Quantum network communication – the butterfly and beyond

Debbie Leung(1), Jonathan Oppenheim(2) and Andreas Winter(3)

(1) Institute for Quantum Computing, University of Waterloo, Waterloo, Canada
(2) Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge, U.K. and
(3) Department of Mathematics, University of Bristol, Bristol, U.K.

We study the problem of $k$-pair communication (or multiple unicast problem) of quantum information in networks of quantum channels. We consider the asymptotic rates of high fidelity quantum communication between specific sender-receiver pairs. Four scenarios of classical communication assistance (none, forward, backward, and two-way) are considered. (i) We obtain outer and inner bounds of the achievable rate regions in the most general directed networks. (ii) For two particular networks (including the butterfly network) routing is proved optimal, and the free assisting classical communication can at best be used to modify the directions of quantum channels in the network. Consequently, the achievable rate regions are given by counting edge avoiding paths, and precise achievable rate regions in all four assisting scenarios can be obtained. (iii) Optimality of routing can also be proved in classes of networks. The first class consists of directed unassisted networks in which (1) the receivers are information sinks, (2) the maximum distance from senders to receivers is small, and (3) a certain type of 4-cycles are absent, but without further constraints (such as on the number of communicating and intermediate parties). The second class consists of arbitrary backward-assisted networks with 2 sender-receiver pairs. (iv) Beyond the $k$-pair communication problem, observations are made on quantum multicasting and a static version of network communication related to the entanglement of assistance.

I. INTRODUCTION

Consider a network of point-to-point communication channels. At any time period, we model the set of users sharing access to the same point as a party. Most generally, any party may want to transmit data to a set of other parties, and such data can be correlated in time and space. A central question is whether a given network can handle a specific joint communication task. For example, in the multicast problem, one party wants to send the same data to a specific list of other parties (the most common example is sending invitations to a wedding). In contrast, the multiple unicast or the $k$-pairs communication problem is concerned with $k$ specific (disjoint) sender-receiver pairs, who are trying to communicate $k$ independent messages in the given network.

We consider networks of parties connected by noiseless channels, and they are represented by vertices and edges in a graph. Each edge is weighted by the capacity of the corresponding channel, and its direction (if any) follows that of the channel.

Network communication was traditionally done by “routing” (also known as the store-and-forward method) in which received data is simply copied and forwarded without data processing. In 2000, Ahlswede, Cai, Li, and Yeung provided the first example that nontrivial coding of data can strictly improve the communication rate for multicasting in the directed “butterfly network” (see Sec. II). The coding method in [1] also applies to the 2-pair communication problem (formalized in [2]) in the same network (see the discussions in [3,4]) demonstrating the general advantage of network coding for the $k$-pair communication problem in directed networks. For undirected networks, it was conjectured that routing is optimal for the $k$-pair communication problem [1,5,8] and it was proved in many cases, such as when $k \leq 2$ [8], and others [4,7].

This paper is concerned with quantum communication through quantum networks. We primarily focus on the $k$-pair communication problem. Our goal is to find the optimal achievable rates (given by the boundary of a $k$-dimensional achievable rate region).

In our study of high fidelity quantum communication through an asymptotically large number of uses of the (quantum) butterfly network, routing turns out optimal. This contrasts with the advantage of network coding in the classical setting, and demonstrates another difference between quantum and classical information. Thus, quantum information flowing through this communication network resembles a classical commodity more than classical information. We believe that such behavior holds for general networks, and provide reasons why it is true for a certain class of “shallow” quantum networks in which the maximum distance between any sender-receiver pair is small. We also study communication scenarios with various auxiliary resources and optimality of routing is essentially unchanged. In particular, free classical back communication effectively makes the quantum channel undirected, and our optimality proof of routing provides some partial answer to the question raised in [5] in the quantum setting.

Our work was inspired by the earlier, complementary, study of Hayashi, Iwama, Nishimura, Raymond, and Yamashita on the quantum butterfly network [8]. They fix the quantum communication rates as in the classical case, and optimize the fidelity of the transmitted states. Deviation from the classical case is manifest in that the optimal 1-shot fidelity is upper bounded by 0.983. Dur-
ing the preparation of this manuscript, we found that Shi and Soljanin have studied a quantum version of multicasting in quantum network [9] that is complementary to our study. After the initial submission of this manuscript to the eprint server [10], Hayashi studied the case of 2-pair communication problem in the directed butterfly network with entanglement shared between the senders, a setting that is also complementary to the current one.

We shall begin in Section II with the butterfly network as a motivating example. Starting from this simpler case, we formalize the network communication problem of interest and review useful techniques, and discuss their generalizations. Then, we focus back on the butterfly network, summarize the classical solution in Sec. II A and present our optimal quantum communication protocols for scenarios with differing free auxiliary resources in Sec. II B. Another example is discussed in Sec. III which will further demonstrate our results for more general networks presented in Sec. IV an an optimality proof for routing of quantum information in certain shallow networks (Sec. IV A), outer and inner bounds of the achievable rate region for the k-pair communication problem in the most general network (Sec. IV B), an optimal solution for the 2-pair case assisted by back classical communication (Sec. IV C), and a reduction of the entanglement assisted case to the classical information flow problem (Sec. IV D).

We discuss two other quantum network communication problems in Sec. V (1) a quantum analogue of the multicasting problem sharing a cat-state between a reference and k receivers – and (2) network communication based on a “static” quantum resource - a pure quantum state shared by the parties – assisted by 2-way classical communication. We conclude with some open problems in Sec. VI.

We use the following notations throughout the paper. The resource of being able to send a classical bit noiselessly from one party to another is called a cbit. A state in a 2-dimensional Hilbert space is called a qubit, and the ability to transmit it is called a qbit. The quantum analogue of a shared random bit is called an ebit – the resource of two parties sharing a copy of the joint state $|00⟩ + |11⟩$). An ebit can be created using other resources (say, qbits, or other quantum states) and be consumed to generate other resources. For example, in teleportation, 2 cbits and 1 ebit generate 1 qbit [11], and in superdense coding 1 ebit and 1 qbit generate 2 cbits [12].

II. MOTIVATING EXAMPLE – THE BUTTERFLY NETWORK

Setting for butterfly network: Consider two senders $A_1$ and $A_2$, who want to send two independent messages $m_1$ and $m_2$ to two respective receivers $B_1$ and $B_2$. Available to them is a network of 7 noiseless directed channels and two helpers $C_1$ and $C_2$ depicted in Fig. 1. For each call to the network, each channel in the network can be used once. The number of calls to the network represents our “cost” to be minimized. (The network is charged as a package.) Local resources are free. In the classical (quantum) setting, both messages and the available channels are classical (quantum).

Definition 1 (Rate region for butterfly network)
In the asymptotic scenario, we allow large number of calls to the network. Let $P_n$ denote a protocol that uses the network $n$ times along with other allowed resources, and communicates $m_1, m_2$ of sizes $n(r_1−δ_n), n(r_2−δ_n)$ bits/qubits with fidelities at least $1−ε_n$ for $δ_n, ε_n → 0$. Then, we say that the rate pair $(r_1, r_2)$ is achievable. The achievable rate region is the set of all achievable rate pairs.

General setting: We consider communication networks in which the number of sender-receiver-pairs and intermediate parties and the capacities of the channels connecting them are arbitrary. To be concrete, consider $k$ senders $A_1, \ldots, A_k$, who want to send $k$ independent messages $m_1, \ldots, m_k$ to $k$ respective receivers $B_1, \ldots, B_k$. Available to them is an arbitrary directed network of noiseless channels and intermediate helpers $C_1$. The rest of the setting is the same as that in the butterfly network and the achievable rate region for such “k-pair communication” problem is defined analogously.

Definition 2 (Rate region for general network)
In the asymptotic scenario, we allow large number of calls to the network. Let $P_n$ denote a protocol that uses the network $n$ times along with other allowed resources, and communicates $m_1, \ldots, m_k$ of sizes $n(r_1−δ_n), \ldots, n(r_k−δ_n)$ bits/qubits with fidelities at least $1−ε_n$ for $δ_n, ε_n → 0$. Then, we say that the rate $k$-tuple $(r_1, \ldots, r_k)$ is achievable. The achievable rate region is the set of all achievable rate $k$-tuples.

We now discuss aspects of the general problem.
Note that in the asymptotic setting, imposing time ordering of the usage of the channels does not affect the achievable rate region.

We choose a measure of fidelity that achieves the strongest notion of approximation. We are concerned with sending quantum messages through networks of quantum channels. In this setting, we require the protocol to transmit a message in a way that preserves arbitrary entanglement between it and any reference system. In other words, the joint state held by the receiver and the reference after the protocol should be close in trace distance to that held by the sender and the reference before the protocol. In the specific cases solved in this paper, the achieving optimal protocols turns out to be exact. In our proofs of optimality (obtaining outerbounds of the rate region), we give full consideration of protocols that have small errors.

We collect tools and techniques that are useful for the general k-pair communication problem, and occasionally refer to Fig. 1 as an example.

1. Exact rate regions and optimal protocols via matching inner and outer bounds

Throughout the paper, whenever possible, we (1) describe simple protocols and the corresponding inner bounds for the rate region and (2) obtain outer bounds that match the inner bounds. Each outer bound has to be completely general, and applies asymptotically. Altogether, these two steps give the exact achievable rate region and prove the optimality of the simple protocols described.

2. Convexity and monotonicity of achievable rate regions

Note that if a rate pair \((r_1, r_2)\) is achievable, so is any \((r'_1, r'_2)\) with \(r'_1 \leq r_1\) and \(r'_2 \leq r_2\). Also, the convex hull of a set of achievable rate pairs are also achievable by time sharing of the underlying protocols. Similarly for the \(k\)-pair communication problem.

3. Outer bounds by cuts

Consider a bipartite cut, i.e., a partition of the vertices into two disjoint subsets of parties \(S_1\) and \(S_2\). We can bound the sum of communication rates from all parties in \(S_1\) to all parties in \(S_2\) by adding the capacities of all forward communication channels from \(S_1\) to \(S_2\) (since grouping the parties together can only increase the communicate rate and back communication does not help \([13]\)). This induces a bound on the sum of rates for the pairs each with the sender in \(S_1\) and the receiver in \(S_2\).

For example, let \(S_1 = \{A_1, B_2, C_1\}\) and \(S_2 = \{A_2, B_1, C_2\}\) in Fig. 1. Then, we can bound \(r_1\), because any protocol on the butterfly network communicating from \(A_1\) to \(B_1\) will also communicate at least the same amount of data from \(S_1\) to \(S_2\). There is only 1 forward channel from \(S_1\) to \(S_2\), so \(r_1 \leq 1\).

We will also see scenarios in which the channels are effectively undirected. In those cases, the total communication rate from all the parties in \(S_1\) to those in \(S_2\) is upper bounded by the total capacities of all the channels between them.

4. Inner bounds via the max-flow-min-cut theorem

By the max-flow-min-cut theorem \([14]\) edges crossing a min-cut can be extended to edge-avoiding paths leading from a sender to a receiver.

5. Sizes of significant shares and quantum parts in quantum-classical dual compression

We will make use of two lower bounds for the sizes of the individual communicated parts when quantum data is sent in a distributed manner.

(a) A quantum secret sharing scheme is an encoding of a quantum state (the secret) in a multiparty system. Each party owns one system called a “share.” Authorized sets of parties can reconstruct the secret (with high fidelity), while unauthorized sets of parties can learn negligible information about the secret. A share \(S_s\) is “significant” if there exists an unauthorized set \(S_u\) such that \(\{S_s\} \cup S_u\) is authorized. It was proved in \([15]\) that for exact schemes (reconstruction and hiding are perfect), the size of any significant share is at least the size of the quantum secret. An alternative proof of this result in \([15]\) extends to the near-exact case.

More precisely, let \(S(\cdot)\) denote the von Neumann entropy, and \(I^{coh}(S_1;S_2) = S(S_2) - S(S_1 S_2)\) denote the coherent information from \(S_1\) to \(S_2\). Let \(S\) be the secret, purified by the reference system \(R\). Then,

\[
S(S_s) \geq S(S) - (\epsilon' + \gamma)/2
\]

(1)

where \(\epsilon'\) and \(\gamma\) are the respective upper bounds on \(I^{coh}(R;S)\) and \(I^{coh}(R,S)\) and the quantum mutual information \(I(S_u;R)\), and they are both negligible when recovery of the secret is near-exact. For completeness, the proof in \([15]\) is duplicated in the endnote \([17]\), with \(\epsilon'\) and \(\gamma\) explicitly derived and inserted.

(b) A quantum-classical dual compression scheme encodes a quantum source into a quantum part and a classical part. It was proved in \([18]\) that the quantum part cannot be smaller than the von Neumann entropy of the source.

(c) We will also use an immediate consequence of Theorem 6 in \([18]\) that logical transformation of the encoded quantum secret can be performed by operating on an authorized set without involving other shares. We prove an extension of this result.
in the endnote \[19\] and give a precise statement here.

Let \( S \) be the system holding the secret and \( R \) be its purifying reference system. Let \( W \) be an isometry encoding \( S \) into systems \( A, B, \) and \( D \) where \( D \) is discarded (to allow the possibility of mixed state secret sharing schemes). Suppose the encoding is invertible on \( A \) with error \( \epsilon \) (i.e., \( 3Y \) an isometry taking \( A \) to \( S \overline{E} \) such that \( RS \) is in a state \( \epsilon \)-close in trace distance to what’s originally in \( RS \)). Then, a desired operation \( U \) to be applied to the secret \( S \) (before the encoding) can be performed with error \( 2\epsilon \) by applying \( Y^\dagger(IE \otimes U_S)Y \) to \( A \) alone.

We state this result for unitary \( U \) but our proof in the endnote \[19\] holds if we replace the unitary \( U \) by an arbitrary quantum operation on \( S \) and \( \overline{S} \). Also, compared to \[13\], the current proof is constructive and operational—it simply asserts that the intuitive approach of “decoding the secret, keeping the auxiliary system \( E \), operating on the decoded state, and reversing the decoding” works in a way that preserves the correlation with the remaining shares.

We will now use this set of general techniques to investigate our example, the butterfly network.

### A. Classical case \[1\]

In the classical case, one use of each channel in the network communicates 1 classical bit, and the messages \( m_1, m_2 \) are classical bit strings.

**Inner bound:** Let \( x_i \) be the 1-bit message to be communicated from \( A_i \) to \( B_i \) for \( i = 1, 2 \). A method that simultaneously communicates \( x_{1,2} \) with exactly 1 call to the network is given by Fig. 2.

**Outer bound:** The above protocol turns out to be optimal because we can prove matching outer bounds \( r_1 \leq 1 \) and \( r_2 \leq 1 \), using the min-cut method. To show \( r_1 \leq 1 \), consider the bipartite cuts \( S_1 = \{A_1, B_2, C_1\} \) and \( S_2 = \{A_2, B_1, C_2\} \). The bound follows from the fact that there is only one forward channel from \( S_1 \) to \( S_2 \). (See the detail argument in item \[3\] in the previous subsection.) A similar argument with the cut \( S_1 = \{A_2, B_1, C_1\} \) and \( S_2 = \{A_1, B_2, C_2\} \) shows \( r_2 \leq 1 \).

Since the outer and inner bounds are matching, by item \[1\] the 1-shot, exact, protocol in Fig. 2 is indeed optimal, and the rate region is just the unit square. (See Fig. 8.)

This example illustrates some common features in network communication—a “bottleneck” from \( C_1 \) to \( C_2 \) and channels that go to the “wrong places.” It also exhibits how nontrivial coding techniques can be applied to improve the communication rates for “information flow” in networks, beyond simple routing.

### B. Quantum case

The setting is the same as the classical case, except now the messages \( m_1, m_2 \) are uncorrelated quantum states \( |\psi_1\rangle, |\psi_2\rangle \), and each use of the channel allows the communication of 1 qubit. (To simplify notations, we denote inputs as pure states, but since communication is entanglement-preserving, the discussion applies to sending parts of entangled states by linearity.)

Clearly the classical coding strategy depicted in Fig. 2 fails in the quantum case—the encoding by \( A_1, A_2, C_2 \) involves cloning unknown quantum states, and quantum analogues of the \( \oplus \) operation do not provide the desired result. In fact, \[8\] showed that if one demands one qubit states \( |\psi_1\rangle, |\psi_2\rangle \) to be communicated by one use of the network, the fidelity is upper bounded by 0.983 (though better than 0.52).

In the following, we will consider an asymptotic number of calls of the network, and demand high fidelity transmission, and optimize the achievable rates. We consider five different scenarios of free auxiliary resources (also known as assisting resources). We first consider the no assistance case, followed by the easier case of having free backward classical communication (which turns out to be no worse than free two-way classical communication). Then, we consider the more intricate case of having free forward classical communication, and finish off with the entanglement assisted case.

- **Unassisted case (no free resource)**

**Inner bound:** The rate pair \((r_1, r_2) = (1, 0)\) is achieved by sending \( |\psi_1\rangle \) from \( A_1 \) to \( C_1 \) to \( C_2 \) and finally to \( B_1 \). The rate pair \((r_1, r_2) = (0, 1)\) is achieved by a similar protocol. By time sharing and monotonicity, any point in the first quadrant with \( r_1 + r_2 \leq 1 \) can be achieved.

**Outer bound:** We will prove \( r_1 + r_2 \leq 1 \).
The main idea is captured in Fig. 3.

![Diagram](image)

**FIG. 3:** Proof ideas for the outer bound for the achievable rate region of the unassisted butterfly network. “\(|\psi_1\rangle|\psi_2\rangle\)” labels a state that is nearly independent of \(|\psi_1\rangle|\psi_2\rangle\).

Consider using the network \(n\) times to enable \(A_1\) to send a state \(|\psi_i\rangle\) of size \(n_i = n(r_i - \delta_n)\) qubits for \(i = 1, 2\) and for \(\delta_n \to 0\). Let \(Q_1, Q_2,\) and \(Q_C\) be the quantum states sent using the \(n\) channel-uses from \(A_1\) to \(B_2, A_2\) to \(B_1,\) and \(C_1\) to \(C_2\) respectively. We can consider \(|\psi_1\rangle\) and \(|\psi_2\rangle\) together as the quantum secret, and apply item \(5(a)\) at the beginning of Sec. III. Clearly \(\{Q_1, Q_2, Q_C\}\) is an authorized set. We will now prove that \(\{Q_1, Q_2\}\) is unauthorized. The basic idea is that, \(Q_1\) has to be independent of \(|\psi_1\rangle\) if \(B_1\) is to receive it faithfully. It is also independent of \(|\psi_2\rangle\) by causality. Thus \(Q_1\) is independent of both \(|\psi_{1,2}\rangle\).

To capture this formally, the \(A_1 \to B_1\) message \(M_1\) should be described as half of a maximally entangled state with a reference system, say, \(R_1\). The \(A_2 \to B_2\) message \(M_2\) likewise has a reference system \(R_2\). Let \(R = R_1 R_2\). Let \(S(\cdot)\) and \(I(\cdot: \cdot)\) denote the von Neumann entropy of a system and the quantum mutual information between two systems (with the underlying state implicit). By independence of the messages and causality, \(I(Q_1 : R_2) = I(Q_1 : Q_2) = I(Q_1 R_1 : Q_2 R_2) = 0\). Our observation above further says that \(I(Q_1 : R)\) and \(I(Q_2 : R)\) are both small. Now,

\[
I(Q_1 Q_2 : R) := S(Q_1 Q_2) + S(R) - S(Q_1 Q_2 R) = S(Q_1) + S(Q_2) + S(R_1) + S(R_2) - S(Q_1 R_1) - S(Q_2 R_2) = I(Q_1 : R_1) + I(Q_2 : R_2)
\]

which is small (the equality is due to the various independence conditions). Thus, \(Q_C\) is a significant share, and it has at most \(n\) qubits, and applying item \(5(a), n \geq n_1 + n_2\) which gives the desired bound.

With the matching inner and outer bounds, we conclude that the achievable rate region is the triangle with vertices \((0, 0), (0, 1), (1, 0)\), and time sharing between the communication paths \(A_1 \to C_1 \to C_2 \to B_1\) and \(A_2 \to C_1 \to C_2 \to B_2\) gives the optimal protocol. Note that the optimal communication protocol is exact and entanglement preserving.

- **Back-assisted case (with free backward classical communication)**

First, note that 2 bits of back classical communication can be used to reverse the direction of a qubit quantum channel: use the quantum channel to create 1 ebit, followed by teleportation in the reverse direction. Thus, free back communication makes quantum networks undirected. With this observation, we describe new communication protocols for the butterfly network.

**Inner bound:** The rate pair \((r_1, r_2) = (0, 2)\) is achieved by an exact, 1-shot, protocol. \(A_2\) sends one qubit along the path \(A_2 \to C_1 \to A_1 \to B_2\) and another qubit along the path \(A_2 \to B_1 \to C_2 \to B_2\) (see Fig. 4). These are edge-avoiding paths, and thus, two qubits can be transmitted in a single network-call. Likewise, \((r_1, r_2) = (2, 0)\) is also achievable, and so is the entire triangle with vertices \((0, 0), (2, 0), (0, 2)\).

![Diagram](image)

**FIG. 4:** The achieving protocol for the rate pair \((0, 2)\) for the back-assisted butterfly network.

- **Outer bound:** We will prove that \(r_1 + r_2 \leq 2\). Consider the cut \(S_1 = \{A_1, B_2\}\) and \(S_2 = \{C_1, C_2, A_2, B_1\}\). Let \(r\) be the maximum amount of entanglement between \(S_{1,2}\) created per network call. There are only two channels across this cut, so, \(r \leq 2\). Now, any asymptotic \(n\)-use protocol on the butterfly network communicating \(n(r_1 - \delta_n)\) qubits from \(A_1\) to \(B_1\) enables \(A_1, B_2\) and \(A_2, B_1\) to share at least \(n(r_1 + r_2 - 2\delta_n)\) ebits (with high fidelity). Per network use, \(r_1 + r_2 - 2\delta_n\) ebits are created. Altogether, taking large \(n\) limit, \(r_1 + r_2 \leq r \leq 2\).

Since the inner and outer bounds are matching, the inner bound gives the exact rate region (see Fig. 5), and the protocol described is optimal.

- **Two-way assisted case (with free two-way classical communication)**

Note that the outer bound for the back-assisted case still applies, thus, free two-way classical communication is no better than free back classical communication alone.

- **Forward-assisted case (with free forward classical communication)**
Intriguingly, we will see how free forward classical communication can effectively reverse the direction of some of the channels, but not all of them. Thus, the situation is intermediate between the unassisted and the back-assisted cases. We first describe a concrete protocol for the butterfly network, before abstracting a general rule.

**Inner bound:** The rate pair \((r_1, r_2) = (1/2, 1)\) is achieved by an exact, 2-shot, protocol. In the first network call, \(A_1\) distributes 1 ebit between \(C_1\) and \(B_2\). \(A_2\) sends one qubit to \(C_1\) who then teleports it to \(B_2\). Note that the classical communication for the teleportation is sent via the path \(C_1 \rightarrow C_2 \rightarrow B_2\). (See the dotted path in Fig. 5.) This leaves the \(C_1 \rightarrow C_2\) channel unused, leaving it as an additional resource for the second network call. For the second network call, the two paths \(A_1 \rightarrow C_1 \rightarrow C_2 \rightarrow B_2\) and \(A_2 \rightarrow C_1 \rightarrow C_2 \rightarrow B_1\) are used to communicate one qubit each from \(A_1\) to \(B_1\) and from \(A_2\) to \(B_2\). These two paths are edge-avoiding except for the \(C_1 \rightarrow C_2\) channel, but an additional use can be borrowed from the first network call. (See the solid paths in Fig. 6.) Likewise, \((r_1, r_2) = (1, 1/2)\) is also achievable. By monotonicity, \((1,0),(0,1),(1,1/2),(1/2,1)\) are also achievable, and so is the convex hull of \((0,0),(1,0),(0,1),(1,1/2),(1/2,1)\). (See Fig. 6.)

**Outer bound:** To match the inner bound, we need to prove three inequalities: \(r_1, r_2 \leq 1\) and \(r_1 + r_2 \leq 3/2\). Again, we consider any \(n\)-use protocol communicating the \(n_i = n(r_i + \delta_n)\)-qubit state \(|\psi_i\rangle\) from \(A_i\) to \(B_i\).

The free forward classical communication provides many other possibilities for encoding – now into both quantum and classical shares. The classical shares can be cloned and "broadcast downstream" for free.

Consider the encoding by \(A_1\). The state \(|\psi_1\rangle\) is encoded into 4 shares: a quantum share for each of \(A_1\), \(C_1\), and \(B_2\), and a common classical share for each of them. The shares to \(C_1\) form an authorized set, and by item \(\text{FIG. 6}\)\((b)\), the quantum portion has at least \(n_1\) qubits. But there are only \(n\) qubit-channels from \(A_1\) to \(C_1\). Thus, \(n_1 \leq n\) and \(r_1 \leq 1\). Similarly, \(r_2 \leq 1\).

We now prove that \(r_1 + r_2 \leq 3/2\). In particular, for any valid protocol, consider using it in the following way: \(A_1\) tries to send \(M_1\) where \(M_1\) is prepared in \(n(r_1 - \delta_n)\) ebits. Similarly for \(A_2\) and \(B_2M_2\). But as mentioned before, \(C_1\) received shares from \(A_{1,2}\) that are authorized for \(M_{1,2}\) respectively. This allows \(C_1\) to play the “man in the middle” attack – to keep \(M_{1,2}\) and to replace them by \(M'_{1,2}\), which is entangled with \(B'_{1,2}\) in possession (i.e., he pretends to \(B_{1,2}\) on the receiving end, and \(A_{1,2}\) on the retransmitting end). (More formally, treat the entire \(M_1M_2M'_1M'_2\) as the combined quantum secret, and \(C_1\) clearly holds an authorized set, and by item \(\text{FIG. 6}\)\(c\) he can perform the logical swap between \(M_1M_2\) and \(M'_1M'_2\)).

A protocol with rate pair \((r_1, r_2)\) can then be modified to one that shares \(n(r_1 - \delta_n)\) ebits between \(C_1\) and each of \(A_1\) and \(B_1\), and \(n(r_2 - \delta_n)\) ebits between \(C_1\) and each of \(A_2\) and \(B_2\). But only \(3n\) qubits have gone in and out of \(C_1\)'s laboratory in this modified protocol, upper bounding his total entanglement with \(A_{1,2}B_{1,2}\), which is \(2n(r_1 + r_2 - 2\delta_n)\). Thus, \(r_1 + r_2 \leq 3/2\), matching our inner bound for the achievable rate region (see Fig. 6).

**A general rule for reversing channels in forward-assisted quantum networks**

Consider a path \(\Gamma : A \leftrightarrow C_1 \leftrightarrow \cdots \leftrightarrow B\), where \(A, B\) are the sender and the receiver of interest, \(C_i\)'s are intermediate parties, and the directions of the quantum channels are variables in the problem. For the purpose of \(A \rightarrow B\) quantum communication via \(\Gamma\), naively, we want the entire path to consist of forward channels, but this turns out unnecessary. We state the following sufficient condition:

The path \(\Gamma\) from \(A\) to \(B\) can be used to communicate 1 qubit in a forward-assisted network if the following condition holds. For each segment \(\gamma\) of \(\Gamma\) running in the opposite direction, with boundary points \(C_i, C_f\), there is an entirely forward path \(\gamma'\) in the network
from $C_i$ to some $C_j \in \Gamma$ with $j \geq f$. Besides the boundary points, $\gamma$ and $\Gamma$ impose no further constraint on $\gamma'$.

In other words, an opposite running segment poses no problem as long as the network provides some forward path bridging its beginning to its end or beyond (see Fig. 7). To prove the sufficiency of this condition, we use teleportation. The opposite running segment $\gamma$, together with the segment between $C_f$ and $C_j$, can be used to establish an ebit between $C_i$ and $C_j$. $C_i$ then teleports the message to $C_j$.

- **Entanglement-assisted case**

We first define the assisting resource. Here, we assume that any two parties share free ebits. We discuss alternative models later.

Since $A_1, B_1$ share ebits, and similarly for $A_2, B_2$, by teleportation and superdense-coding, the rates for quantum communication are exactly half of those for classical communication via the quantum network, so we focus on the latter.

**Inner bound for classical communication:** Given free ebits, each quantum channel in the network can transmit 2 cbits by superdense coding [12]. Twice the unit square is achievable.

**Outer bound for classical communication:** The Holevo bound [20] (see also [13]) states that by using $n$ forward qubit-channels, unlimited back quantum communication, and arbitrary prior entanglement one cannot send more than $2n$ forward ebits. Consider the cut $S_1 = \{A_1, B_2\}$ and $S_2 = \{A_2, B_1, C_1, C_2\}$. Since there is only one forward quantum channel, no more than 2 ebits can be communicated from $A_1$ to $B_1$ per use of the network. Similarly for the classical communication from $A_2$ to $B_2$.

Thus the exact rate region for classical communication is twice the unit square, and that for quantum communication is the unit square.

**Alternative assisting models**

Another natural model of assistance is to allow free ebits only between neighboring parties in the network. We leave the achievable rate region for the butterfly network in this case as an open question. So far, we cannot find a good protocol that achieves the quantum rate pair $(1, 1)$. We believe that it is not achievable. If our belief holds, this alternative model has a continuity problem. Consider adding a complete graph of channels to the network, with arbitrarily small capacity for each edge, so that all pairs of parties are now “neighbors.” Then, the pair $(1, 1)$ is achievable – these added channels with negligible capacities change the communication rates abruptly.

Since the initial posting of this manuscript, Hayashi [21] has considered entanglement assistance between the senders and also between neighbors in the network, but this model is out of our present scope.

- **Summary for the butterfly network**

![FIG. 8: Summary of the achievable rate regions of the butterfly network. The entanglement assisted quantum rate region is also given by the left diagram.](image)

**III. ANOTHER EXAMPLE - THE INVERTED CROWN NETWORK**

We consider the quantum version of a more complicated network studied in [4] to illustrate our more general results. It is depicted in Fig. 9 and we will call it the inverted crown network.

![FIG. 9: The inverted crown network](image)

We will use techniques similar to those in Sec.II, skipping details in the arguments that should now be familiar.

- **Unassisted case**
**Inner bound:** The rate triplets $(1, 1, 0)$, $(0, 0, 2)$, $(1, 0, 1)$, and $(0, 1, 1)$ are achievable due to the following sets of paths:

![Diagram of achievable rate triplets](image)

FIG. 10: Paths for achieving the extremal rate triplets $(1, 1, 0)$, $(0, 0, 2)$, $(1, 0, 1)$, and $(0, 1, 1)$.

By monotonicity, $(1, 0, 0)$ and $(0, 1, 0)$ are also achievable. The convex hull of these points (together with the origin) is plotted in Fig. 12.

**Outer bound:** We will first use the mincut method (item 3 in Sec. 11). Let $S_{1,2}$ be a bipartite cut. Consider forward communication from $S_1$ to $S_2$. We obtain the following bounds:

$$
\begin{align*}
    r_1 &\leq 1 \quad \text{for } S_1 = \{A_1, C_1, B_2, B_3\} \\
    r_2 &\leq 1 \quad \text{for } S_2 = \{A_2, C_2, B_1, B_3\} \\
    r_3 &\leq 2 \quad \text{for } S_1 = \{A_1, B_2\} \\
    r_1 + r_2 &\leq 2 \quad \text{for } S_1 = \{A_1, B_2\} \\
    r_1 + r_3 &\leq 2 \quad \text{for } S_1 = \{A_1, A_3, C_1, B_2\}
\end{align*}
$$

(2)

Note that the 3rd and the 4th bounds hold even with free two-way classical communication.

By inspection, the inner bound in Fig. 12 can be matched given the 1st and 2nd inequalities above, together with $r_1 + r_2 + r_3 \leq 2$. The last inequality can be proved similarly to the case for the butterfly network, and we will be brief here. Let $M_i$ be the $n_i$-qubit message from $A_i$ to $B_i$, with reference $R_i$. We take the quantum secret to be $M_1, M_2, M_3$, and the combined reference $R = R_1, R_2, R_3$. Let $Q_1$ denote the $A_1 \rightarrow B_2$ communication, $Q_2$ the $A_2 \rightarrow B_1$ communication, and $Q_C$ denote the $A_3 \rightarrow C_{1,2}$ communications combined. Again, for $B_1$ to recover $M_1, I(Q_1 : R_1)$ has to be small, and similarly for $I(Q_2 : R_2)$. By causality $R_1Q_1, R_2Q_2$ and $R_3$ are all independent. Then, $I(Q_1Q_2 : R) = S(Q_1Q_2) + S(R_1R_2R_3) - S(Q_1Q_2R_1R_2R_3) = I(Q_1 : R_1) + I(Q_2 : R_2)$ is small, where once again, the equality is due to the various independence conditions. But $Q_{1,2,C}$ is authorized, thus $Q_C$ is significant, and has at least $n_1 + n_2 + n_3$ qubits, while having at most $2n$ qubits. Thus $r_1 + r_2 + r_3 \leq 2$ as claimed, and the inner bound is matched by the outer bound.

We remark that in the analogous problem of sending classical information through the classical inverted crown network, the same outer bound on the rate region holds. (Bounds on $r_{1,2}$ due to the mincut property also hold classically, and [4] proves that $r_1 + r_2 + r_3 \leq 2$.)

**Forward-assisted case**

**Inner bound:** The rate triplets $(1, 1, 0)$, $(1, 0, 2)$, $(0, 1, 2)$ are achievable. The first is achieved without assistance (see previous subsection). The point $(0, 1, 2)$ is achieved by the paths depicted in the left diagram of Fig. 11. To reverse the path $A_2 \rightarrow A_3$, we use the “bridge” $\gamma' = A_3 \rightarrow C_2 \rightarrow B_1$ (see the general rule for reversing paths in Sec. 11). Similarly for the triplet $(0, 1, 2)$. Thus we obtain an inner bound that is the convex hull of $(0, 0, 2)$, $(1, 1, 0)$, $(1, 0, 2)$, $(0, 1, 2)$, $(1, 0, 0)$, $(0, 1, 0)$, and the origin. (See Fig. 12.)

**Outer bound:** From Fig. 12, it suffices to show that $r_{1,2} \leq 1$, $r_3 \leq 2$, and $2(r_1 + r_2) + r_3 \leq 4$ in order to match the inner bound. We have $r_{1,2} \leq 1$ even with free forward classical communication, because the messages to $A_3$ still form an authorized set and quantum-classical compression does not decrease the sizes of the quantum parts. The bound $r_3 \leq 2$ proved in the unassisted case holds even with two-way assistance. The remaining bound $2(r_1 + r_2) + r_3 \leq 4$ can be proved as follows.

In the absence of back communication, the $A_1 \rightarrow A_3$ message has to be authorized for $|\psi_1\rangle$ and the $A_2 \rightarrow A_3$ message has to be authorized for $|\psi_2\rangle$. Running an argument similar to that for the butterfly network, on $A_3$ replacing $|\psi_{1,2}\rangle$ by her own messages, a protocol that communicates $n_i$ qubits from $A_i$ to $B_i$ can be used to establish $2(n_1 + n_2) + n_3$ bits between $A_3$ and $A_{1,2}B_{1,2,3}$. But there are only $4n$ channels in and out of $A_3$, thus $2(r_1 + r_2) + r_3 \leq 4$.

We summarize the results for the last two subsections in the following figure:

**Back-assisted case**

**Inner bound**

The rate points $(1, 0, 2)$ and $(0, 1, 2)$ can be achieved as in the forward-assisted case. In addition, the rate points $(2, 0, 1)$ and $(0, 2, 1)$ are also achievable. The paths to

![Diagram of achievable rate triplets](image)

FIG. 11: Sets of paths for achieving the extremal rate triplets $(1, 0, 2)$ and $(0, 1, 2)$ for the forward-assisted inverted crown network.
FIG. 12: The achievable rate regions for the inverted crown network in the cases with no free classical communication and free forward classical communication.

FIG. 13: Paths for achieving the extremal rate triplet \((2, 0, 1)\) for the backward or two-way assisted inverted crown network. All six paths can be used by calling the network twice, thus achieving the stated rates.

FIG. 14: The achievable rate region for the inverted crown network given free backward or two-way classical communication.

achieve the former are shown in Fig. 13 and the latter can be achieved similarly. Thus, we obtain Fig. 14 for the inner bound.

**Outer bound**

Consider the cuts used in Eq. (2) for the unassisted case, but allow free two-way classical communication now. The 3rd and the 4th inequalities, \(r_3 \leq 2\) and \(r_1 + r_2 \leq 2\), stay the same, while the 5th inequality becomes \(r_1 + r_2 + r_3 \leq 3\), matching our inner bound.

- **Entanglement assisted case**

Inner bounds can be obtained from known classical solutions [4], whose outer bounds will also apply if proposition \(P\) in Sec. IV.D is proven true.

IV. GENERALIZATION TO OTHER NETWORKS

As we have seen in Sec. II, routing (with time sharing) is sufficient to generate the entire achievable rate region. It is suggestive that routing is indeed optimal for more general networks, and finding maximal sets of edge avoiding paths provides optimal protocols. We have not been able to prove such a conjecture in full generality. In this section, we present some ideas and proofs in special cases.

In the following, each channel in the network has a capacity that is an arbitrary nonnegative number. Since we allow an asymptotically large number of network calls, without loss of generality, the capacities can be taken as integers. Conditions imposed on the network and assisting resources will vary from case to case.

We have not encountered a situation that requires nontrivial time-ordering of individual channel uses (within or across network calls) to achieve optimality. In any case, time-ordering will not affect the optimal rates since in the asymptotic limit, nontrivial time-ordering can be effectively achieved, by using a negligible fraction of earlier network calls inefficiently or by “double-blocking” (running in parallel many copies of an arbitrarily ordered use protocol).

A. The case with a general number of sender-receiver pairs in shallow networks

In this class of networks, we impose three conditions: (1) there are no out-going channels from any receiver in the given network, and (2) the maximum length of any simple (i.e. without closed loops) path from a sender to any receiver is bounded by \(d = 3\), and (3) there is no 4-cycle involving a sender (detail later). The most general situation manifesting conditions (1) and (2) is depicted in Fig. 15 and condition (3) disallows any 4-cycle with vertices \(A_i, C_{1j_1}, C_{2j_2}, C_{1j_3}\) for any \(i, j_1, j_2, j_3\). For an arbitrary positive integer \(k\), for each \(i = 1, \ldots, k\), a sender \(A_i\) wants to send a message \(|\psi_i\rangle\) to the receiver \(B_i\). It is crucial that \(|\psi_i\rangle\) are independent messages. There are outgo-
We show that routing is optimal in the case without any classical communication assistance.

**Proof (or proof ideas):**

Consider the most general $n$-use protocol. For each channel, we can group together the messages from all $n$ uses as a single piece.

Denote the message from $C_{2j}$ to $B_i$ as $Q_{2ji}$. The quantum messages $\{Q_{2ji}\}$ received by $B_i$ form an authorized set for $|\psi_i\rangle$. It also means that the quantum messages $\{Q_{2ji'}\}_{j' \neq i}$ form an unauthorized set. In other words, the entire set of messages $\{Q_{2ji}\}$ from all the $C_{2j}$’s to all the $B_i$’s form a tensor product encoding scheme for the tensor product secret $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$. The salient property here is that, we can say that message $Q_{2ji}$ is a share of $|\psi_i\rangle$ alone, and not of any other $|\psi_{i'}\rangle$ for $i' \neq i$.

(Possible entanglement between the messages of $B_i$ and $B_j$ will be decoded to a state independent of their messages $|\psi_i\rangle$ and $|\psi_j\rangle$.)

Now consider messages from the $C_{1j}$’s to the $C_{2j}$’s. Each $C_{1j}$ has just received from each $A_i$ and if he entangles the messages from $A_{i_1}$ and $A_{i_2}$ and distributes shares to different $C_{2j}$’s, the latter will not be able to re-encode the shares to the product form mentioned above (the only case in which this is not obvious is a 4-cycle of the forbidden type). Thus, the messages $|\psi_i\rangle$ are never jointly coded in any part of the network, and the optimality of routing follows.

Our proof technique has not taken advantage of the optimality of the protocol analyzed. In the presence of these 4-cycles, we cannot rule out a protocol that entangles the messages at the $C_{1j}$’s, but such a protocol appears less efficient. Unfortunately, we have not been able to turn this intuition into a rigorous argument.

**Forward-assisted, back-assisted and two-way assisted cases:**

The forward-assisted case can be analyzed similarly, provided the possible inversion of the intermediate edges is taken into account. In the back-assisted case, and in network not obeying condition (1), the receivers are no longer information sinks, but it still holds that each receiver can only retain unauthorized shares of other messages (though they can help in transmitting them). However, including all the extra possible paths through the receivers makes most networks too deep for the proof to apply. For example, our proof applies to the butterfly network (Fig. 1) but not the inverted crown network (Fig. 9).

**General discussion**

The proof ideas used in this subsection, unfortunately, do not extend readily to deeper networks. Whether there are deeper networks that require entangling coding strategies remains an interesting open issue to be resolved.
B. Outer and inner bounds on the achievable rate regions

Consider the $k$-pair communication problem in the most general network. For any subset $\Sigma$ of the $k$ pairs of sender/receiver, we will derive upper and lower bounds for their rate sum.

Outer bound

The upper bound of the rate sum is via the min-cut idea discussed at the beginning of Sec. II. Let $S$, $R$ be any bipartite cut (partition) of the vertices such that the senders of $\Sigma$ are in $S$ and the receivers are in $R$. Let $c_\rightarrow(S)$ be the sum of the capacities of all the channels from $S$ to $R$ and $c_\leftarrow(S)$ be that from $R$ to $S$. Then, the rate sum for $\Sigma$ is upper bounded by $\min_S c_\rightarrow(S)$ in the unassisted case. A weaker bound holds in networks assisted by forward, backward, or two-way classical communication as follows. For any cut $S$, $R$ that separates each sender/receiver pair in $\Sigma$, the rate sum is upper bounded by $\min_S c_\rightarrow(S) + c_\leftarrow(S)$. To see the first statement, for any cut $S$ and $R$, any protocol for the $k$-pair communication problem gives a method to communicate from $S$ to $R$, whose rate cannot exceed $c_\rightarrow(S)$. For the second statement, any protocol for the $k$-pair communication problem gives a method to generate entanglement between $S$ and $R$ at a rate that cannot exceed $c_\rightarrow(S) + c_\leftarrow(S)$ even when assisted by free two-way classical communication.

Inner bound

A lower bound for the rate sum for $\Sigma$ is given by constructing edge avoiding paths. Here, we can interpret an edge with capacity $c$ as $c$ edges of unit capacity. (Recall that integer values of capacities are general.) The lower bound for the rate sum is simply the maximum number of paths connecting each sender in $\Sigma$ to the correct receiver. In the unassisted case, all edges in each path have to be properly oriented; similarly in the forward assisted case, except we allow reversal of the edges if the general rule described in Sec. II is satisfied; in the back assisted or two-way assisted case, the edges are simply undirected.

C. 2-pair communication in arbitrary networks with back-assistance

The setting is a special case of the previous subsection with $k = 2$ and with free classical back communication (thus the channels are undirected). Here, we will first tighten the rate sum. Then, we show that the upper bounds on the individual rates and the rate sum completely define the achievable rate region, by proving their achievability.

Improved upper bound on the rate sum

Consider any $n$-use protocol that communicates from $A_1$ to $B_1$ and from $A_2$ to $B_2$ with a rate sum $r$. Clearly the protocol can generate, at the same rate, entanglement between $A_1, A_2$ and $B_1, B_2$. Thus, for any bipartite cut $S_h, R_h$ separating $A_1, A_2$ from $B_1, B_2$, if $c_\rightarrow(S_v)$ is the sum of the capacities of all the channels (in both directions) between $S_v$ and $R_v$, then, $r \leq c_\rightarrow(S_h)$. But the communication protocol also generates entanglement between $A_1, B_2$ and $A_2, B_1$ at a rate $r$, and applying an argument similar to the above, $r \leq c_\rightarrow(S_h)$. Thus, for any bipartite cut $S_h, R_h$ separating $A_1, B_2$ from $A_2, B_1$. Minimizing over all $S_v$, $S_h$, it follows that

$$r \leq \min \left[ \min_{S_v} c_\rightarrow(S_v), \min_{S_h} c_\rightarrow(S_h) \right].$$

Achievability

We now show that the above upper bound on the rate sum, together with the upper bounds on the individual rates given by Sec. IV B, define the achievable rate region. Take the partitions $S_v, R_v$ and $S_h, R_h$ that respectively minimize $c_\rightarrow(S_v)$ and $c_\rightarrow(S_h)$, and take intersections to obtain a partition of the vertices into 4 subsets (see Fig. [17]). We can bundle the channels between these 4 subsets into 6 groups (labeled $v_1, h_1$, and $d_1$ pertaining to the vertical cut, the horizontal cut, and the diagonals).

Use the max-flow-min-cut theorem (see Sec. II), we can find the paths for the vertical cut, extending $v_1, d_1$ to $A_1, B_1$, and similarly for the horizontal cut. (See the red paths in Fig. [18].) The paths through $d_1$ avoid all other red paths, but those through $h_1$ and $v_1$ may share edges. In Fig. [18] we schematically show merged paths running towards $A_2, B_1$. Most generally, the red paths may merge and diverge in other locations, but the important features are that they reach $A_1$ and $B_2$, and may impose bottlenecks for flows in/out of the individual $A_1, B_1$. We label the possible bottlenecks by $u_1, b_1$. With a slight abuse of notations, we denote the capacities

FIG. 17: How the two mincuts partition the vertices into 4 groups

4 subsets into 6 groups (labeled $v_1, h_1$, and $d_1$ pertaining to the vertical cut, the horizontal cut, and the diagonals).
the rate sum is already achieved by maximizing
way described above, without the need for any further
\( \gamma \) qubits through \( A \).

By symmetry of the problem, the rate pair \((r_1, r_2, \cdots)\), \(A_1\) and \(A_2\) use the
paths \(d_1, 2\) independently. They have to share the use of
\(v_1, h_1, v_2, h_2\) (collectively called the “square”). \(A_1\) can send qubits independently through the paths
\[ r_1 \leq r_1^* := \min(a_1, b_1, v_1 + h_1, v_2 + h_2) + d_1 \] (4)
\[ r_2 \leq r_2^* := \min(a_2, b_2, v_1 + h_2, v_2 + h_1) + d_2 \] (5)
\[ r \leq r^* := \min(v_1 + v_2, h_1 + h_2) + d_1 + d_2 \] (6)

To achieve the rate pair \((r_1^*, r^* - r_1^*)\), \(A_1\) and \(A_2\) use the
paths \(d_1, 2\) independently. They have to share the use of
\(v_1, h_1, v_2, h_2\) (collectively called the “square”). \(A_1\) can send qubits independently through the paths
\[ \gamma_1 : a_1 \rightarrow v_1 \rightarrow h_2 \rightarrow b_1 \] (7)
\[ \gamma_2 : a_1 \rightarrow h_1 \rightarrow v_2 \rightarrow b_1 \] (8)

Case (1) If \(r_1\) is limited by \(a_1\) or \(b_1\), \(A_1\) sends
\( \frac{1}{2} \min(a_1, b_1) \) qubits through each of \(\gamma_1, 2\). But the rate
sum is limited by the square, and it is easy to check that the unused channels in the square support enough
\(A_2 \rightarrow B_2\) communication to achieve the rate sum given
by Eq. (9). Case (2) If \(r_1\) is limited by the square,
\(A_1\) sends \(\min(r_1, h_2)\) qubits through \(\gamma_1\) and \(\min(h_1, v_2)\) qubits through \(\gamma_2\). Case (2a) If \(v_1 < h_2\) and \(h_1 < v_2\), the path \(h_2 \rightarrow v_2\) will be available for \(A_2\) to communicate to \(B_2\) to achieve the rate sum. Similarly for the case \(v_1 > h_2\) and \(h_1 > v_2\). Case (2b) Otherwise, either \(h_1 + h_2\) or \(v_1 + v_2\) will be the limiting factor, and the rate sum is already achieved by maximizing \(r_1\) in the
way described above, without the need for any further contribution from the \(A_2 \rightarrow B_2\) communication.

By symmetry of the problem, the rate pair \((r^* - r_2^*, r_2^*)\)
is also achievable. Invoking monotonicity and time sharing, the characterization of the achievable region is com-
pleted.

D. Any arbitrary entanglement-assisted network

Our discussion for the quantum butterfly network applies to the most general quantum network communication
problem. Because of superdense coding and teleportation, the achievable rate region for classical communica-
tion in a quantum network is exactly twice of that for quantum communication. The latter is clearly inner
bounded by the achievable rate region for sending classical data via the corresponding classical network. This
inner bound is tight if the following network generalization of Holevo’s bound holds.

Let \(P\) be the following proposition:

If \((r_1, r_2, \cdots)\) is not an achievable point in the
classical rate region of a classical network, then, \((2r_1, 2r_2, \cdots)\) is not an achievable point in the
classical rate region of the corresponding quantum network with arbitrary entan-
glement assistance.

If proposition \(P\) holds, then, the exact achievable rate region for quantum (classical) communication in
an entanglement-assisted quantum network is exactly (twice) the classical rate region of the (unassisted) classical
network.

V. OTHER NETWORK COMMUNICATION
PROBLEMS

In this section, we discuss two other quantum network communication problems that are very different from the
\(k\)-pair communication problem.

A. Quantum multicasting

Reference [1] also studies the multicast problem in which a single source transmits the same message to \(k\) different
receivers.

We define a quantum analogue to the problem, by considering \(k\) pairs of senders and receivers, \(A_i\) and \(B_i\). A
reference party \(R\) creates the state \(|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes (k+1)} + |1\rangle^{\otimes (k+1)})\) and gives one qubit of \(|\psi\rangle\) to each \(A_i\), keeping
one qubit to himself. The goal is for \(R\) to share \(|\psi\rangle\) with the \(B_i\)’s, enabled by the quantum communication
through the given quantum network. The optimal rate is given by the maximum number of copies of \(|\psi\rangle\) shared per
use of the network, allowing a large number of network calls.

In the quantum problem, one can achieve at least the rate
region of the classical problem, by applying any classical
strategy in the computation basis. Whether this inner
bound is tight or not is an open problem.
B. Multi-party entanglement of assistance

In quantum communication theory, in some settings, one believes that it is easy to perform classical communication but hard to obtain any quantum resource. It is a common scenario to assume that the remote parties share a quantum state and the problem is to determine the amount of quantum communication that can be generated given unlimited classical communication (between all of them). By teleportation, the problem reduces to generating ebits between sender-receiver pairs. Much has been done for one sender-receiver pair, analogous to the one sender-receiver pair situation in network communication. Here, we consider the problem of generating ebits simultaneously among many pairs of parties, which relates to simultaneous network communication (though not specifically the k-pair communication problem). Related problems have been considered recently [22, 23, 24, 25].

Suppose \( m \) parties share a pure state \( |\psi\rangle \). Parties \( A_1, B_1 \) are special. The other \( m-2 \) parties are allowed to send classical communication to them (but not vice versa). The entanglement of assistance for \( A_1, B_1 \) \([26]\), (also known as localizable entanglement \([27]\)) is defined as the maximum number of ebits they can share afterwards. Clearly, the optimal strategies for those \( m-2 \) parties are to make measurements (with rank-1 measurement operators) and to communicate the measurement outcomes to \( A_1, B_1 \). This gives rise to the following expression for the regularized entanglement of assistance, the maximum number of ebits between \( A_1, B_1 \) created per copy of the state \( |\psi\rangle \), when large number of copies are shared.

\[
E^\infty_n(|\psi\rangle, A_1; B_1) = \sup_k \sum p_k E(|\psi_k\rangle) \tag{9}
\]

where the supremum is taken over the \( m-2 \) local measurements, \( k \) denotes the \( m-2 \) measurement outcomes, and \( |\psi_k\rangle \) is the corresponding postmeasurement state of \( A_1, B_1 \), and \( E(\cdot) \) is the usual measure for pure state bipartite entanglement defined as follows. For any pure bipartite state \( |\phi\rangle \), let \( \phi_{1,2} \) be the reduced density matrices on the two parties and \( S(\rho) := -\text{Tr} \log \rho \) be the von Neumann entropy of \( \rho \). Then, \( E(|\phi\rangle) := S(\phi_1) = S(\phi_2) \). Thus, for a set of parties holding a pure state and a subset of parties \( \Sigma \), we simply write \( S(\Sigma) \) for the entanglement between \( \Sigma \) and the rest of the parties. It was found in \([22, 24]\) that

\[
E^\infty_n(|\psi\rangle, A_1; B_1) = \min_T \{ S(\mathcal{A}T), S(BT^c) \} \tag{10}
\]

where \( T \) and \( T^c \) is a partition of the other \( m-2 \) parties. With extra classical communication from \( A_1 \) to \( B_1 \), we relate back to the usual communication problem of one sender-receiver pair in a static version of a network (a multipartite state).

In fact, by the state merging protocol in \([22, 24]\), for any \( T, T^c \), each copy of \(|\psi\rangle\) can generate:

1. \( S(A_1T) \) ebits between \( A_1 \) and \( B_1 \)
2. \( -S(T|A_1) \) ebits between \( T \) and \( A_1 \)
3. \( -S(T^c|B_1) \) ebits between \( T^c \) and \( B_1 \)
where the conditional entropy \( S(T|A_1) \) is defined as \( S(A_1T) - S(A_1) \) and similarly for \( -S(T^c|B_1) \).

In fact, using the chain rule, one can see that each party within the groups \( T \) and \( T^c \) can distill (or consume) an amount of entanglement given by \( -S(T_i|A_1T_1T_2...T_{i-1}) \) for the parties in the partition \( T \) and likewise \( -S(T^c_j|B_1T^c_1T^c_2...T^c_{j-1}) \) for the individual parties within \( T^c \). Here, the \( T_i \) are the parties in the partition \( T \), and \( T^c_j \) are in \( T^c \). Yang and Eisert \([arXiv:0907.3457]\) have since shown that if the partition \( T^c \) is empty, then one can eliminate the need to consume entanglement.

This allows more sender-receiver pairs to communicate with one another depending on the initial state and the exact form of classical communication assistance.

VI. CONCLUSION

We have studied the k-pair communication problem for quantum data in quantum networks under different assisted scenarios. We obtained a general statement for the optimality of routing in shallow networks without a certain type of 4-cycles and worked out the exact rate regions in a number of simple cases. A number of problems remain unresolved, including the validity of proposition \( P \) in Sec. IV D (outer-bounding the entanglement assisted classical rate points in quantum networks), and the optimality of routing in networks with larger depth.

Acknowledgments

We are indebted to David Bacon for drawing our attention to reference [9] and Daniel Gottesman for discussions on quantum secret sharing and for providing one of our upper bounds. We thank Andris Ambainis and Rahul Jain for comments on communication complexity, Yaoyun Shi for constructive criticisms, and Michael Ben-Or and Nicholas Harvey for chats on other open problems in the classical setting. We thank Panos Aliferis for an inspiring verse, which is modified and shared here:

Eat and drink and smoke and write and sleep
and eat and drink and play and prove and correct and laugh and ... submit!
... and sleep and eat and edit and replace.

DL was supported by CRC, CRC-CFI, CIAR, NSERC, ARO, and MITACS. JO acknowledges the support of the Royal Society and EU Project QAP (IST-3-015848). AW was supported by EU grant RESQ (IST-2001-37559), the U.K. Engineering and Physical Sciences Research Coun-
[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] R. Yeung and Z. Zhang, “Distributed source coding for satellite communications,” IEEE Trans. Inf. Theory, vol. 45, no. 4, pp. 1111, 1999.

[3] Z. Li and B. Li, “Network coding: The case of multiple unicast sessions,” in In Proceedings of the 42nd Allerton Annual Conference on Communication, Control, and Computing, 2004.

[4] N. J. A. Harvey, R. D. Kleinberg, and A. R. Lehman, “Comparing network coding with multicommodity flow for the k-pairs communication problem.” Technical Report MIT-LCS-TR-964, September 2004.

[5] Z. Li and B. Li, “Network coding in undirected networks,” in In Proceedings of the 38th Conference on Information Science and Systems (CISS), 2004.

[6] K. Jain, V. Vazirani, R. Yeung, and G. Yuval, “On the capacity of multiple unicast sessions in undirected graphs,” IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2805–2809, 2006.

[7] N. J. A. Harvey, R. D. Kleinberg, and A. R. Lehman, “On the capacity of information networks,” IEEE Trans. Inf. Theory, vol. XX, no. Y, pp. ZZZZ, 2006.

[8] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “Quantum network coding,” 2006, quant-ph/0601088.

[9] Y. Shi and E. Soljanin, “On multicast in quantum networks,” in Proceedings of the 40th Annual Conference on Information Science and Systems (CISS), 2006.

[10] D. Leung, J. Oppenheim, and A. Winter, “Quantum network communication – the butterfly and beyond,” 2006, quant-ph/0608223.

[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett., vol. 70, pp. 1895–1899, 1993.

[12] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,” Phys. Rev. Lett, vol. 69(20), pp. 2881–2884, 1992.

[13] R. Cleve, W. van Dam, M. A. Nielsen, and A. Tapp, “Quantum entanglement and the communication complexity of the inner product function,” in Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications, Lecture Notes in Computer Science. 1998, vol. 1509, pp. 61–74, Springer-Verlag, quant-ph/9708019.

[14] L. R. Ford, Jr. and D. R. Fulkerson, Flows in networks, Princeton University Press, 1962.

[15] D. Gottesman, “On the theory of quantum secret sharing,” Phys. Rev. A, vol. 61, pp. 042311, 2000, quant-ph/9910067.

[16] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, “A quantum information theoretical model for quantum secret sharing schemes,” Quant. Inf. Comp., vol. 5(1), pp. 68–79, 2005.

[17] Let \( S() \) denote the von Neumann entropy, and \( I^\text{coh}(S_1)S_2 = S(S_2) - S(S_1,S_2) \) be the coherent information from \( S_1 \) to \( S_2 \). Let \( S \) be the secret, purified by the reference system \( R \), encoded into a secret sharing scheme, and to be decoded in \( \tilde{S} \). If the initial state in \( SR \) and the final state in \( SR \) are \( \epsilon \)-close to each other in trace distance, then the coherent information \( I^\text{coh}(R)\tilde{S} \) has to be \( \epsilon \)-close to \( I^\text{coh}(R)S \). (Note that \( \epsilon \) and \( \epsilon \) are related by Fannes inequality. For constant size secret, they vanish together. For asymptotically large secret of dimension \( 2^m \), where \( m \) is the number of uses of the network and \( r \) is the rate of transmission, \( \epsilon \approx n \epsilon \approx \epsilon \rightarrow 0. \) That \( \epsilon \rightarrow 0 \) is often used as an alternative condition for preserving entanglement fidelity.) Let \( S_u \) be the significant share, and \( S_u \) be the unauthorized set such that \( S_u \cup S_u \) is authorized. In other words, \( \tilde{S} \) is obtained from \( S_uS_u \) by a quantum operation. But the coherent information is monotonically decreasing under such operations. Therefore,

\[
I^\text{coh}(R)S_uS_u \geq I^\text{coh}(R)\tilde{S} \geq I^\text{coh}(R)S - \epsilon'.
\]

Using the expression of \( I^\text{coh} \) and the joint purity of \( RS_u \),

\[
S(S_uS_u) - S(RS_uS_u) \geq S(S) - \epsilon'.
\]

Applying to the above the Araki-Lieb inequality, which states that \( \forall S_1S_2S(S(S_1) - S(S_2)) \geq S(RS_uS_u) = S_1S_u = S_2 \), we have

\[
S(S_uS_u) - S(RS_u) \geq S(S) - \epsilon'.
\]

Since \( S_u \) is unauthorized, the mutual information between \( S_u \) and \( R \) is small, so we have \( S_u(S_u(S_u) + S(R)) - S_u(S_u) \leq \gamma \) for some small \( \gamma \). Substituting this in the above,

\[
S(S_uS_u) + \gamma - [S(S_u) + S(R)] + [S(S_u) \geq S(S) - \epsilon'.
\]

Finally, applying subadditivity \( S(S_u) \leq S(S_u) \leq S(S_u) \) to the LHS, and noting that \( S(R) = S(S) \), and rearranging terms,

\[
S(S_u) \geq S(S) - (\epsilon' + \gamma)/2
\]

[18] H. Barnum, R. Josza, P. Hayden, and A. Winter, “On the reversible extraction of classical information from a quantum source,” Proc. Roy. Soc. (Lond.) A, vol. 457, pp. 2019–2039, 2001.

[19] All notations are as defined in the statement of the result in the main text. Let \( \tilde{\approx} \) denote the relation between two states differing by at most \( \epsilon \) in trace distance. The isometry \( Y \) can be represented as a unitary taking \( AC \) to \( SE \), with \( C \) initially in some fixed state \( |0 \rangle \). Then, the approximate invertibility condition can be stated as:

\[
\forall |\psi\rangle_RS \quad (IBDE \otimes Y_{AC})(IR \otimes W_S)|\psi\rangle_RS |0\rangle_c \tilde{\approx} |\psi\rangle_RS |\phi\rangle_{BDE}
\]

Equation (16) holds when the systems \( BDE \) are traced out, due to the notion of approximation in the achievable
rate region. Without tracing out BDE, the global state is pure, and Eq. (14) follows from Uhlmann’s theorem. Note that the same state |φ⟩_{BDE} appears on the RHS for all |ψ⟩_{RS}, or else |φ⟩_{BDE} allows extraction of more information about the state |ψ⟩_{RS} beyond what is allowed by the error ε. We will use Eq. (16) in two different ways. First, due to the universal quantifier, we apply Eq. (16) to the state (I_R ⊗ U_S)|ψ⟩_{RS} instead.

∀ |ψ⟩_{RS} (I_R ⊗ Y_{AC})(I_R ⊗ W_S U_S)|ψ⟩_{RS}|0⟩_C 
\approx (I_{RBDE} ⊗ U_S)|ψ⟩_{RS}|0⟩_C (17)

Second, we replace the expression in the square bracket above by using Eq. (16):

∀ |ψ⟩_{RS} (I_R ⊗ W_S U_S)|ψ⟩_{RS}|0⟩_C 
\approx (I_R ⊗ Y_{AC})(I_R ⊗ W_S)|ψ⟩_{RS}|0⟩_C (18)

where the error above is obtained by using the triangle inequality for the trace distance, and it is at most the sum of the errors in Eqs. (16) and (17). Now, applying Y† to both sides of Eq. (18), we obtain

∀ |ψ⟩_{RS} (I_R ⊗ W_S)|ψ⟩_{RS}|0⟩_C 
\approx (I_R ⊗ Y_{AC})(I_R ⊗ W_S U_S)|IBDE ⊗ Y_{AC}⟩ \times (I_R ⊗ W_S)|ψ⟩_{RS}|0⟩_C (19)

which is the result we asserted.

[20] A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” Problemy Peredachi Informatsii, vol. 9(3), pp. 3–11, 1973, [A. S. Kholevo, Problems of Information Transmission, vol. 9, pp. 177-183 (1973)].