

# Perfect Quantum Network Communication Protocol Based on Classical Network Coding

Hirotsada Kobayashi<sup>\*†</sup>   François Le Gall<sup>†</sup>   Harumichi Nishimura<sup>‡</sup>   Martin Rötteler<sup>§</sup>

<sup>\*</sup>Principles of Informatics Research Division  
National Institute of Informatics, Tokyo, Japan

<sup>†</sup>Quantum Computation and Information Project  
Solution Oriented Research for Science and Technology  
Japan Science and Technology Agency, Tokyo, Japan

<sup>‡</sup>Department of Mathematics and Information Sciences  
Graduate School of Science  
Osaka Prefecture University, Sakai, Osaka, Japan

<sup>§</sup>NEC Laboratories America, Inc., Princeton, NJ, USA

8 February 2009

## Abstract

This paper considers a problem of quantum communication between parties that are connected through a network of quantum channels. The model in this paper assumes that there is no prior entanglement shared among any of the parties, but that classical communication is free. The task is to perfectly transfer an unknown quantum state from a source subsystem to a target subsystem, where both source and target are formed by ordered sets of some of the nodes. It is proved that a lower bound of the rate at which this quantum communication task is possible is given by the classical min-cut max-flow theorem of network coding, where the capacities in question are the quantum capacities of the edges of the network.

# 1 Introduction

Consider a communication network consisting of a set  $V$  of several nodes, each of which can hold a small number of qubits and which have no prior entanglement among them. Furthermore, these nodes are connected via a set  $E$  of edges which correspond to quantum communication channels, each of a certain capacity. Let  $G = (V, E)$  be the weighted graph corresponding to this network. Consider the following communication problem: given a set  $S \subseteq V$  of source nodes in the network which all together hold a quantum state  $\rho_S$  and a set of target nodes  $T \subseteq V$  of nodes to which the quantum state is supposed to be sent, where  $|S| \leq |T|$ , the task is to devise a communication protocol that, for any selected subset  $T_0 \subseteq T$  with  $|T_0| = |S|$ , transmits the state  $\rho_S$  through the network such that after the transmission the state of the system corresponding to  $T_0$  is equal to  $\rho_S$  and for any particular ordering of the elements of  $T_0$ .

Clearly, this task depends on the particular properties of the network and it might or might not be possible to achieve this task for the given  $G$ ,  $S$ , and  $T$ . A trivial case where it is impossible to transmit any state perfectly is when  $S$  and  $T$  are disconnected, i. e., there is no quantum communication path between any node of  $S$  and any node of  $T$ . Another trivial case where it is possible to transmit any state perfectly is when each node in  $S$  is directly connected with each node in  $T$ . We shall be concerned with cases in between these two extremes, where the actual network topology given by  $G$  does not allow disjoint paths between the qubits in  $S$  and the qubits in  $T$ , but we nevertheless want to achieve perfect state transfer via quantum teleportation [2]. If perfect state transfer is possible, we also want to achieve it with as few uses of the network as possible.

If  $G$  is a classical network, a celebrated result of network coding is the min-cut max-flow theorem for network information flow [1, 9, 11] which states that perfect transfer from  $S$  to  $T$  at rate  $h$  is possible whenever for each  $t \in T$  the max-flow between  $\sigma$  and  $t$  is at least  $h$ . Here  $\sigma$  is a special source node  $\sigma \notin S$  from which the input information is supposed to originate and is passed to  $S$ . This is the so-called multi-cast model for which optimal network coding is linear [11] and can be constructed in polynomial time [8]. This is in contrast to the general network model in which linear coding is not enough [3].

The strategy this paper presents to achieve perfect quantum teleportation through the quantum network  $G$  is very simple and works whenever the associated classical multi-casting task is feasible. It consists of five steps: (i) First, a state  $|0\rangle + |1\rangle$  (normalization omitted) is created at each node  $s_i \in S$ ,  $1 \leq i \leq |S|$ . (ii) Next, a classical linear network coding protocol for  $G$ ,  $S$ ,  $T$  is translated into a sequence of Clifford operations to be applied at each node of the network. It is proved that the states can be sent through the network in such a way that the final state is given by  $|S|$  cat states each of the form  $|0\rangle_{S_i}|0\rangle_{T_{1,i}} \cdots |0\rangle_{T_{|T|,i}} + |1\rangle_{S_i}|1\rangle_{T_{1,i}} \cdots |1\rangle_{T_{|T|,i}}$ , albeit some of the phases in this state might be incorrect. Here, for each  $1 \leq i \leq |S|$ ,  $S_i$  is the single-qubit register possessed by the node  $s_i$  and each  $T_{j,i}$  is the single-qubit register possessed by the node  $t_j \in T$ ,  $1 \leq j \leq |T|$ . (iii) Now the classical information obtained by measuring internal network qubits in the Hadamard basis is sent to one dedicated output node  $t_1 \in T$ . Using this information, the phase errors are fixed and indeed  $|S|$  perfect cat states are generated. (iv) After the selection of  $T_0 \subseteq T$  is revealed, the cat states are converted into  $|S|$  EPR pairs shared between the corresponding node pairs. For this purpose, it is again necessary to measure in the Hadamard basis and exchange the obtained classical information. (v) Finally, using the EPR pairs the state  $\rho_S$  over  $S$  is teleported to the target nodes in  $T_0$ .

It is perhaps interesting to note that deciding what the target nodes  $T_0$  are (and in particular their order!) to which the state is teleported can be done *after* the quantum network has been used. At this point the only required communication is purely classical.

**Related work** It should be noted that, prior to this work, several papers studied the problem of sending quantum states using the idea of network coding, that is, allowing any coding at intermediate nodes of the network. Hayashi, Iwama, Nishimura, Raymond, and Yamashita [7] showed that network coding (without free classical communication) does not give us any benefit for perfect transmission on the butterfly network, a famous network with two source-target pairs. Leung, Oppenheim, and Winter [10] showed that this negative result can be general-

ized to several types of networks even if the transmission is allowed to be asymptotically perfect. Also, they studied several variants of situations including the one where free classical communication is allowed. On the contrary, Hayashi [6] showed that perfect transmission of two source states on the butterfly network can be efficiently done by network coding if the sources have prior entanglement and each link has a capacity of one qubit or two classical bits. It should be noted that all of the above results focus on the (multiple-source) uni-cast model, a well-studied network coding model, while the model discussed in this paper is close to the multi-cast model. The quantum network coding for the multi-cast model was previously studied by Shi and Soljanin [13]. In their model, however, the source was restricted to the product of copies of a state, and hence in fact they could use only source coding for perfect transmission, instead of coding at intermediate nodes.

## 2 Preliminaries

### 2.1 Quantum Information

Quantum states are normalized vectors in a complex Hilbert space  $\mathcal{H} = \mathbb{C}^d$ . The simplest case of  $\mathcal{H} = \mathbb{C}^2$  is of particular importance, and a system supporting such a state space is called a *qubit* (*quantum bit*). This paper mainly treats the case of two-dimensional quantum systems, but the results in this paper can be generalized to any  $d$ -dimensional systems. Notice that even if the quantum information to be transmitted is originally given by qubits, higher-dimensional systems may be necessary in the coding schemes. Intuitively, this is because the protocols to be presented are based on classical network coding which itself might require higher alphabets for the coding, even if the original information is binary. These points will be discussed further in Theorem 5.

The orthonormal basis states of a qubit are written as  $|0\rangle$  and  $|1\rangle$ , and the general state of a qubit is given by  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ , where  $\alpha, \beta \in \mathbb{C}$  and  $|\alpha|^2 + |\beta|^2 = 1$ . If both  $\alpha$  and  $\beta$  are non-zero, the state  $|\phi\rangle$  is a so-called superposition of  $|0\rangle$  and  $|1\rangle$  with amplitudes  $\alpha$  and  $\beta$ . For a  $d$ -dimensional system, we label the orthonormal basis states by the elements of some alphabet of size  $d$ , e. g., the numbers  $\{0, 1, \dots, d-1\}$  or the elements of a finite field, if  $d$  is a prime power. A normalized vector in  $\mathbb{C}^d$  is called a *qudit*, and is written as  $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$ , where  $\alpha_i \in \mathbb{C}$  and  $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$ . *Quantum registers* consist of several qudits. The basis states of a quantum register of  $n$  qudits are tensor products of the basis states of the single qudits. The following notation is used:

$$|x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle = |x_1\rangle|x_2\rangle \dots |x_n\rangle = |x_1, x_2, \dots, x_n\rangle,$$

where  $x_1, \dots, x_n$  are elements of  $\{0, 1, \dots, d-1\}$ . From now we focus on the case where  $d = 2$ . A general state of a quantum register of  $n$  qubits is a normalized vector in  $\mathcal{H} = (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ , given by  $|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$ , where  $\alpha_{\mathbf{x}} \in \mathbb{C}$  and  $\sum_{\mathbf{x} \in \mathbb{F}_2^n} |\alpha_{\mathbf{x}}|^2 = 1$ . For two vectors  $\mathbf{x}$  and  $\mathbf{y}$  in  $\mathbb{F}_2^n$ , let  $\mathbf{x} \cdot \mathbf{y}$  denote the usual inner product. When writing states of quantum registers, normalization factors may be omitted. We next discuss some basic elementary quantum operations that can be used to manipulate the content of quantum registers. This is all standard, see for example [12].

**Definition 1** (Elementary Clifford Operations). The following four operations are called elementary Clifford operations:

$$\begin{aligned} \sigma_X &:= \sum_{x \in \mathbb{F}_2} |x+1\rangle\langle x|, \\ \sigma_Z &:= \sum_{x \in \mathbb{F}_2} (-1)^x |x\rangle\langle x|, \\ H &:= \frac{1}{\sqrt{2}} \sum_{x, y \in \mathbb{F}_2} (-1)^{xy} |y\rangle\langle x|, \\ \text{CNOT}^{(A, B)} &:= \sum_{x, y \in \mathbb{F}_2} |x\rangle\langle x|_A \otimes |x+y\rangle\langle y|_B. \end{aligned}$$

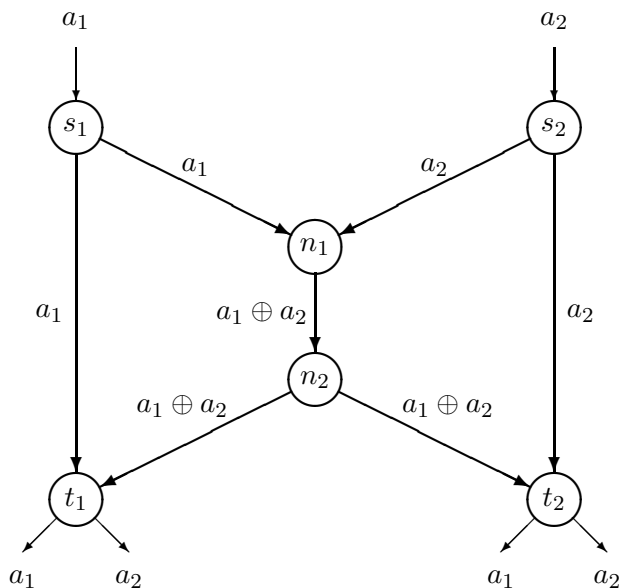


Figure 1: The butterfly network and a classical linear coding protocol. The node  $s_1$  (resp.  $s_2$ ) has for input a bit  $a_1$  (resp.  $a_2$ ). The task is to send  $a_1$  and  $a_2$  to both  $t_1$  and  $t_2$ . The capacity of each edge is assumed to be one bit. Our convention here is that  $s_1$  (resp.  $s_2$ ) receives  $a_1$  (resp.  $a_2$ ) through a virtual incoming edge, and that  $t_1$  (resp.  $t_2$ ) has two virtual outgoing edges through which it should output  $a_1$  and  $a_2$ , respectively.

Here, when writing  $(-1)^x$  for  $x \in \mathbb{F}_2$ , we identify  $\mathbb{F}_2$  and  $\mathbb{Z}/2\mathbb{Z}$ , the integers modulo 2. The operation  $\sigma_X$  corresponds to the addition of the identity element. The operation  $\sigma_Z$  has no direct classical analogue and changes the phases of the basis states. The operator  $H$  is called the *Hadamard operator*, and CNOT the *controlled-NOT operator*.

Finally, let

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

and for convenience, we say that measuring a qubit in the basis  $\{|+\rangle, |-\rangle\}$  (the *Hadamard basis*) gives a bit  $b$ , where  $b = 0$  if  $|+\rangle$  is measured, and  $b = 1$  if  $|-\rangle$  is measured.

## 2.2 Convention on Classical Multi-Cast

The key result of this paper is a quantum simulation of any classical linear network coding scheme in the multi-cast model. Here we use the standard definition of classical linear network coding (see [11, 8]). For convenience, the following simple but very useful convention is assumed when describing a classical multi-cast (linear) protocol.

Each source  $s_i \in S$  is supposed to have a “virtual” incoming edge from which it receives its input  $a_i$ . Also, each target  $t_j \in T$  is supposed to have  $|S|$  “virtual” outgoing edges, where  $a_i$  must be output through the  $i$ th virtual outgoing edge, for  $1 \leq i \leq |S|$ . In this way, the source and target nodes perform a linear-coding operation on their inputs, and this convention enables us to ignore the distinction between source/target nodes and internal nodes. These conventions are illustrated in Figure 1 on the well-known coding protocol over the butterfly network.

### 3 Sending Quantum States through Networks

First, the following lemma is proved to describe the effect of measuring in the Hadamard basis.

**Lemma 2.** Consider a system of  $n$  qubits and a partition of  $\{1, \dots, n\}$  into two disjoint subsets  $A$  and  $B$ . Let  $|\psi_{(A,B)}\rangle$  be a joint state given by

$$|\psi_{(A,B)}\rangle = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \alpha_{\mathbf{x}} |f(\mathbf{x})\rangle_A |g(\mathbf{x})\rangle_B,$$

where  $\alpha_{\mathbf{x}} \in \mathbb{C}$ ,  $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{|A|}$ ,  $g: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{|B|}$ , and registers  $A$  and  $B$  correspond to the qubits belonging to  $A$  and  $B$ , respectively. Then the state in  $A$  obtained from  $|\psi_{(A,B)}\rangle$  by measuring each qubit in  $B$  in the  $\{|+\rangle, |-\rangle\}$  basis has the form

$$|\psi_A\rangle = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{y}_0 \cdot g(\mathbf{x})} \alpha_{\mathbf{x}} |f(\mathbf{x})\rangle,$$

where  $\mathbf{y}_0 \in \mathbb{F}_2^{|B|}$  is a (in general random) vector of measurement results.

*Proof.* Applying the Hadamard transform  $H^{\otimes |B|} = \frac{1}{\sqrt{2^{|B|}}} \sum_{\mathbf{y}, \mathbf{z} \in \mathbb{F}_2^{|B|}} (-1)^{\mathbf{y} \cdot \mathbf{z}} |\mathbf{y}\rangle \langle \mathbf{z}|$  to the qubits in  $B$  gives the new state

$$(I_A \otimes H^{\otimes |B|}) |\psi_{(A,B)}\rangle = \frac{1}{\sqrt{2^{|B|}}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} \alpha_{\mathbf{x}} |f(\mathbf{x})\rangle \sum_{\mathbf{y} \in \mathbb{F}_2^{|B|}} (-1)^{\mathbf{y} \cdot g(\mathbf{x})} |\mathbf{y}\rangle.$$

Measuring the qubits in  $B$  in the computational basis  $\{|0\rangle, |1\rangle\}$  gives a certain result  $\mathbf{y}_0 \in \mathbb{F}_2^{|B|}$  and the state collapses to the state claimed in the lemma.  $\square$

The next lemma shows the way of fixing phase errors that have happened to a state, provided that the phase errors are of a benign type.

**Lemma 3.** Let  $|\psi\rangle$  be a state of the form

$$|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{L(\mathbf{x})} \alpha_{\mathbf{x}} |\mathbf{x}\rangle,$$

where  $L$  is a known linear function. Then by applying local  $\sigma_Z$  operations,  $|\psi\rangle$  can be mapped to  $\sum_{\mathbf{x} \in \mathbb{F}_2^n} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$ .

*Proof.* Note that if  $L: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  is linear, then  $L$  maps  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_2^n$  to  $L(\mathbf{x}) = \mathbf{b} \cdot \mathbf{x}$  for some fixed vector  $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_2^n$ . Further note that since  $L$  is known, the vector  $\mathbf{b}$  is also known, and therefore the operation  $\bigotimes_{i=1}^n \sigma_Z^{b_i}$  can be applied to the state, which has the effect of canceling out the phases.  $\square$

Next, we present three types of operations necessary for the network communication protocol: *quantum coding operations*, *quantum fan-out operations*, and *measurements*. Quantum fan-out operations can be formally viewed as quantum coding operations, but we deal with them separately since no coding is actually performed. All the operations required for the protocol are elementary Clifford operations and a supply of ancilla states that are initialized to  $|0\rangle$ .

**Quantum coding operations** Classical network coding protocols in general perform coding at intermediate nodes.

For simplicity, consider the case where each edge has capacity one. It is straightforward to generalize this to the case where the capacities are positive integers. Consider a node  $v \in V$  with  $m$ -fan-in and  $n$ -fan-out performing classical linear coding. The node  $v$  has then  $m$  incoming edges, each one conveying an element of  $\mathbb{F}_2$  and labeled with a vector  $\mathbf{v}_i \in \mathbb{F}_2^{|S|}$ , for  $i = 1, \dots, m$ . The outputs of the node are  $n$  elements  $w_j \in \mathbb{F}_2$  for  $j = 1, \dots, n$  that are computed as suitable linear combinations  $w_j = \sum_{i=1}^m \gamma_{i,j} \sum_{k=1}^{|S|} v_{i,k}$ , where  $v_{i,k}$

denotes the  $k$ th entry of  $\mathbf{v}_i$ , and are further propagated through the network. Here  $\gamma_{i,j}$  are fixed elements of  $\mathbb{F}_2$ . The quantum coding operation associated with this classical operation is as follows: attach  $n$  new ancilla qubits initialized to  $|0\rangle$  and, for each  $i = 1, \dots, m$  and  $j = 1, \dots, n$ , apply a controlled-NOT operation if and only if  $\gamma_{i,j} = 1$ , using the  $i$ th incoming qubit as control and the  $j$ th ancilla as target. The effect of this is to map, for any  $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{F}_2^m$ , the basis state  $|\mathbf{x}\rangle \otimes |0\rangle^{\otimes n}$  to  $|\mathbf{x}, z_1, \dots, z_n\rangle$  where  $z_j = \sum_{i=1}^m \gamma_{i,j} x_i$ . Next, the  $n$  ancilla qubits are sent along on the  $n$  outgoing edges and all the incoming qubits are retained at the node.

**Fan-out operations** The  $n$ -fan-out operation is the special case of the quantum coding operations with one-fan-in and  $n$ -fan-out, such that  $\gamma_{1,j} = 1$  for each  $j = 1, \dots, n$ . For a given basis vector  $|x\rangle$  on one qubit (with  $x \in \mathbb{F}_2$ ), we attach  $n$  further ancillas initialized to  $|0\rangle$  and apply a sequence of  $n$  controlled-NOT operations using the given qubit as control and each ancilla as target. The effect on the state is given by  $|x\rangle|0\rangle^{\otimes n} \mapsto |x\rangle^{\otimes(n+1)}$ .

**Measurements** They are used to make the superfluous qubits (kept at each node) collapse, by measuring them in the Hadamard basis. More details will be given below in the proof of Theorem 4.

Putting it all together, we have the following result:

**Theorem 4.** *Let  $G = (V, E)$  be a quantum network with a subset  $S \subseteq V$  of source nodes and a subset  $T \subseteq V$  of target nodes, where each edge  $e \in E$  has an integral weight that describes its quantum capacity. Assume that classical linear network coding over  $\mathbb{F}_2$  is possible in the multi-cast model from  $S$  to  $T$ . Then perfect quantum teleportation from  $S$  to any ordered subset  $T_0 \subseteq T$  with  $|T_0| = |S|$  is possible.*

*Proof.* First, each node  $s \in S$  creates the state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . Next, we simulate a classical coding scheme for the associated multi-cast task in such a way that the fan-out operation is applied whenever a broadcast is performed in the associated classical protocol and the quantum coding operation is applied whenever a classical coding operation is applied in the associated classical protocol. Remember that, from the convention of Subsection 2.2, the sources and target nodes are not necessary to be treated as special nodes.

Because of the classical network coding property that each output can perfectly recover all the inputs  $a_1, \dots, a_{|S|}$ , we obtain the following state after the sequence of quantum coding and fan-out operations above:

$$\frac{1}{\sqrt{2^{|S|}}} \sum_{a_1, \dots, a_{|S|} \in \mathbb{F}_2} \underbrace{|a_1, \dots, a_{|S|}\rangle}_S \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_1} \otimes \dots \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_{|T|}} \otimes |f_1(a_1, \dots, a_{|S|})\rangle \otimes \dots \otimes |f_m(a_1, \dots, a_{|S|})\rangle$$

for some functions  $f_i: \mathbb{F}_2^{|S|} \rightarrow \mathbb{F}_2$ ,  $1 \leq i \leq m$ , where the first  $|S|$  qubits are owned by the source nodes in  $S$ , the next  $|T| \cdot |S|$  qubits are owned by the nodes  $t_1, \dots, t_{|T|}$  in  $T$ , and the last  $m$  qubits are owned by several nodes in the network. Note that by induction all functions  $f_i$  are linear. By Lemma 2, the first  $(|T| + 1) \cdot |S|$  qubits must form the following state after measuring all the last  $m$  qubits in the Hadamard basis:

$$\frac{1}{\sqrt{2^{|S|}}} \sum_{a_1, \dots, a_{|S|} \in \mathbb{F}_2} (-1)^{L(a_1, \dots, a_{|S|})} \underbrace{|a_1, \dots, a_{|S|}\rangle}_S \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_1} \otimes \dots \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_{|T|}},$$

where  $L: \mathbb{F}_2^{|S|} \rightarrow \mathbb{Z}/2\mathbb{Z}$  is a linear function determined by the measurement results. Now, the information about  $L$  is propagated through (free) classical communication to one of the target nodes, without loss of generality the first target node. Using Lemma 3, node  $t_1$  can apply a local unitary operation that fixes the phase and leads to the state

$$\frac{1}{\sqrt{2^{|S|}}} \sum_{a_1, \dots, a_{|S|} \in \mathbb{F}_2} \underbrace{|a_1, \dots, a_{|S|}\rangle}_S \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_1} \otimes \dots \otimes \underbrace{|a_1, \dots, a_{|S|}\rangle}_{t_{|T|}}.$$

This state is a collection of  $|S|$  cat states, each of  $|T| + 1$  qubits, which are shared in such a way that each source node has one qubit and each target node has one qubit.

When a subset  $T_0 \subseteq T$  with  $|T_0| = |S|$  and a permutation  $\pi$  over the  $|S|$  elements of  $T_0$  are revealed, the  $|T|$  parties run a protocol to prepare  $|S|$  EPR pairs from the  $|S|$  cat states. For this, again Lemmas 2 and 3 can be used to achieve the preparations of the EPR pairs using local measurements and classical communication only. Finally, the state  $\rho_S$  is teleported [2] to the qubits in  $T_0$  with the particular ordering given by  $\pi$ .  $\square$

In fact, Theorem 4 can be generalized to the following statement.

**Theorem 5.** *Let  $G = (V, E)$  be a quantum network with a subset  $S \subseteq V$  of source nodes and a subset  $T \subseteq V$  of target nodes, where each edge  $e \in E$  has an integral weight that describes its quantum capacity. Assume that classical network coding is possible in the multi-cast model from  $S$  to  $T$ . Then perfect quantum teleportation from  $S$  to any ordered subset  $T_0 \subseteq T$  with  $|T_0| = |S|$  is possible.*

*Proof (sketch).* It is known [11, 8] that, if classical multi-cast is feasible on a network, a linear coding scheme exists over some large enough finite field. The techniques developed in this section generalize to any finite field as follows. Suppose that the finite field has size  $q$ . Each source node starts with the  $q$ -dimensional quantum state  $\frac{1}{\sqrt{q}} \sum_{x \in \mathbb{F}_q} |x\rangle$ . The node-by-node simulation of Theorem 4 is then performed in a similar way. To deal with the measurements, we need a simple generalization of Lemmas 2 and 3 to  $q$ -dimensional quantum systems. This can be done using the concept of  $q$ -ary Clifford operations (see Refs. [4, 5] for a description of these operations in the framework of quantum error-correcting codes).  $\square$

## 4 Example: The Butterfly Graph

This section illustrates the techniques developed in the previous section with the example of the quantum network shown in Figure 2. The topology of this network is the same as the classical butterfly network (see Figure 1) with the main difference that each edge represents a quantum channel of capacity one. Recall that in our model classical communication is free. The task is to send a quantum state from the source ( $s_1$  and  $s_2$ ) to the target ( $t_1$  and  $t_2$ ). In this example, there are two internal nodes  $n_1$  and  $n_2$ . The difficulty is that the order of the target qubits are part of the input, i. e., we have to realize either the association corresponding to the pairs  $(s_1, t_1)$  and  $(s_2, t_2)$  or the association corresponding to the pairs  $(s_1, t_2)$  and  $(s_2, t_1)$ . The former corresponds to the identity permutation and the latter to the swap, if we think of the qubits in some fixed order.

This task can be achieved perfectly, i. e., with fidelity one, using the protocol given in Theorem 4. We give the explicit details for this example of the butterfly network. More precisely, we describe how the protocol simulates the classical linear coding scheme for multi-casting presented in Figure 1. The protocol applies the fan-out operations at nodes  $s_1$ ,  $s_2$ , and  $n_2$ , while performs appropriate quantum coding operations at nodes  $n_1$ ,  $t_1$ , and  $t_2$ . Hereafter, all the registers are assumed to be single-qubit registers each initialized to  $|0\rangle$ .

First, the source node  $s_1$  (resp.  $s_2$ ) prepares a register  $S'_1$  (resp.  $S'_2$ ) and applies an Hadamard operator to it. The quantum state after this step is described as

$$\frac{1}{2}(|0\rangle + |1\rangle)_{S'_1} \otimes (|0\rangle + |1\rangle)_{S'_2} = \frac{1}{2}(|0\rangle_{S'_1}|0\rangle_{S'_2} + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle).$$

Then  $s_1$  (resp.  $s_2$ ) further introduces two registers  $R_1$  and  $R_2$  (resp.  $R_3$  and  $R_4$ ), and applies the operators  $\text{CNOT}^{(S'_1, R_1)}$  and  $\text{CNOT}^{(S'_1, R_2)}$  (resp.  $\text{CNOT}^{(S'_2, R_3)}$  and  $\text{CNOT}^{(S'_2, R_4)}$ ). The resulting state is

$$\frac{1}{2}(|\mathbf{0}\rangle_{(S'_1, R_1, R_2)}|\mathbf{0}\rangle_{(S'_2, R_3, R_4)} + |\mathbf{0}\rangle|\mathbf{1}\rangle + |\mathbf{1}\rangle|\mathbf{0}\rangle + |\mathbf{1}\rangle|\mathbf{1}\rangle).$$

Hereafter, let  $\mathbf{0}$  and  $\mathbf{1}$  denote strings of all-zero and all-one, respectively, of appropriate length (three here). The registers  $R_1$  and  $R_2$  are sent to  $t_1$  and  $n_1$ , respectively, while  $R_3$  and  $R_4$  are sent to  $t_2$  and  $n_1$ , respectively.

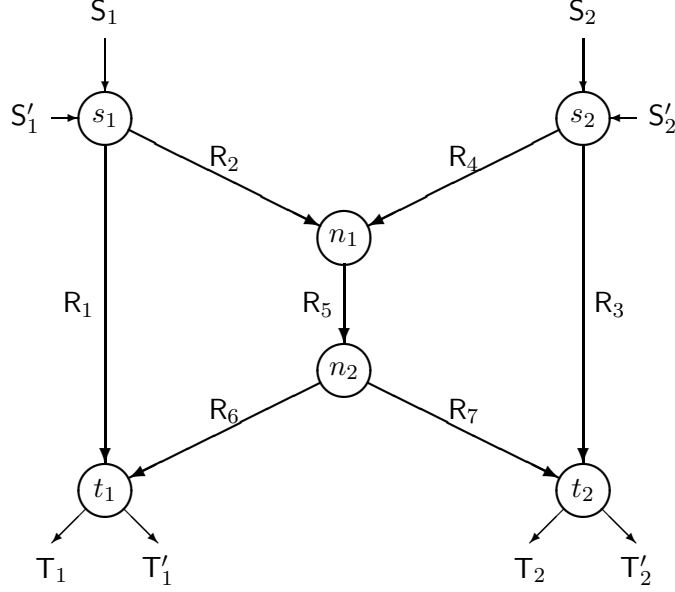


Figure 2: Example for perfect quantum state transfer through a quantum network. This example is based on the well-known butterfly network. Each edge has quantum capacity one. The task is to send a given input quantum state  $\rho_S$  in  $(S_1, S_2)$  to either  $(T_1, T_2)$  or  $(T_2, T_1)$  in this order of registers. Here, the quantum register  $S_1$  (resp.  $S_2$ ) is possessed by the source node  $s_1$  (resp.  $s_2$ ), while the quantum register  $T_1$  (resp.  $T_2$ ) is possessed by the target node  $t_1$  (resp.  $t_2$ ). The protocol given in Theorem 4 realizes perfect quantum teleportation of  $\rho_S$  for both possible orders of the target registers. Each  $R_i$  indicates the quantum register to be sent along the corresponding edge in the protocol. The quantum registers  $S'_1, S'_2, T'_1,$  and  $T'_2$  possessed by the source nodes  $s_1$  and  $s_2$  and the target nodes  $t_1$  and  $t_2$ , respectively, are used at the stage of sharing the cat states. Overall, a total of seven qubits of communication are necessary to transfer the state from the source to the target registers.

The node  $n_1$  then prepares a new register  $R_5$ , and applies the operators  $\text{CNOT}^{(R_2, R_5)}$  and  $\text{CNOT}^{(R_4, R_5)}$ . The resulting state is

$$\frac{1}{2}(|\mathbf{0}\rangle_{(S'_1, R_1, R_2)}|\mathbf{0}\rangle_{(S'_2, R_3, R_4)}|\mathbf{0}\rangle_{R_5} + |\mathbf{0}\rangle|\mathbf{1}\rangle|\mathbf{1}\rangle + |\mathbf{1}\rangle|\mathbf{0}\rangle|\mathbf{1}\rangle + |\mathbf{1}\rangle|\mathbf{1}\rangle|\mathbf{0}\rangle),$$

and the register  $R_5$  is sent to  $n_2$ .

The node  $n_2$  then performs a quantum fan-out, i. e., prepares two registers  $R_6$  and  $R_7$  and applies the operators  $\text{CNOT}^{(R_5, R_6)}$  and  $\text{CNOT}^{(R_5, R_7)}$ . The resulting state is

$$\frac{1}{2}(|\mathbf{0}\rangle_{(S'_1, R_1, R_2)}|\mathbf{0}\rangle_{(S'_2, R_3, R_4)}|\mathbf{0}\rangle_{(R_5, R_6, R_7)} + |\mathbf{0}\rangle|\mathbf{1}\rangle|\mathbf{1}\rangle + |\mathbf{1}\rangle|\mathbf{0}\rangle|\mathbf{1}\rangle + |\mathbf{1}\rangle|\mathbf{1}\rangle|\mathbf{0}\rangle),$$

and the registers  $R_6$  and  $R_7$  are sent to  $t_1$  and  $t_2$ , respectively.

At this point, the node  $s_1$  has the register  $S'_1$ ;  $s_2$  has  $S'_2$ ;  $n_1$  has  $R_2$  and  $R_4$ ;  $n_2$  has  $R_5$ ;  $t_1$  has  $R_1$  and  $R_6$ ;  $t_2$  has  $R_3$  and  $R_7$ . Finally,  $t_1$  (resp.  $t_2$ ) prepares two registers  $T_1$  and  $T'_1$  (resp.  $T_2$  and  $T'_2$ ), and applies the operators  $\text{CNOT}^{(R_1, T_1)}$ ,  $\text{CNOT}^{(R_1, T'_1)}$  and  $\text{CNOT}^{(R_6, T'_1)}$  (resp.  $\text{CNOT}^{(R_3, T_2)}$ ,  $\text{CNOT}^{(R_3, T'_2)}$  and  $\text{CNOT}^{(R_7, T_2)}$ ). The resulting state is

$$\begin{aligned} & \frac{1}{2}(|\mathbf{0}\rangle_{(S'_1, R_1, R_2)}|\mathbf{0}\rangle_{(S'_2, R_3, R_4)}|\mathbf{0}\rangle_{(R_5, R_6, R_7)}|0, 0\rangle_{(T_1, T'_1)}|0, 0\rangle_{(T_2, T'_2)} \\ & + |\mathbf{0}\rangle|\mathbf{1}\rangle|\mathbf{1}\rangle|0, 1\rangle|0, 1\rangle + |\mathbf{1}\rangle|\mathbf{0}\rangle|\mathbf{1}\rangle|1, 0\rangle|1, 0\rangle + |\mathbf{1}\rangle|\mathbf{1}\rangle|\mathbf{0}\rangle|1, 1\rangle|1, 1\rangle). \end{aligned}$$



Now every qubit in  $(R_1, R_2, R_3, R_4, R_5, R_6, R_7)$  is measured in the Hadamard basis. The outcome  $\mathbf{y}_0 \in \{0, 1\}^7$  is then communicated to the target node  $t_1$ . Using the information of  $\mathbf{y}_0$ , the state can be mapped to

$$\frac{1}{2}(|0\rangle_{S'_1}|0\rangle_{S'_2}|0,0\rangle_{(T_1,T'_1)}|0,0\rangle_{(T_2,T'_2)} + |0\rangle|1\rangle|0,1\rangle|0,1\rangle + |1\rangle|0\rangle|1,0\rangle|1,0\rangle + |1\rangle|1\rangle|1,1\rangle|1,1\rangle) \otimes (H^{\otimes 7}|\mathbf{y}_0\rangle_{(R_1,R_2,R_3,R_4,R_5,R_6,R_7)})$$

by a local operation at  $t_1$ .

The state in  $(R_1, R_2, R_3, R_4, R_5, R_6, R_7)$  is then discarded. Observe that the state in  $(S'_1, T_1, T_2, S'_2, T'_1, T'_2)$  in this order of the registers forms two cat states

$$\frac{1}{2}(|0,0,0\rangle + |1,1,1\rangle)_{(S'_1,T_1,T_2)} \otimes (|0,0,0\rangle + |1,1,1\rangle)_{(S'_2,T'_1,T'_2)}.$$

From these two cat states, two EPR pairs can be created easily either in  $(S'_1, T_1)$  and  $(S'_2, T'_2)$  or in  $(S'_1, T_2)$  and  $(S'_2, T'_1)$ , according to the two possible communication scenarios. For instance, an EPR pair in  $(S'_1, T_2)$  shared by  $s_1$  and  $t_2$  can be created as follows. The node  $t_1$  measures the qubit in  $T_1$  in the Hadamard basis  $\{|+\rangle, |-\rangle\}$  and sends the result  $b \in \{0, 1\}$  of the measurement to  $s_1$ . The node  $s_1$  then applies the operator  $\sigma_Z^b$  to the qubit in  $S'_1$ . It can be checked easily that the remaining two qubits in  $(S'_1, T_2)$  form an EPR pair.

Finally, using these EPR pairs either in  $(S'_1, T_1)$  and  $(S'_2, T'_2)$  or in  $(S'_1, T_2)$  and  $(S'_2, T'_1)$ , the quantum state  $\rho_S$  in  $(S_1, S_2)$  is teleported either to  $(T_1, T'_2)$  or to  $(T_2, T'_1)$  in this order of registers. By appropriately applying swap operators, the state  $\rho_S$  is recovered either in  $(T_1, T_2)$  or in  $(T_2, T_1)$  in this order of registers.

## 5 Conclusions

It has been proved that the problem of teleporting an unknown quantum state through a network can be solved perfectly, i. e., with fidelity one, by efficiently using the idea of network coding. The method presented in this paper allows the state to be teleported for all quantum networks whenever classical linear network coding is possible for the network. Moreover, it only uses Clifford operations and is based on three simple rules that are applied at each node of the network: fan-out operations, quantum coding operations, and measurements.

## Acknowledgements

The authors are grateful to Tsuyoshi Ito for helpful discussions.

## References

- [1] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.
- [2] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.
- [3] Randall Dougherty, Christopher F. Freiling, and Kenneth Zeger. Insufficiency of linear coding in network information flow. *IEEE Transactions on Information Theory*, 51(8):2745–2759, 2005.
- [4] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos, Solitons, & Fractals*, 10(10):1749–1758, 1999.

- [5] Markus Grassl, Martin Rötteler, and Thomas Beth. Efficient quantum circuits for non-qubit quantum error-correcting codes. *International Journal of Foundations of Computer Science*, 14(5):755–776, 2003.
- [6] Masahito Hayashi. Prior entanglement between senders enables perfect quantum network coding with modification. *Physical Review A*, 76(4):040301(R), 2007.
- [7] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Quantum network coding. In *STACS 2007, 24th Annual Symposium on Theoretical Aspects of Computer Science*, volume 4393 of *Lecture Notes in Computer Science*, pages 610–621, 2007.
- [8] Sidharth Jaggi, Peter Sanders, Philip A. Chou, Michelle Effros, Sebastian Egner, Kamal Jain, and Ludo Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory*, 51(6):1973–1982, 2005.
- [9] Ralf Koetter and Muriel Médard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, 2003.
- [10] Debbie Leung, Jonathan Oppenheim, and Andreas Winter. Quantum network communication — the butterfly and beyond. arXiv.org e-Print archive, quant-ph/0608223, 2006.
- [11] Shuo-Yen Robert Li, Raymond W. Yeung, and Ning Cai. Linear network coding. *IEEE Transactions on Information Theory*, 49(2):371–381, 2003.
- [12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [13] Yaoyun Shi and Emina Soljanin. On multicast in quantum networks. In *40th Annual Conference on Information Sciences and Systems*, pages 871–876, 2006.