

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 communication of quantum information in networks of (directed) quantum channels. We consider the asymptotic rates of high fidelity quantum communication between specific sender-receiver pairs, and obtain outer and inner bounds of the achievable rate regions. All four scenarios of classical communication assistance (none, forward, backward, and two-way) are considered. For networks in which (1) the receivers are information sinks, (2) the maximum distance from senders to receivers is small, and without further constraints on the networks (such as the number of intermediate parties), we prove that rerouting of quantum information is optimal. Furthermore, the optimal use of the free assisting classical communication is simply 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. These complete solutions apply to many networks, including the butterfly network.

I. INTRODUCTION

The problem of network coding was introduced in the classical setting by Ahlswede, Cai, Li, and Yeung [1]. Consider a communication network, represented by a weighted directed graph, in which vertices represent parties and edges represent perfect communication channels (with capacities given by the weight). Most generally, any party may want to send data to any other party, and the communicated data can be correlated in time and space.

This paper is concerned with quantum communication through quantum networks. We primarily focus on the k -pairs communication problem, in which there are k specific (disjoint) sender-receiver pairs, who are trying to communicate k independent messages in the given network. Our goal is to find the optimal achievable rates (given by the boundary of a k -dimensional achievable rate region).

Classically, there are scenarios [1] in which optimal solutions are achieved with nontrivial coding techniques (i.e., at each node, the party can transmit any function of the data), in sharp contrast to a “multicommodity” flow with commodities simply being rerouted (like water flowing through a network of pipes, or cars getting through a traffic network). For example, that is the case in the butterfly network (see Sec. II).

In our study of high fidelity quantum communication through an asymptotically large number of uses of the (quantum) butterfly network, the optimal protocol turns out to involve only rerouting. We also study communication scenarios with various auxiliary resources, and optimality of rerouting is essentially unchanged. Thus, quantum information flowing through a communication network resembles a classical commodity more than classical information. We believe that such behavior holds for a general network, and provide reasons why it is true for an arbitrary “shallow” quantum network in which

the maximum distance between any sender-receiver pair is small.

Our work was inspired by the earlier, complementary, study of Hayashi, Iwama, Nishimura, Raymond, and Yamashita on the quantum butterfly network [2]. 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 $2/3$. During the preparation of this manuscript, we found that Shi and Soljanin have studied a quantum version of multicasting in quantum network [3] that is complementary to our study.

We shall begin in Section II with the butterfly network as a motivating example. For this simpler case, we formalize the network communication problem of interest and review useful techniques. Then, we 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 optimality proof for rerouting of quantum information in 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 noise-

lessly 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 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. 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 [4], and in superdense coding 1 ebit and 1 qbit generate 2 cbits [5].

II. MOTIVATING EXAMPLE – THE 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* channels and two helpers C_1 and C_2 depicted in Fig. 1.

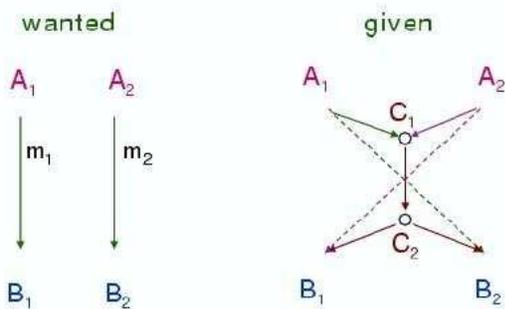


FIG. 1: The butterfly network. The left diagram represents the task to be achieved, the right diagram represents the available resources.

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.

Definition 1 *In the asymptotic scenario, we allow large number of calls to the network. Let \mathcal{P}_n denote a protocol that uses the network n times along with other allowed resources, and communicates m_1, m_2 of sizes $n(r_1 - \delta_n), n(r_2 - \delta_n)$ bits/qubits with fidelities at least $1 - \epsilon_n$ for $\delta_n, \epsilon_n \rightarrow 0$. 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.*

More generally, 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. The achievable rate region for such “ k -pair communication” can be defined analogously.

Note that in the asymptotic setting, imposing time ordering of the usage of the channels does not affect the achievable rate region. Also, we have not specified the measure of fidelity. Here, we want to have 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 optimal protocols turn out to be exact.

We collect some *general* tools and techniques that are useful, 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. For example, $S_1 = \{A_1, B_2, C_1\}$ and $S_2 = \{A_2, B_1, C_2\}$ in Fig. 1. We can bound the sum of communication rates from all parties in S_1 to all parties in S_2 by the sum of capacities of all forward communication channels from S_1 to S_2 .

For example, using the previous sample cut, 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 and back communication does not help, so, the capacity from S_1 to S_2 is at most 1. Since grouping the parties together can only increase the communicate rate, the rate sum from S_1 to S_2 in the original butterfly network is also at most 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 [6] 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 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 [7] that for exact schemes (reconstruction and hiding are perfect), the size of any significant share is at least the size of the quantum secret. A generalization of this result to the near-exact case was given in [8].

A quantum-classical dual compression scheme encodes a quantum source into a quantum part and a classical part. It was proved in [9] that the quantum part cannot be smaller than the von Neuman entropy of the source.

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 cut $S_1 = \{A_1, B_2, C_1\}$ 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,

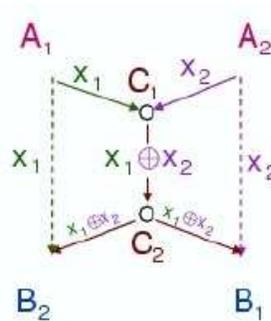


FIG. 2: The optimal protocol for the classical butterfly network. In the above, and from now on, we rearrange the locations of B_1, B_2 to improve diagrammatic clarity.

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 rerouting.

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, [2] 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 $2/3$ (though strictly better than $1/2$).

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

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. 6.) 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, $(1, 0), (0, 1)$ are also achievable, and so is the convex hull of $(0, 0), (1, 0), (0, 1), (1, 1/2), (1/2, 1)$. (See Fig. 8.)

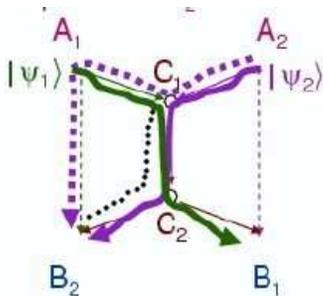


FIG. 6: The achieving protocol for the rate pair $(1/2, 1)$ in the back-assisted butterfly network. The dotted paths represent the teleportation of 1 qubit from A_2 to B_2 , with the quantum portion sent via the thick purple path, and the classical portion sent via the thin black path. Two other qubits are sent in the usual way via the other two solid paths.

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” 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 classical share for everyone. What B_1 can acquire about $|\psi_1\rangle$ has to go through C_1 , and since it is a significant share, its size is at least n_1 . Furthermore, 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, $r_2 \leq 1$.

To prove $r_1 + r_2 \leq 3/2$, note that the quantum part of the significant share of $|\psi_1\rangle$ from A_1 to B_1 has to go into the laboratory of C_1 and then out of it (either to C_2 or A_2). The same for the significant share of $|\psi_2\rangle$. Thus, a total of $2n(r_1 + r_2 + 2\delta_n)$ qubits go in and out of C_1 , but there are only $3n$ such channels in the protocol. Thus, $r_1 + r_2 \leq 3/2$. Therefore, our inner bound is exactly the achievable rate region (see Fig. 8).

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

Consider a path $\Gamma : A \leftrightarrow C_1 \leftrightarrow \dots \leftrightarrow B$, 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 Γ , naively, we want the entire path to consist of forward channels, but this turns out unnecessary. We state the following sufficient condition:

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

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

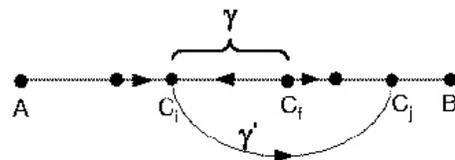


FIG. 7: A sufficient condition for reversing an opposite running segment γ in a communication path Γ from A to B

teleportation. The opposite running segment γ , 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 [5]. Twice the unit square is achievable.

Outer bound for classical communication: The Holevo bound [10] (see also [11]) states that by using n forward qubit-channels, unlimited back quantum communication, and arbitrary prior entanglement one cannot send more than $2n$ forward cbits. 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 cbits 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.

An alternative assisting model

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 so, this alternative model poses 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.

• Summary for the butterfly network

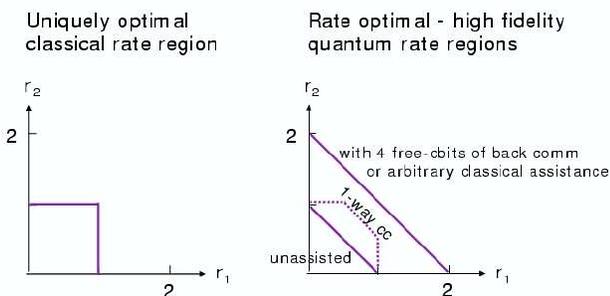


FIG. 8: Summary of the achievable rate regions of the butterfly network. The entanglement assisted quantum rate region is also given by the left diagram.

III. ANOTHER EXAMPLE - THE INVERTED CROWN NETWORK

We consider the quantum version of a more complicated network studied in [12] to illustrate our more general results. It is depicted in Fig. 9 and we will call it the inverted crown network.

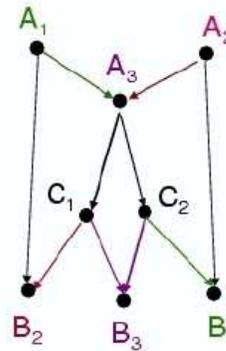


FIG. 9: The inverted crown network

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:

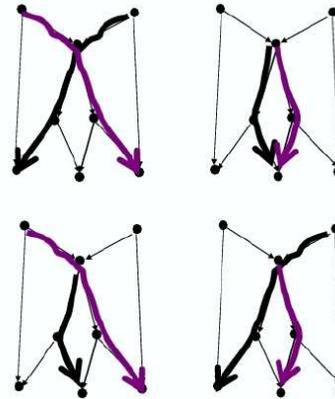


FIG. 10: Paths for achieving the extremal rate triplets $(1, 1, 0)$, $(0, 0, 2)$, $(1, 0, 1)$, and $(0, 1, 1)$.

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. II). Let $S_{1,2}$ be a bipartite cut. Consider forward communication from S_1 to S_2 . We obtain the

following bounds:

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

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 using the theory of quantum secret sharing. Let $|\psi_i\rangle$ of n_i qubits be the message from A_i to B_i . The $C_1 \rightarrow B_2$ communication is significant for the message $|\psi_2\rangle$, the $C_2 \rightarrow B_1$ communication is significant for the message $|\psi_1\rangle$, and the messages from $C_{1,2}$ to B_3 have to contain at least n_3 qubits. It follows that $C_{1,2}$ have to transmit at least a total of $n_1 + n_2 + n_3$ qubits, and they only receive 2 per network call from A_3 . 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 [12] 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 $(1, 0, 2)$ 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. II B). Similarly for the triplet $(0, 1, 2)$. Thus we obtain an inner bound that is the con-

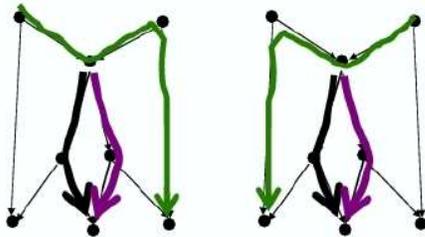


FIG. 11: Sets of paths for achieving the extremal rate triplets $(1, 0, 2)$ and $(0, 1, 2)$ for the forward-assisted inverted crown network.

vex 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 significant shares 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 messages from C_1 to B_2 has to be independent of $|\psi_{1,3}\rangle$ and depends only on $|\psi_2\rangle$. Likewise, the $C_1 \rightarrow B_3$ message can only depend on $|\psi_3\rangle$. If C_1 can uncorrelate these messages from the quantum and classical data received from A_3 , A_3 could have uncorrelated them before the transmission. Thus, the $A_3 \rightarrow C_1$ message already has the B_2 and B_3 portions separated. Similarly, the $A_3 \rightarrow C_2$ message contains separate quantum data for B_3 and B_1 . Furthermore, data for $B_{1,2}$ sent out of A_3 has to be first received from $A_{1,2}$. Noting that there are only 4 channels in and out of A_3 , we have $2(r_1 + r_2) + r_3 \leq 4$.

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

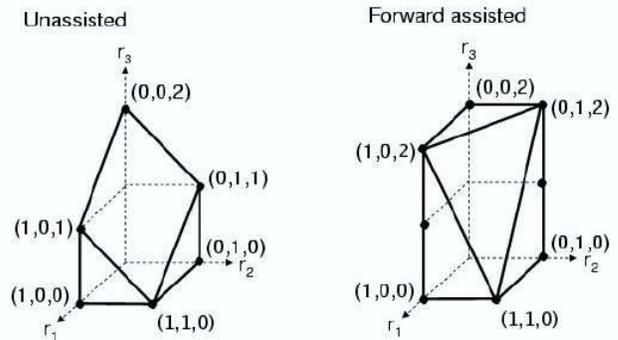


FIG. 12: The achievable rate regions for the inverted crown network in the cases with no free classical communication and free forward classical communication.

• 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 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. (1) 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



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.

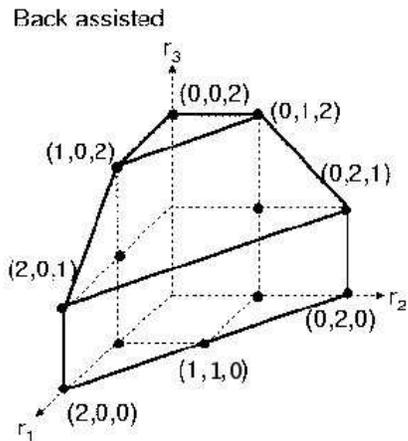


FIG. 14: The achievable rate region for the inverted crown network given free backward or two-way classical communication.

Inner bounds can be obtained from known classical solutions [12], 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, rerouting (with time sharing) is sufficient to generate the entire achievable rate region. It is suggestive that rerouting 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 proofs for some 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 non-trivial 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 n -use protocol).

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

In this class of networks, we impose two 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 some small constant d ($d = 3$ here).

The situation is depicted in Fig. 15. For an arbitrary pos-

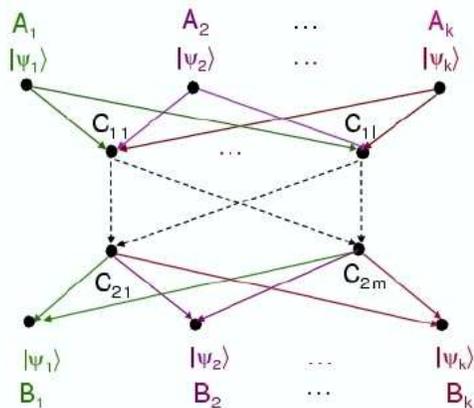


FIG. 15: A general shallow network of distance d .

itive integer k , for each $i = 1, \dots, k$, 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 outgoing channels from the A_i 's to the $C_{1,j}$'s ($j = 1, \dots, l$), from the $C_{1,j}$'s to the $C_{2,j}$'s ($j = 1, \dots, m$), and from the $C_{2,j}$'s to the B_i 's. The absence of a channel is signified by a zero capacity. Note that elements in the sets $\{A_i\}$, $\{C_{1,j}\}$, and $\{C_{2,j}\}$ are defined by their relative distances to the A_i 's and B_i 's. In a general network, these three sets need not be disjoint. For example, a sender A_i may receive information from others and may directly communicate with a specific B_j . The first case holds for A_3 in the inverted crown network in Fig. 9 and the second case holds for both $A_{1,2}$ in the butterfly network in Fig. 1. Such a configuration can easily be handled by assigning multiple vertices to the same party (e.g. A_i is duplicated

as an additional $C_{1,j}$) and connecting the parties with a high capacity channel (from A_i to $C_{1,j}$ in this example). Thus, Fig. 15 still covers these cases. To illustrate the idea, we express the inverted crown network (Fig. 9) in the form of Fig. 15 in Fig. 16.

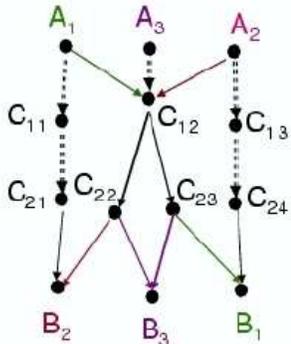


FIG. 16: The inverted crown network in the form of Fig. 15. The dotted channels have unlimited capacities.

Unassisted case:

We show that rerouting is optimal in the case without any classical communication assistance.

Proof:

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 $\{Q_{2ji}\}_j$ received by B_i form an authorized set for $|\psi_i\rangle$. The part of his messages that is used to recover $|\psi_i\rangle$ will not be entangled with the quantum messages sent to other parties. We can also assume, without loss of generality for an optimal protocol, that no other useless messages are sent to B_i . Running the same argument for all B_i 's, the sets $\{Q_{2ji}\}_j$ are independent of one another. In other words, messages related to each $|\psi_i\rangle$ are sent independently by the C_{2j} 's.

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 uncorrelate the messages for the different B_i 's, contradicting our earlier observation.

Thus, the messages $|\psi_i\rangle$ are never jointly coded in any part of the network.

Forward-assisted case:

The analysis is the same as in the unassisted case, but the set of all possible sender-receiver paths may now include opposite running edges, as long as they can be reversed under the general rule described in Sec. II.

Back-assisted and two-way assisted cases:

Even though the receivers are no longer information

sinks, the fact that each has to be able to decode his message implies that other receivers can only *retain* unauthorized shares (though they can help in transmitting them). The argument in the unassisted or the forward-assisted cases holds essentially, giving a unified proof for the optimality of rerouting in shallow networks. However, in the back- and two-way-assisted cases, we have to include possible paths through the receivers, making 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).

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 Σ 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 Σ 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 Σ 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 Σ , 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 Σ 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 Σ 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 $c_{\leftrightarrow}(S_v)$ is the sum of the capacities of all the channels (in both directions) between S_v and R_v , then, $r \leq c_{\leftrightarrow}(S_v)$. 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, $r \leq c_{\leftrightarrow}(S_h)$ 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

$$r \leq \min \left[\min_{S_v} c_{\leftrightarrow}(S_v), \min_{S_h} c_{\leftrightarrow}(S_h) \right]. \quad (2)$$

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 $c_{\leftrightarrow}(S_v)$ and $c_{\leftrightarrow}(S_h)$, 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 $v_{1,2}, h_{1,2}$, and $d_{1,2}$ 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 $v_{1,2}, d_{1,2}$ to $A_{1,2}, B_{1,2}$, and similarly for the horizontal cut. (See the red paths in Fig. 18). The paths through $d_{1,2}$ avoid all other red paths, but those through $h_{1,2}$ and $v_{1,2}$ may share edges. In Fig. 18 we schematically show merged paths running towards $A_{1,2}, B_{1,2}$. Most generally, the red paths may merge and diverge in other locations, but the important features are that they reach $A_{1,2}$ and $B_{1,2}$, and may impose bottlenecks for flows in/out of the individual $A_{1,2}, B_{1,2}$. We label the possible bottlenecks by $a_{1,2}, b_{1,2}$. With a slight abuse of notations, we denote the capacities

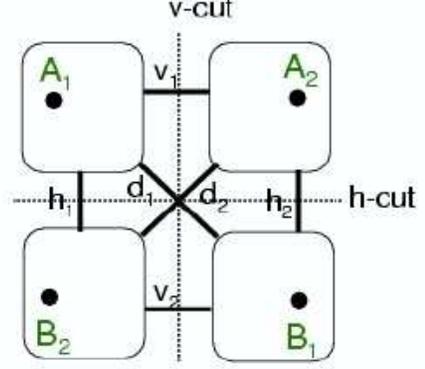


FIG. 17: How the two mincuts partition the vertices into 4 groups

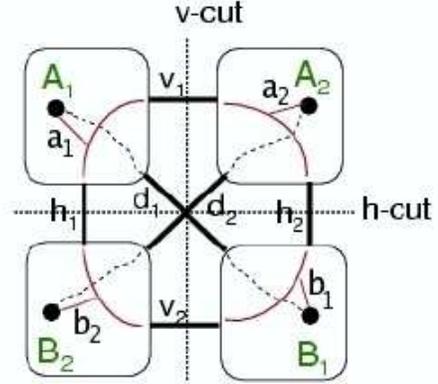


FIG. 18: The structure of an arbitrary quantum network relevant to the 2-pair communication problem with free back communication

of a_1, a_2, \dots, h_2 by the same symbols. Then,

$$r_1 \leq r_1^* := \min(a_1, b_1, v_1 + h_1, v_2 + h_2) + d_1 \quad (3)$$

$$r_2 \leq r_2^* := \min(a_2, b_2, v_1 + h_2, v_2 + h_1) + d_2 \quad (4)$$

$$r \leq r^* := \min(v_1 + v_2, h_1 + h_2) + d_1 + d_2 \quad (5)$$

To achieve the rate pair $(r_1^*, r_2^* - r_1^*)$, 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

$$\gamma_1 : a_1 \rightarrow v_1 \rightarrow h_2 \rightarrow b_1 \quad (6)$$

$$\gamma_2 : a_1 \rightarrow h_1 \rightarrow v_2 \rightarrow b_1 \quad (7)$$

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. (5). **Case (2)** If r_1 is limited by the square, A_1 sends $\min(v_1, h_2)$ qubits through γ_1 and $\min(h_1, v_2)$ qubits through γ_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 completed.

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 communication 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, \dots) is not an achievable point in the classical rate region of a classical network, then, $(2r_1, 2r_2, \dots)$ is not an achievable point in the classical rate region of the corresponding quantum network with arbitrary entanglement 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 [13–16].

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 [17], (also known as localizable entanglement [18]) 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.

$$E_a^\infty(|\psi\rangle, A_1:B_1) = \sup \sum_k p_k E(|\psi_k\rangle) \quad (8)$$

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 $S(\rho) := -\text{Tr}\rho \log \rho$ be the von Neumann entropy of ρ . 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 Σ , we simply write $S(\Sigma)$ for the entanglement between Σ and the rest of the parties. It was found in [13, 15] that

$$E_a^\infty(|\psi\rangle, A_1:B_1) = \min_T \{S(AT), S(BT^c)\} \quad (9)$$

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 [14, 15], 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 $-S(T^c|B_1)$.

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 as-

sisted scenarios. We obtained a general statement for the optimality of rerouting in shallow networks 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. IVD (outer-bounding the entanglement assisted classical rate points in quantum networks), and the optimality of rerouting in networks with larger depth.

Acknowledgments

We are indebted to David Bacon for drawing our attention to reference [3] and Daniel Gottesman for discussions on quantum secret sharing and for providing one of our upper bounds. We also thank Andris Ambainis and Rahul Jain for comments on communication complexity. One of us thanks 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 Council's "QIP IRC", and a University of Bristol Resesarch Fellowship.

-
- [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] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum network coding," 2006, quant-ph/0601088.
- [3] Y. Shi and E. Soljanin, "On multicast in quantum networks," in *Proceedings of the 40th Annual Conference on Information Sciences and Systems (CISS)*, 2006.
- [4] 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.
- [5] 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.
- [6] L. R. Ford, Jr. and D. R. Fulkerson, *Flows in networks*, Princeton University Press, 1962.
- [7] D. Gottesman, "On the theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, pp. 042311, 2000, quant-ph/9910067.
- [8] 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.
- [9] 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.
- [10] 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)].
- [11] 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.
- [12] 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.
- [13] J. A. Smolin, F. Verstraete, and A. Winter, "En-

- tanglement of assistance and multipartite state distillation,” *Phys. Rev. A*, vol. 72, pp. 052317, 2005, quant-ph/0505038.
- [14] M. Horodecki, J. Oppenheim, and A. Winter, “Partial quantum information,” quant-ph/0505062, 2005.
- [15] M. Horodecki, J. Oppenheim, and A. Winter, “Quantum state merging and negative information,” quant-ph/0512247.
- [16] B. Fortescue and H.-K. Lo, “Random bipartite entanglement from w and w -like states,” quant-ph/0607126, 2006.
- [17] D. P. DiVincenzo, C. A. Fuchs, H. Mabuchi, J. A. Smolin, A. Thapliyal, and A. Uhlmann, “Entanglement of assistance,” in *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications, Lecture Notes in Computer Science*. 1998, vol. 1509, Springer-Verlag, quant-ph/9803033.
- [18] M. Popp, F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, “Localizable entanglement,” *Phys. Rev. A*, vol. 71, pp. 042306, 2005, quant-ph/0411123.