important consequence of this result is that it shows that entanglement support is essential to any quantum network coding protocol. As a side benefit it also explicitly specifies the regions in the graph where entanglement assistance is critical. Further, the class of networks which are nonentanglement-supported includes the butterfly network.

The rest of the paper is organized as follows. The network model and the coding problem are defined in Sec. II. The results proven in the paper are stated in Sec. III. In Sec. IV, we review some concepts of quantum information theory and use them in Sec. V to derive some preliminary results for quantum channels with entanglement assistance. In Sec. VI, we use these results to prove that in the butterfly network the flow achieved by any quantum network coding protocol is upper bounded by the flow achieved by routing. Section VII considers the problem single-pair unicast over arbitrary directed acyclic networks (DANs). In Sec. VIII, we prove that on any nonentanglement-supported $k$-pair network, the flow achieved by any coding protocol is upper bounded by the sparsest multicut capacity.

II. QUANTUM NETWORK MODEL

A graph $G$ is given by the sets $(V, E)$ where $V$ is the set of nodes and $E$ is the set of edges that connect pairs of nodes in $V$. A region of a graph is any subset of $V$. A directed acyclic graph (DAG) is a graph with directed edges such that there does not exist a set of adjacent edges which can be traversed along their direction to form a cycle. The edge $(u, v) \in E$ denotes a directed edge from node $u \in V$ to node $v \in V$. A path between nodes $a_0$ and $a_n$ is denoted by $[a_0, a_1, a_2, \ldots, a_{n−1}, a_n]$ and consists of $n$ edges $(a_{i−1}, a_i) \in E$ with their directions aligned. Any path between $a_0$ and $a_n$ that passes through $a_i$ is denoted by $a_0 \rightarrow a_i \rightarrow a_n$. A DAN $\mathcal{N} = (G, c)$ consists of a DAG $G$ and capacity function $c : E \rightarrow \mathbb{Z}^+$. If $\mathcal{H}_{(u,v)}$ denotes the Hilbert space of the quantum state transmitted with fidelity one over edge $(u, v) \in E$ in $n$ uses of $(u, v)$, then

$$\log |\mathcal{H}_{(u,v)}| \leq n \cdot c((u, v)),$$

where $|\cdot|$ denotes the dimension of the Hilbert space. This is called the edge capacity constraint.

A $k$-pair multiple unicast problem on $\mathcal{N}$ is specified by $k$ source–target pairs

$$(s_1, t_1), (s_2, t_2), \ldots, (s_k, t_k),$$

where each source $s_i$ wants to communicate with target node $t_i$ by transmitting the state of a quantum system $Q_i$ in Hilbert space $\mathcal{H}_i$ over $n$ uses of $\mathcal{N}$. A single network use implies that no network edge is used more than once. The ratio

$$R^{(n)}_i = \frac{1}{n} \log |\mathcal{H}_i|$$

can be thought of as the desired rate of communication between $s_i$ and $t_i$ in $n$ network uses.

Every intermediate node in the network transmits over $n$ uses of each of its output edges the result of a trace preserving completely positive (TPCP) quantum operation$^{13}$ over $n$ uses of its input edges. If the joint state of the quantum system over the input edges to node $u$ is given by the density operator $\rho_u$, then the joint state over the output edges is given by $\rho_J = \xi(\rho_J)$ where $\xi$ is a TPCP operation and $I$ and $J$ are the respective input and output edge sets to the node $u$. The state $\rho_{(u,v)}$ over each output edge $(u,v) \in J$ is represented by the reduced density operator obtained by partial tracing$^{13}$ over all other output edges $(u,w) \neq (u,v)$, i.e., $\rho_{(u,v)} = \text{tr}_J[(u,v)\rho_J]$. The TPCP operation performed at the sink node $t_i$ to recover the state of the system transmitted by $s_i$ is called the decoding operation. To precisely define routing, let us assume that each edge $(q,u) \in I$ is replaced by parallel edges of unit capacity such that the joint Hilbert space of the quantum state over these parallel edges satisfies the capacity constraint of the original edge. Let $I'$ represent the set of edges
incident on node \( u \) after such a replacement. When node operations are restricted such that the output state on any out-edge is the partial trace over a part of the input edges’ space, i.e., \( \rho_{(u,v)} = \text{tr}_T \rho_T \), for some \( T \subseteq I' \), we say that the network implements a routing scheme, otherwise we say that the network implements a coding scheme.

Given a suitable fidelity measure\( ^{13} \), the network is said to admit an \( F \)-solution for the rate vector \( \{R_i^{(n)}\}_i^k \) in \( n \) uses of \( \mathcal{N} \), if it is possible to assign decoding operations at the nodes \( t_i \), \( \forall 1 \leq i \leq k \), and node operations at all remaining nodes \( v \in V \), such that for all \( 1 \leq i \leq k \) the state of the quantum system \( Q_i \) can be recovered at \( t_i \) with fidelity \( F \) without violating any edge capacity constraint. In this case the rate vector \( \{R_i^{(n)}\}_i^k \) is said to be achievable and the network is said to have an \( F \)-flow of value \( \sum_i R_i^{(n)} \). An \( F \)-max flow solution is one that maximizes the \( F \)-flow over all achievable rate vectors and the \( F \)-network capacity is the supremum of the \( F \)-max flow over \( n \). In all of our results, we bound the \( 1 \)-max flow by the sum capacity of the edges in a subset of \( E \), irrespective of the choice of \( n \). Therefore, it follows that the bound also holds for \( 1 \)-network capacity.

Finally, we observe that for any quantum state \( \rho \) on Hilbert space \( \mathcal{H} \), the Von Neumann entropy\( ^{13} \) is given by \( S(\rho) = \log |\mathcal{H}| \), with equality achieved for every completely mixed state. It then follows from the capacity constraint that for any state \( \rho_{(u,v)} \in \mathcal{H}_{(u,v)} \otimes \mathcal{H}'_{(u,v)} \) of the quantum system transmitted over edge \( (u, v) \) in \( n \) uses of \( (u, v) \),

\[
S(\rho_{(u,v)}) \leq n \cdot c((u, v)).
\]

This is the entropy edge capacity constraint. Since \( \frac{1}{n} S(\rho_Q) \) is equal to the rate for the \( i \)th source–destination pair \( R_i^{(n)} = \frac{1}{n} \log |\mathcal{H}_i| \) when \( \rho_Q \) is any completely mixed state of the quantum system \( Q_i \) in \( \mathcal{H}_i \), we can then compute the maximum flow by maximizing the entropy flow \( \sum_i S(\rho_Q) \) subject to the above entropy edge capacity constraints and then choosing the states of \( Q_i \) to be completely mixed.

III. STATEMENT OF RESULTS

Proposition III.1: Consider the butterfly network depicted in Fig. 1 with \( c(5, 6) = 1 \) and no capacity constraint on any other edge. If \( Q_1 \) and \( Q_2 \) are the quantum systems associated with source nodes \( s_1 = 1 \) and \( s_2 = 3 \), whose states \( \rho_{Q_1} \) and \( \rho_{Q_2} \) are recovered at the sink nodes \( t_1 = 4 \) and \( t_2 = 2 \), respectively, with fidelity equal to 1, then \( \forall \rho_{Q_1} \in \mathcal{H}_1 \otimes \mathcal{H}_1^i \) and \( \rho_{Q_2} \in \mathcal{H}_2 \otimes \mathcal{H}_2^i \), we have

\[
\frac{1}{n} (S(\rho_{Q_1}) + S(\rho_{Q_2})) \leq 1.
\]

The proof of the above proposition requires a number of preliminary results, and it is offered in Sec. VI. An immediate consequence of it is the following theorem.

Theorem III.2: There exists a multiple unicast problem on a network \( \mathcal{N} \) for which the maximum flow achieved by classical network coding is larger than the maximum flow achieved by routing, but the maximum flow achieved by quantum network coding is equal to the one achieved by routing.

Proof (of Theorem III.2): The first part of the theorem is well known and follows from (1). The second part of the theorem follows from Proposition III.1 by choosing \( \rho_{Q_1} \) and \( \rho_{Q_2} \) to be completely mixed states.

A converse result is stated and proven next.

Theorem III.3: For all \( k \geq 2 \), there exists a \( k \)-pair multiple unicast problem on a network \( \mathcal{N} \) for which the flow achieved by quantum network coding is \( k \) times larger than the max-flow achieved by routing.

Proof (of Theorem III.3): We prove the theorem by providing a quantum network coding protocol for the network shown in Fig. 2. Assume that \( c((u, v)) = 1 \) on edge \( (u, v) \) and \( c(\cdot) \geq 1 \) on every other edge. Since every path between a source–target pair passes through the common edge
(u, v), the 1-max flow achievable via routing is \(c((u, v)) = 1\). We now show that the extra edges originating from node \(p\) and \(q\) can help nodes \(s_i\) and \(t_i\) share an entanglement, thus providing coding advantage. Let us consider the following quantum network coding protocol. For the moment, let us ignore the edges emerging from the node \(q\).

(i) The node \(p\) generates a maximally entangled *Einstein Podolsky Rosen* (EPR) pair of qubits for each source–target pair \((s_i, t_i)\) and sends one qubit of the pair to \(s_i\) via edge \(p \rightarrow s_i\) and the other qubit to \(t_i\) via \(p \rightarrow t_i\);

(ii) Each source node \(s_i\) performs the first step of the quantum teleportation protocol\(^{20}\) on the incoming qubit and the entangled qubit it receives from \(p\). This generates two classical bits;

(iii) Each source node sends, over two uses of the network, its two classical bits to the corresponding target node, using a classical network coding protocol which is a generalization of (1) to \(k\)-pair communication. The protocol is described explicitly in Ref. 3.

(iv) Each target node recovers the original qubit from two classical bits and the other half of the EPR pair using the last step of the quantum teleportation protocol.

The flow of the above described protocol is \(k/2\) qubits per network use. In addition, edges from node \(q\) can also be used in such a way that nodes \(u\) and \(v\) can share an entangled EPR pair. It is well known that two classical bits can be transmitted using one qubit over edge \((u, v)\) if \(u\) and \(v\) share an entangled pair using the super-dense coding protocol\(^{21}\). Therefore if \(c(\cdot) \geq 2\) for every edge other than \((u, v)\), we need only a single use of the network to recover at \(t_i\) the two classical bits generated at \(s_i\). We can thus achieve a 1-flow of \(k\) qubits if there are no other limiting edges.

Before stating our next results, we need the following graph-theoretic definitions.

Given any multiple unicast problem on \(\mathcal{N} = (G, c)\) the set \(M \subseteq E\) is called a multicut if for all \(i \in \{1, 2, \ldots, k\}\) there is no \(s_i \rightarrow t_i\) path in the graph \((V, E \setminus M)\). The capacity of the multicut is \(\text{cap}(M) = \sum_{(u, v) \in M} c((u, v))\). A sparsest multicut \(M^\ast\) is any multicut in the set \(\arg \min \text{cap}(M)\) and \(\text{cap}(M^\ast)\) is called the sparsest multicut capacity. A set \(S \subseteq E\) is called a supercut if for all \(i, j \in \{1, 2, \ldots, k\}\), there is no \(s_i \rightarrow t_j\) path in the graph \((V, E \setminus S)\). The capacity of the supercut is \(\text{cap}(S) = \sum_{(u, v) \in S} c((u, v))\). Note that every supercut is also a multicut.

For single-pair unicast, a multicut is simply called a cut and a sparsest multicut is called a min-cut. In this case, we have the following theorem.

**Theorem III.4:** For any single-pair quantum unicast, 1-max flow = min-cut capacity.

The proof of the above theorem is given in Sec. VII. Since a supercut separates each source from all the destinations, by aggregating all sources into a single node and all destinations into a single node, an easy consequence of Theorem III.4 is that for any multiple unicast problem the flow achieved by quantum network coding is bounded by the supercut capacity. It follows that if there exists a sparsest multicut \(M^\ast\) which is also a supercut, then the flow achieved by quantum network coding is bounded by \(\text{cap}(M^\ast)\). However, this sufficient condition is too restrictive for
the butterfly network in Fig. 1 and the $k$-pair network in Fig. 2. Note that in the network of Fig. 2, irrespective of the presence of dashed edges $((p, s_i))$, the only sparsest multicut is $\{(u, v)\}$, that is not a supercut. For this network, the dashed edges $((p, s_i))$ are critical in providing entanglement assistance, without them the flow achieved by any coding protocol would be indeed upper bounded by $\text{cap}(u, v))$. In the following, we seek for a graph-theoretic condition for general networks that strengthens the supercut bound and captures the possibility for having entanglement assistance provided by the nodes of the kind $p$ over paths of the kind $(p, s_i)$.

**Definition III.1 (EPN, EAN, EPP):** For any source–target pair $(s_i, t_i)$, consider the set of all ordered pairs of nodes $(p, a)$, such that there exists a path $s_i \rightarrow a \rightarrow t_i$ that does not pass through $p$ and there exists paths $p \rightarrow a$ and $p \rightarrow t_i$. Then $p$ is called entanglement providing node (EPN) and a is called entanglement assisted node (EAN). Any path $p \rightarrow a$ is called an entanglement providing path (EPP).

In Fig. 2, $p, q$ are EPNs, $s_i, u$ are EANs, and $(p, s_i), (q, u)$ are EPPs. Next, we introduce the entanglement assisted region (EAR), which is the set of nodes where entanglement support can potentially lead to quantum network coding advantage over routing. To formally define the EAR, we first introduce the notion of $M$-connectivity, where $M \subseteq E$.

**Definition III.2 (M-connectivity):** Given an edge set $M \subseteq E$, a node $v \in V$ is said to be $M$-connected to $u \in V$, if there exists a path from $u$ to $v$ in reduced graph $(V, E \setminus M)$. The set of paths $u \rightarrow v$ in $(V, E \setminus M)$ is denoted by $\text{Aug}_M(u, v)$.

**Definition III.3 (EAR):** Given a multiple unicast problem on $N$ and a sparsest multicut $M^*$, we define the following two regions associated with the source–destination pair $(s_i, t_i)$:

$$S_i = \{q \in V | \text{Aug}_M(s_i, q) \neq \emptyset, \text{Aug}_M(q, t_i) \neq \emptyset\}$$

$$T_i = \{q \in V | \text{Aug}_M(q, t_i) \neq \emptyset\}.$$  

(2)

The entanglement assisted region for the pair $(s_i, t_i)$, with respect to the sparsest multicut $M^*$ is then defined as

$$\text{EAR}_i(M^*) = \bigcup_{j=1}^{k} (S_i \cap T_j).$$

(3)

The shortened notation $\text{EAR}_i$ will be used when either the choice of $M^*$ is evident from the context or the statement is true irrespective of the choice of $M^*$.

Note that EPN, EAN, EPP, and EAR are all defined with respect to a source–target pair. For the network in Fig. 2 there is only a single sparsest multicut $M^* = \{(u, v)\}$ and given this multicut we have that $\text{EAR}_i(M^*) = \{s_i\}$.

Now, given a path $p \rightarrow a$ in a directed graph $G$, let us denote by $G_i(p \rightarrow a)$ the graph obtained by reversing the direction of the edges in $p \rightarrow a$. We finally have all the ingredients necessary to introduce the graph condition required to have quantum network coding advantage over routing.

**Definition III.4 (Entanglement-supported multiple unicast):** A $k$-pair multiple-unicast problem on a network $N = (G, c)$ is entanglement-supported if for every sparsest multicut $M^*$, there exists an EPP $p \rightarrow a, a \in \text{EAR}_i(M^*)$ for some $i \in \{1, ..., k\}$, such that $M^*$ is not a multicut for the same $k$-pair multiple-unicast problem on the modified network $N_i = (G_i(p \rightarrow a), c)$.

A multiple-unicast problem that does not satisfy the above condition is called nonentanglement-supported. In this case there exists an $M^*$ such that for all EPP’s $p \rightarrow a, a \in \text{EAR}_i(M^*), i \in \{1, ..., k\}$. $M^*$ is a multicut for both $G$ and $G_i(p \rightarrow a)$.

Notice that the multiple unicast problem depicted in Fig. 2 is entanglement-supported. Consider the unique sparsest multicut $M^* = \{(u, v)\}$ and the EPP $p \rightarrow s_i$, incident on $\text{EAR}_i(M^*) = \{s_i\}$. When $p \rightarrow s_i$ is reversed, the modified graph $G_i(p \rightarrow s_i)$ is shown in Fig. 3 and it is easy to see that $M^* = \{(u, v)\}$ is not anymore a multicut for this modified graph.

On the other hand, consider the nontrivial example of a nonentanglement-supported network depicted in Fig. 4(a). For the only sparsest multicut $M^* = \{(u, v)\}$, entanglement assisted regions
\[ \text{EAR}_n(M^*) = \{ s_i \} \] are nonempty. Still the network is nonentanglement-supported, as \( M^* \) is still a multicut for the network in Fig. 4(b) obtained by reversing any of the EPPs (\( p \rightarrow s_i \)).

Our main result is for nonentanglement-supported \( k \)-pair multiple unicast problems.

**Theorem III.5:** Given a nonentanglement-supported \( k \)-pair multiple unicast problem on a network \( \mathcal{N} \), the 1-max flow is bounded by the sparsest multicut capacity.

Note that with the exception of Theorem III.3, Theorem III.5 includes all other results presented so far:

- It is easy to verify that the butterfly network in Fig. 1 is nonentanglement-supported, since there are no EPP’s. Hence, Theorem III.5 implies Theorem III.1.
- Any single-pair unicast problem is nonentanglement-supported, since for any sparsest multicut \( M^* \), \( \text{EAR}_n(M^*) = S_1 \cap T_1 = \emptyset \). Hence, Theorem III.5 implies Theorem III.4.
- If a sparsest multicut \( M^* \) is a supercut, then \( \text{EAR}_n(M^*) = \emptyset \), \( \forall i \). The network is therefore nonentanglement-supported and by Theorem III.5, 1-max flow is bounded by \( \text{cap}(M^*) \).

For the clarity of exposition, we prove each result separately, so that the arguments are built from the bottom up, and give some insight into the more general case, which is finally proven in Sec. VIII.

**IV. BACKGROUND**

In order to prove Proposition III.1, Theorem III.4, and Theorem III.5, we review some aspects of quantum information theory. We denote \( S(\rho_Q) \) by \( S(Q) \), where \( \rho_Q \) is the state of the system \( Q \). We also rely on the concept of purification,\(^\text{13}\) where every mixed state \( \rho_Q \) over \( \mathcal{H}_Q \) can be viewed as a reduced state of some pure state \( \rho_{RQ} \) over \( \mathcal{H}_Q \otimes \mathcal{H}_R \) such that \( \rho_Q \) and \( \rho_R \) have same eigenvalues.
and any two purifications $\rho_{R1}$ and $\rho_{R2}$ are unitarily equivalent, i.e., $\rho_{R1} = U \rho_{R2} U^\dagger$, for some unitary transformation $U$. Sometimes, it may be convenient to think of $\rho_R = \rho_R \otimes |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle\langle\psi|$, when considering the purification in a higher dimensional Hilbert Space.

A. Fidelity measures

In the literature, different closely related notions of fidelity have been defined. We work with entanglement fidelity defined by Schumacher.\textsuperscript{15} This definition is relevant in scenarios of information transmission through noisy channels. Let $\xi : Q \to Q'$ be the quantum channel given by a trace preserving quantum operation $\rho_Q' = \xi(\rho_Q)$. The notation $Q'$ is used to represent the resulting quantum system available at the decoder with state $\rho_Q'$, while its correlation and entanglement with the environment depend on the state $\rho_Q$ and the operation $\xi$. To define the entanglement fidelity, consider a virtual system $\mathcal{R}$ that purifies $Q$. Also, let $\zeta : Q' \to \tilde{Q}$ be the recovery (or decoding) operation defined as $\rho_{\tilde{Q}} = \zeta(\rho_Q')$. $\tilde{Q}$ is in the same Hilbert space as $Q$. If $|\psi^{RQ}\rangle$ is the pure state vector of the joint system $R \tilde{Q}$, and $\rho_{R\tilde{Q}}$ is the density operator representing the final state of $R \tilde{Q}$, then the entanglement fidelity is defined as

$$F_e(\rho_Q, \zeta \circ \xi) \equiv \langle \psi^{RQ} | \rho_{R\tilde{Q}} | \psi^{RQ} \rangle.$$ \hfill (4)

The entanglement fidelity, henceforth abbreviated as $F_e$, does not depend on a particular purification $|\psi^{RQ}\rangle$.\textsuperscript{15}

Knill and Laflamme\textsuperscript{18} examined the relation between different fidelity measures when the state space of $Q$ is two-dimensional. They showed that under general conditions, different fidelity measures approach 1 as $F_e \to 1$. In arbitrary finite dimensional state spaces, Horodecki et al.\textsuperscript{16} related the average fidelity given by Jozsa,\textsuperscript{14} averaged over all states on $\mathcal{H}_Q$, to the entanglement fidelity (4) of the completely mixed state. They showed that

$$\overline{F} = (d F_e(\rho_Q, \zeta \circ \xi) + 1)/(d + 1),$$ \hfill (5)

where $d = \log |\mathcal{H}_Q|$, $\rho_Q$ is the completely mixed state, and $\overline{F}$ is the average fidelity given by Jozsa.\textsuperscript{14} An alternative proof of (5) is also given in Ref. 17. Therefore, it follows that when $F_e \to 1$ for a completely mixed state, $\overline{F} \to 1$ for every finite dimensional Hilbert space.

We apply the notion of fidelity that we have discussed to the quantum system $Q$ transmitted over $n$ network uses, hence we call it the block fidelity. This is a stronger notion of fidelity than the per-qubit fidelity considered in Refs. 7 and 8.

B. Quantum Fano inequality

In Ref. 15, the following inequality, also called the quantum Fano inequality, relates entanglement fidelity $F_e$ with the entropy of entanglement $S(R \tilde{Q})$:

$$S(R \tilde{Q}) \leq H(F_e) + (1 - F_e) \log(|\mathcal{H}_Q|^2 - 1),$$ \hfill (6)

where $H(\cdot)$ refers to classical entropy. Barnum et al. in Ref. 19 use (6) to derive the following bound:

$$2H(F_e) + 4(1 - F_e) \log(|\mathcal{H}_Q|) \geq S(R) - (S(Q') - S(RQ')). \geq 0.$$ \hfill (7)

The bound in (7) holds for every recovery operation $\zeta$, including the one that maximizes $F_e$ in (4). We call $F_e$ the fidelity of recovery. When $F_e \geq 1 - \delta$ for $0 \leq \delta < 1$, we have from (7):

$$\frac{1}{n}(S(R) - (S(Q') - S(RQ'))) = \epsilon(\delta),$$ \hfill (8)

where $\epsilon(\delta) \to 0$ as $\delta \to 0$. From now onward, we assume $F_e = 1$ which implies $\delta = 0$ and $\epsilon(\delta) = 0$, though we want to emphasize that the results we prove next can easily be extended for $\delta \neq 0$ and our bounds hold within $\epsilon(\delta)$ margin of error for $F_e \geq 1 - \delta$. 
V. QUANTUM CHANNELS WITH ENTANGLEMENT ASSISTANCE

We now give a diagrammatic representation of reversible quantum channel and show an information-theoretic inequality for a reversible quantum channel in presence of entanglement which is needed to prove our results.

Let $E$ be the environment initially in a pure state interacting with the system of interest $Q$. Any quantum operation is a unitary transformation in the Hilbert space $\mathcal{H}_Q \otimes \mathcal{H}_E$, resulting in $Q'$ and discarded system $E'$. The corresponding diagram for this quantum channel is given in Fig. 5(a), where $\zeta$ represents the decoding operation which leads to the estimated state $\hat{Q}$.

Note that the joint state $\rho_{RQ'E}$ is a pure state, where $R$ purifies $Q$. This implies $S(Q') = S(RE')$ and $S(RQ') = S(E')$, and by substitution in (8) we obtain the following equation at $F_\epsilon = 1$:

$$\frac{1}{n}(S(R) + S(E') - S(RE')) = 0. \quad (9)$$

We want to give a diagrammatic representation of the channel corresponding to the above equation. Let us define $E'_p$ to be the system with the smallest dimension that purifies $E'$. Then $\rho_{E'E_p}$ is a pure state with $S(E'E_p) = 0$. Since $\rho_{RQ'E}$ is also a pure state, $E'_p$ is contained in the system $RQ'$. We recall that entropy is subadditive. Since subadditivity is satisfied with equality in (9), it follows that $\rho_{RE} = \rho_R \otimes \rho_{E'}$. Further, $Q'$ purifies $RE'$, $Q$ purifies $R$, and $E'_p$ purifies $E'$ by construction. Given the unitary equivalence of purifying systems, we obtain the diagram in Fig. 5(b), where $\xi_1$ is a unitary transformation represented by the following relation:

$$\rho_{Q'} \in [\rho_Q \otimes \rho_{E'_p}], \quad (10)$$

where the equivalence class $[\rho_Q \otimes \rho_{E'_p}] = \{U(\rho_Q \otimes \rho_{E'_p})U^\dagger | UU^\dagger = I\}$.

The following lemma extends the result in the presence of entanglement assistance available at the decoder and gives the corresponding diagrammatic representation.

**Lemma VI.1:** Consider the representation of a quantum channel shown in Fig. 6. Suppose that $E'_p$ is available to the decoder in addition to $Q' = \xi(Q)$, and that it is possible to recover $Q$ from $\{Q', E'_p\}$ with fidelity one. Then, we have

$$\frac{1}{n}(S(Q') - S(Q)) \geq \frac{1}{2n}S(Q' : E'_p) \geq 0, \quad (11)$$

where $S(Q' : E'_p)$ is the quantum mutual information between $Q'$ and $E'_p$ as defined in Ref. 13.

**Proof** (of Lemma VI.1): Let $E = E'E'_p$ be a pure state. After the quantum operation, let $E'$ purify the joint system $RQ'E'_p$. $Q'E'_p$ plays the same role as $Q'$ in (8) which can be rewritten as $(S(Q) - (S(Q'E'_p) - S(E'))) = 0$ at fidelity one, with $S(Q)$ replacing $S(R)$ and $S(E')$ replacing $S(RE')$. 

FIG. 5. Quantum channels: diagrammatic representations.

FIG. 6. Quantum channel with entanglement assistance.
More explicitly, the following set of inequalities holds:

\[
S(Q') - S(Q) = S(Q') + S(E') - S(Q' E'_p) \\
\geq S(Q' E') - S(Q' E'_p) \\
= S(Q E') - S(Q' E'_p) \\
= S(Q) + S(E') - S(Q' E'_p) \\
= S(Q) + S(E') - S(Q' E'_p),
\]

It then follows

\[
2(S(Q') - S(Q)) \geq S(Q' : E'_p) \geq 0,
\]

where the first equality follows from (8) at \( F_v = 1 \). The positivity of mutual information \( S(Q' : E'_p) \) follows from quantum subadditivity \(^{13}\).

Remarks: Lemma V.1 can be related to results in quantum secret sharing, specifically Theorem 5 in Ref. 10 or its information-theoretic equivalent Theorem 6 in Ref. 11. In an analogy with secret sharing terminology, \( Q \) represents a quantum secret and \( (E'_p) \) is a set unauthorized to reconstruct the secret, i.e., \( S(R : E'_p) = 0 \), where \( R \) purifies \( Q \). Since the set \( Q' \cup (E'_p) \) is authorized to reconstruct the secret, \( Q' \) represents an important share. Both the results in Refs. 10 and 11 state that the size of the important secret \( Q' \) is at most as large as the size of the secret \( Q \), i.e., \( S(Q') \geq S(Q) \). This was the argument used in Ref. 9 to present a different proof of Proposition III.1. We observe that Lemma V.1 also gives a lower bound in terms of the mutual information: \( S(Q') - S(Q) \geq (1/2)S(Q' : E'_p) \).

Lemma V.1 is also applicable to quantum teleportation.\(^{20}\) When \( \rho_Q \) is a two-dimensional quantum state with \( S(Q) = 1 \), \( E' \) and \( E'_p \) represent the EPR pair, and \( Q' \) represents the classical information, it can easily be verified given the operation performed at the encoder that \( S(Q' : E'_p) = 2 \). Therefore from (11), \( S(Q') \geq 2 \) and so 2 bits is the minimum amount of classical information the decoder requires for recovering the state of \( Q \).

As a side note, one must be careful in the application of Lemma V.1. It is applicable when preserving entanglement fidelity is a reasonable criterion, i.e., when the quantum state \( \rho_Q \) can be any arbitrary state in \( \mathcal{H}_Q \otimes \mathcal{H}^\perp_Q \). It is not applicable, for example, when \( \rho_Q \) is known to take some finite fixed orthonormal states and therefore behaves as a classical system. The well known example in this case is super-dense coding.\(^{21}\)

VI. THE BUTTERFLY NETWORK EXAMPLE

We apply the results in Sec. V to provide a proof of Proposition III.1.

Proof (of Proposition III.1): Consider the purifying systems \( P \) and \( R \) for systems \( A \) and \( B \), respectively. In this proof we assume that \( A \) and \( B \) are uncorrelated, i.e., \( \rho_{AB} = \rho_A \otimes \rho_B \). Since there are no capacity restrictions on the side links, for notational simplicity, we assume that \( E' \) and \( F' \) contain information not contained in \( A' \) and \( B' \), respectively. To be more precise, \( \rho_{PA'E'} \) and \( \rho_{RB'F'} \) are pure states. We first consider the cut 1 in Fig. 1. If \( D'' \) suffices to recover \( B \) with fidelity 1, then \( B' \) can recover \( B \) with fidelity 1. The analogous result holds for \( A \). From (10), we have

\[
\rho_{B'} \in [\rho_B \otimes \rho_{E'_p}],
\]

\[
\rho_{A'} \in [\rho_A \otimes \rho_{E'_p}],
\]

where \( E'_p \) and \( F'_p \) purify \( E' \) and \( F' \), respectively.
Next, consider the cut 2 in Fig. 1. The quantum channels corresponding to the butterfly network to the left of cut 2 are drawn in Fig. 7. Applying Lemma V.1 yields the desired result:

\[
\frac{1}{n} S(AB) \leq \frac{1}{n} S(C^\prime) - \frac{1}{2n} S(C^\prime : E'F') \\
\leq \frac{1}{n} S(C^\prime) \leq 1,
\]

since for uncorrelated A and B, \(S(AB) = S(A) + S(B)\).

\[\square\]

It is worth noting that the application of Lemma V.1 helps to quantify the loss in performance due to the quantum operations at the intermediate nodes. In the case of the butterfly network, since the flow of 1 is achievable by routing, the performance loss due to the quantum operations at nodes 1, 3, and 5 is lower bounded by \(\frac{1}{2n} S(C^\prime : E'F')\).

**VII. SINGLE-PAIR UNICAST**

Let us now consider the single-pair unicast problem over any DAN and show that the min-cut max-flow result stated in Theorem III.4 holds. As noted in Sec. I, Ford–Fulkerson’s constructive algorithm gives a routing solution to achieve a 1-flow of value equal to the min-cut capacity. To prove Theorem III.4, we need to show that 1-max flow is upper bounded by the min-cut capacity irrespective of coding at the intermediate nodes. This is not immediately obvious due to possible entanglements between nodes.

Given a cut \(M\), we consider a partition of \(V\) using \(M\)-connectivity (Definition III.2). Let \(A = \{v \in V | \text{Aug}_M(s_1, v) \neq \emptyset\}\), and \(A^c = V \setminus A\). Then \(\{A, A^c\}\) represents a partition of the vertex set \(V\) such that \(M = \text{cut}(A, A^c) = \{(u, v) \in E : u \in A, v \in A^c\}\).

Next, we define the outflow in the context of quantum information.

**Definition VII.1** Let \(S(\cdot | \cdot)\) be the joint entropy of states on edges in the set \(\cdot\). The outflow from \(A\) to \(A^c\) in \(n\) uses of \(\mathcal{N}\) is defined as:

\[
\text{outflow}(A, A^c) \equiv \frac{1}{n} S((u, v) : (u, v) \in M)).
\]

**Lemma VII.1:** For every cut \(M\), \(1\)-flow \(\leq \text{cap}(M)\).

**Proof** (of Lemma VII.1): Consider a cut \(M = \text{cut}(A, A^c)\). It follows from the definition of capacity constraint that \(\text{outflow}(A, A^c) \leq \text{cap}(M)\). However, due to possible entanglement, it is not immediately obvious that

\[
1\text{-flow} = \text{outflow}(\{s_1\}, V \setminus \{s_1\}) \leq \text{outflow}(A, A^c).
\]

To prove (14), let us label the various quantities involved in the flow between \(A\) and \(A^c\) as shown in Fig. 8. Let \(\rho_Q\) be the state of the input quantum system \(Q\) at node \(s\). Then \(1\text{-flow} = \frac{1}{n} S(Q)\). Let \(Q^\prime\)
be the quantum system over the outflow edge set $M$ from $A$ to $A^c$. Then outflow$(A, A^c) = \frac{1}{n} S(Q')$. Let $E'$ be the quantum system over the inflow edges from $A^c$ to $A$. Since we are interested in proving an upper bound, we assume that $E'_p$ is available at the target node to recover $Q$ from $\{Q', E'_p\}$ with fidelity equal to 1. Now direct application of Lemma V.1 implies that $S(Q) \leq S(Q')$ and therefore $1$-flow $\leq$ outflow$(A, A^c)$.

Theorem III.4 is an easy consequence of Lemma VII.1.

**Proof** (of Theorem III.4): Let us consider any min-cut $M^*$. From Lemma VII.1, $1$-max flow $\leq \text{cap}(M^*)$ irrespective of coding in the intermediate nodes. Ford–Fulkerson’s algorithm\(^1\) shows that the bound is achievable by constructing a routing algorithm.

\[ \square \]

**VIII. MULTIPLE UNICAST**

We now turn to the proof of the more general result, stated in Theorem III.5. We break the proof into three steps:

1. **Step 1:** Enhance the network with the addition of nodes and edges such that if Theorem III.5 is true for the enhanced network, it is also true for the original network.
2. **Step 2:** Partition the enhanced network into regions on which joint quantum operations can be considered.
3. **Step 3:** Consider an appropriate network cut and apply the quantum information inequality of Lemma V.1 to finally get the desired result.

**A. Step 1. Enhancing the network**

We consider a nonentanglement-supported $k$-pair multiple unicast problem on a network $\mathcal{N} = (G, c)$ and enhance the network to $\mathcal{N}' = (G', c)$ by adding new nodes and edges. The enhancement is such that: (i) there is no change to the sparsest multicut capacity; and (ii) the $k$-pair problem on $\mathcal{N}'$ is still nonentanglement-supported. It follows that if we can show that Theorem III.5 holds for $\mathcal{N}'$, then Theorem III.5 holds for the original network $\mathcal{N}$.

The enhancements are as follows. First, we split each source node into two, in such a way that the new source has no in-edges and a single out-edge with no capacity constraints. Similarly, we split each target node into two, in such a way that the new target has no out-edges and single in-edge with no capacity constraints. This ensures that there are no direct paths $s_i \rightarrow s_j$ and $t_i \rightarrow t_j$, for all $i \neq j$. It is easy to see that this modification does not affect the sparsest multicut capacity and the problem is still nonentanglement-supported.

Second, for every $i \in [1, k]$ we add a directed edge $(s_i, t_j)$ for some arbitrary $j \neq i$. Notice that the added edge $(s_i, t_j)$ is not part of any multicut and therefore the sparsest multicut capacity is unchanged. Furthermore, since $s_i$ has no in-edges, the addition of $(s_i, t_j)$ does not create any EPP and the problem remains nonentanglement-supported.
As a consequence of the above operation, notice that now there exists a \( j \neq i \) such that \( s_i \in T_j \), and since by definition \( s_i \in S_i \), now we also have that for any sparsest multicut \( M^* \), \( s_i \in \text{EAR}(M^*) \).

As a third step of the enhancement, recall that since the \( k \)-pair problem is nonentanglement-supported, there exists a sparsest multicut \( M^* \) such that this is a multicut for both \( G \) and \( G', (p \rightarrow a) \), for all the EPP’s \( p \rightarrow a \). For every \((u, w) \in M^* \) we place a new node \( v \) on the edge \((u, w) \), such that \( c((u, w)) = c((u, v)) = c((v, w)) \). Then we consider the multicut \( M^* = [(u, v)|(u, w) \in M^*] \). Notice that after this operation \( M^* \) is still a sparsest multicut for the enhanced network and the \( k \)-pair problem is still nonentanglement-supported.

B. Step 2. Partitioning the network

Let us consider the enhanced network \( N' \) and a sparsest multicut \( M^* \) obtained after the enhancement, as described in Sec. VIII A. For every source–target pair \((s_i, t_i)\), we define the partition:

\[
A_i = \{v \in V | \text{Aug}_{M^*}(s_i, v) \neq 0\} \quad \text{and} \quad A_i^c = V \setminus A_i.
\]

Let \( A = \bigcup_i A_i \) and \( A^c = \bigcap_i A_i^c = V \setminus A \). Then \( A^c \) denotes the region of nodes which are not \( M^* \)-connected to any of the \( s_i \).

**Lemma VIII.1:** For the enhanced network \( N' \), \( M^* = \text{cut}(A, A^c) \).

**Proof** (of Lemma VIII.1): Let us consider any edge \((u, v) \in \text{cut}(A, A^c) \). Since \( u \in A \), \( u \) is \( M^* \)-connected to \( s_i \) for some \( i \in \{1, ..., k\} \). On the other hand, since \( v \in A^c \), \( v \) is not \( M^* \)-connected to any \( s_i \). This implies \((u, v) \in M^* \) and therefore \( M^* \geq \text{cut}(A, A^c) \).

Next, let us consider any edge \((u, v) \in M^* \). Since \( M^* \) is a sparsest multicut, this implies that there exists a path \( s_i \rightarrow u \rightarrow v \rightarrow t_i \) for some \( i \), and \( u \) is \( M^* \)-connected to \( s_i \), i.e., \( u \in A \). On the other hand, by the enhancement \((u, v) \) is the only in-edge at \( v \) and \( v \) is not \( M^* \)-connected to any \( s_i \), i.e., \( v \in A^c \). Therefore, \((u, v) \in \text{cut}(A, A^c) \) and therefore \( M^* \leq \text{cut}(A, A^c) \).

By Definition III.3, we have that \( \bigcup_i S_i \subseteq A \). Next, we partition the set \( A \) into the following regions:

(i) \( \text{EAR}(\cdot) \) as specified in Definition III.3.
(ii) \( T'_i \equiv T_i \cap \bigcup_{j \neq i} \text{EAR}_j \cap A \), where \( \text{EAR}_j \equiv V \setminus \text{EAR}_j \). In words, \( T'_i \) are those nodes in \( T_i \) which are also in \( A \), but not in any of the \( \text{EAR}_i \). This is to ensure that \( \text{EAR}_i \) and \( T'_i \) are disjoint.

(iii) \( J \equiv \bigcup_i S_i \setminus \bigcup_i \text{EAR}_i \).

(iv) The region of all nodes in \( A \) that are not included in the three regions defined above can be ignored in the computation of the capacity, since there is no path from any node inside it to any \( t_i \).

Figure 9 shows the partition for \( k = 2 \). Only those edges connecting the regions that show the regions which are \( M^* \)-connected to either \( s_1 \) or \( s_2 \).

**Lemma VIII.2:** The enhanced network \( N' \) satisfies the following properties:

(a) For all \( i \), \( s_i \in \text{EAR}_i \).

(b) For all \( i \), \( t_i \in T'_i \).

(c) When \( k = 2 \), all the regions considered in Fig. 9 are mutually disjoint.

**Proof** (of Lemma VIII.2): Property a) follows immediately from the enhancement construction. Property b) follows because \( t_i \in T'_i \) by definition, \( t_i \in A \) by the enhancement construction, and \( t_i \notin \text{EAR}_j \), \( \forall j \), because there is no out-edge at \( t_i \). Next, we prove property c). For \( k = 2 \), we have \( \text{EAR}_1(M^*) \cap \text{EAR}_2(M^*) = (S_1 \cap T_2) \cap (S_2 \cap T_1) = \emptyset \). Similarly, for \( k = 2 \), if \( u \in T'_1 \), then there exists a path \( s_1 \rightarrow u \rightarrow t_1 \) without any edge in \( M^* \). This implies \( u \notin T'_2 \), otherwise there would be a path \( s_1 \rightarrow u \rightarrow t_2 \) without an edge in \( M^* \). Therefore, \( T'_1 \cap T'_2 = \emptyset \). The regions \( \text{EAR}_1, T'_1, A^c \), and \( J \) are also mutually disjoint, as \( S_i \cap T_i = \emptyset \) (this is true \( \forall k \geq 2 \)).
We now introduce some notation to represent the different quantum systems interacting between the regions defined above. Let $X, Y \subseteq V$ be any two regions in $G$. Then

- $(X, Y)$ denotes the quantum system over the set of directed edges from a node in $X$ to a node in $Y$.
- $\rho_{E^{XY}}$ denotes the entangled state that can be shared between any two regions of the graph without using any edge in $M^*$. $E^{XY}$ is the part of the entanglement available at $X$ and $E^{YX}$ is the part of the entanglement available at $Y$.

**Lemma VIII.3:** If a multiple unicast problem is nonentanglement-supported, then there exists a sparsest multicut $M^*$ such that no entanglement can be shared between $\text{EAR}_i(M^*)$ and $T'_i$ without using any edge in $M^*$, i.e.,

$$\rho_{E^{\text{EAR}_i T'_i \text{EAR}_i}} = \rho_{E^{\text{EAR}_i T'_i \text{EAR}_i}} \otimes \rho_{E^{T'_i \text{EAR}_i}}.$$  

**Proof** (of Lemma VIII.3): Since the problem is nonentanglement-supported, there exists a sparsest multicut $M^*$ such that for all EPP’s $p \rightarrow a$, $a \in \text{EAR}_i(M^*)$, $i \in \{1, \ldots, k\}$, $M^*$ is a multicut for both $G$ and $G_r(p \rightarrow a)$. Let us consider the partition of the regions in Fig. 9 with respect to this $M^*$. We now argue by contradiction. If an entangled state $\rho_{E^{\text{EAR}_i T'_i \text{EAR}_i}}$ can be shared between $\text{EAR}_i$ and $T'_i$ without using an edge in $M^*$, then there exists a $p \in A^*$ such that there are paths from $p \rightarrow u$, $u \in \text{EAR}_i$, and $p \rightarrow v$, $v \in T'_i$. On reversing the EPP $p \rightarrow u$, there is a path $s_i \rightarrow u \rightarrow p \rightarrow v \rightarrow t_i$ which does not include an edge in $M^*$. This is a contradiction. 

We have now done all the groundwork to give a proof of Theorem III.5. We first give a proof for the two-pair unicast problem, followed by a proof for the $k$-pair unicast, with $k \geq 2$.

**C. Step 3. Two-pair unicast case**

In a two-pair network, by Lemma VIII.2, property (c), all the regions of the considered partition are disjoint. In particular, $\text{EAR}_1(\cdot) \cap \text{EAR}_2(\cdot) = \emptyset$. The disjointness of the entanglement assisted
regions makes the proof of Theorem III.5 easier to illustrate and hence the reason to consider the two-pair case separately.

Proof (of Theorem III.5, for \( k = 2 \)): By Lemma VIII.2 (a)–(b), the input operation at \( s_i \) is a part of a joint operation in the region \( \text{EAR}_i \), while the decoding operation at \( t_i \) is a part of a joint operation at \( T'_i \). In the the proof we focus on these joint operations at \( \text{EAR}_i \) and \( T'_i \) instead of the marginal operations at \( s_i \) and \( t_i \).

Let the state of the quantum system flowing into each \( \text{EAR}_i \) via node \( s_i \) be \( \rho_{Q_i} \). The TPCP quantum operation over the set of nodes \( A \), before transmission on the edges of the cut \( M^* \), is given by the composition \( \hat{\xi}(\cdot) = (\hat{\xi}_{\text{EAR}} \otimes \hat{\xi}_{\text{EAR}_{\text{op}}})(\cdot) \), where subscripts denote the region over which the operation is considered.

We refer to Fig. 10. Note that only the quantum states on the edges connecting \( \text{EAR}_i \) to \( A' \cup J \) can be sent to the decoder at \( T'_i \) via edges in \( M^* \), and that of the entangled states from node \( p_i \) only \( E^J_{\text{EAR}_i} \) should be considered after the operation at \( \text{EAR}_i \). Furthermore, for any other entangled state of the type \( \rho_{E_{\text{EAR}} \otimes X_{\text{EAR}}}, \) with \( X \in \{ \text{EAR}_j, T'_j, A' \} \), \( j \neq i \), we have that \( E^X_{\text{EAR}_i} \) cannot be sent to the decoder at \( T'_i \) without violating Lemma VIII.3.

This implies that if \( \rho_{O_{i}} \) can be recovered at \( T'_i \), it should be recoverable from \( (\text{EAR}_i, A')(\text{EAR}_i, J), \text{EAR}_i \), and \( E^X_{\text{EAR}_i} \).

Let now \( F'_i \) be defined such that the joint state \( \rho_{F'_i} = (\text{EAR}_i, A')(\text{EAR}_i, J), E^X_{\text{EAR}_i} \) is a pure state. From (10), we have

\[
\rho_{F'_i} = \rho_{O_{i}} \otimes \rho_{F'_p},
\]

where \( F'_p \) purifies \( F'_i \). We assume that, as in the case of the butterfly network, the resulting environment \( F'_i \) after the operation at \( \text{EAR}_i \) is not discarded but it is available at \( T'_i, j \neq i \).

Next, we consider the possible entanglement shared between \( J \) and \( T'_i, i \in \{1, 2\} \), and apply Lemma V.1 to obtain the final result. We refer to Fig. 11, where \( U_1 \) and \( U_2 \) are unitary operations. Notice that \( Q \) in Fig. 6 corresponds to \( Q_1 Q_2 \) in Fig. 11. Similarly, \( Q' \) corresponds to the quantum system over \( M^* \), and \( E \) corresponds to all remaining input states in Fig. 11. Furthermore, \( Q E'_p \) corresponds to \( (\text{EAR}_i, A')(\text{EAR}_i, J), E^X_{\text{EAR}_i}, E^{J T_i} | i = 1, 2 \) and \( E' \) corresponds to \( E^{T J F'_i} | i = 1, 2 \).
Now, applying Lemma V.1, we have
\[
\frac{1}{\pi} S([Q_i | V_i]) \leq \frac{1}{\pi} S(M^*) \leq \frac{1}{2\pi} S(M^* : F'_i F'_2 E^{T'_1 J} E^{T'_2 J}) 
\leq \frac{1}{\pi} S(M^*) \leq \text{cap}(M^*)
\]
and the proof is complete.

□

D. Step 3. k-pair unicast case

Next, we prove Theorem III.5 for the case \( k \geq 2 \). The proof proceeds along the same line as for \( k = 2 \) case. The argument is slightly more complex because \( \text{EAR}_i \) and \( \text{EAR}_k \), as well as \( T'_i \) and \( T'_k \), may no longer be disjoint for some \( k \neq i \).

Proof (of Theorem III.5): As in the proof for the two-pair problem let us enhance and partition the network.

Next, let us consider the flow of information. The TPCP operation over \( A \), before transmission on \( M^* \), is given by the composition \( \xi_J \circ \xi_{(\cup_i \text{EAR})} \), where subscripts denote the region over which the operation is considered. Note that unlike the two-pair case, \( \xi_{(\cup_i \text{EAR})} \neq \otimes_{i=1}^{k} \xi_{\text{EAR}_i} \), for \( k > 2 \) as \( \text{EAR}_i \) may not be disjoint.

Note that the constraints on the entanglement that can be shared between any two regions without using any edge in \( M^* \) remains the same as in two-pair case because Lemma VIII.3 is applicable to every nonentanglement-supported \( k \)-pair network, even if the regions are not disjoint.

As before, let us represent the state of the quantum system entering into each \( \text{EAR}_i \) via node \( s_i \) by \( \rho_{Q_i} \). Our first step is to explicitly describe the TPCP operation \( \xi_{\text{EAR}} \), before considering the joint operation \( \xi_{(\cup_i \text{EAR})} \). This is similar to the two-pair case. We consider \( \text{cut}(\text{EAR}_i, \text{EAR}_j) \) that disconnects \( \text{EAR}_i \) from the rest of the network. Let \( F'_i \) be defined such that the joint state \( \rho_{F'_i(\text{EAR}_i, A'^i)(\text{EAR}_i, J)E^{\text{EAR}_i}} \) is a pure state. Then, from (10), we have
\[
\rho_{(\text{EAR}_i, A'^i)(\text{EAR}_i, J)E^{\text{EAR}_i}} \in [\rho_{Q_i} \otimes \rho_{F'_i}], \tag{16}
\]
where \( F'_i \) purifies \( F'_i \). Note that \( F'_i \) plays no role in recovering \( \rho_{Q_i} \) as no component of it is available at \( T'_i \). However, it may contain information relevant for recovering \( \rho_{Q_i} \), \( k \neq i \). So, we revisit (16) and see what it tells us about the joint operation \( \xi_{(\cup_i \text{EAR}_i)} \) in the region \( \cup_i \text{EAR}_i \). From (16), it follows that we should be able to recover \( \otimes_i \rho_{Q_i} \) from \( \{|(\text{EAR}_i, A'^i)(\text{EAR}_i, J)E^{\text{EAR}_i} | i = 1 \ldots k \} \).
This is the information we need to describe the TPCP operation \( \tilde{\xi}_{(\cup_i \mathrm{EAR}_i)} \). Define \( G' \) such that 
\[ \rho_{\{(\mathrm{EAR}_i, A') | \{(\mathrm{EAR}_i, J) \in J^{\mathrm{EAR}_i} | \forall i \}\}} \] is a pure state. Then \( G \) can be thought as the environment interacting with \( \{Q_i\}_{i=1}^k \) resulting in useful \( \{(\mathrm{EAR}_i, A') | \{(\mathrm{EAR}_i, J) \in J^{\mathrm{EAR}_i} | \forall i \}\} \) and \( G' \) as being the part not required for decoding after \( \tilde{\xi}_{(\cup_i \mathrm{EAR}_i)} \). From (10), this implies that

\[
\rho_{\{(\mathrm{EAR}_i, A') | \{(\mathrm{EAR}_i, J) \in J^{\mathrm{EAR}_i} | \forall i \}\} | \forall i} \in \bigotimes_i \rho_{Q_i} \otimes \rho_{G'_p},
\]

where \( G'_p \) purifies \( G' \). As we are interested in proving an upper bound, we assume that \( G' \) is not discarded at \( \cup_i \mathrm{EAR}_i \), but is available at \( \{T'_i | \forall i \}\).

Next, let us consider the TPCP operation at \( J \). As before, the operation \( \xi_A \) can be represented as in Fig. 6. \( Q' \) corresponds to \( M^* \). \( Q'E_p \) corresponds to

\[ \{(\mathrm{EAR}_i, A') | \{(\mathrm{EAR}_i, J) \in J^{\mathrm{EAR}_i} | \forall i \}\} \in \bigotimes_i \rho_{Q_i} \otimes |\psi\rangle \langle \psi| \] for some pure state \( |\psi\rangle \langle \psi| \). Then, applying Lemma V.1 yields the desired result:

\[
\frac{1}{n} S(Q_i | \forall i) \leq \frac{1}{n} S(M^*) - \frac{1}{2n} S(M^*: G' | E^{T'_i} | \forall j) \leq \frac{1}{n} S(M^*) \leq \text{cap}(M^*). \]

\( \square \)

**IX. CONCLUSION**

We have provided a quantum information-theoretic framework for analyzing quantum communication with fidelity 1 over networks. We showed that in case of multiple unicast communication, quantum network coding in directed quantum networks can outperform routing. Entanglement support intrinsic to the network topology can enable such a coding protocol. Theorem III.5 showed that the entanglement support is in fact crucial. Since removing EPPs in any given graph does not change the performance of classical network coding, it is easy to see that a large category of quantum networks exist where the quantum network coding performance is bounded by the sparsest multicut capacity while classical network coding performance is not.

Finally, we want to emphasize that it is not necessary for a problem to be nonentanglement-supported to upper bound the network coding capacity by the sparsest multicut capacity, i.e., the converse of Theorem III.5 is not true. This is illustrated by the network depicted in Fig. 12. In this case, there is only one sparsest multicut \( M^* = \{(s_1, t_1), (s_2, t_2)\} \). For such \( M^* \), \( \text{EAR}_i(M^*) = \{s_i\} \), \( i = 1, 2 \), and the corresponding multiple unicast problem is entanglement-supported. Nevertheless, the total coding capacity is still upper bounded by the sparsest multicut capacity \( \text{cap}(M^*) \).
ACKNOWLEDGMENTS

The authors would like to thank Rathinakumar Appuswamy for constructive observations and insightful discussions.