Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols

HIROTADA KOBAYASHI[1] FRANCOIS LE GALL[2] HARUMICHI NISHIMURA[3] MARTIN RÖTTELER[4]

[1]National Institute of Informatics, Tokyo, Japan; hirotada@nii.ac.jp
[2]The University of Tokyo, Tokyo, Japan; legall@is.s.u-tokyo.ac.jp
[3]Osaka Prefecture University, Japan; hnishimura@mi.s.osakafu-u.ac.jp
[4]NEC Laboratories America, Inc., Princeton, NJ, USA; mroetteler@nec-labs.com

Abstract. The k-pair problem in network coding theory asks to send k messages simultaneously between k source-target pairs over a directed acyclic graph. In a previous paper [ICALP 2009, Part I, pages 622–633] the present authors showed that if a classical k-pair problem is solvable by means of a linear coding scheme, then the quantum k-pair problem over the same graph is also solvable, provided that classical communication can be sent for free between any pair of nodes of the graph. Here we address the main case that remained open in our previous work, namely whether *nonlinear* classical network coding schemes can also give rise to quantum network coding schemes. This question is motivated by the fact that there are networks for which there are no linear solutions to the k-pair problem, whereas nonlinear solutions exist. In the present paper we overcome the limitation to linear protocols and describe a new communication protocol for perfect quantum network coding that improves over the previous one as follows: (i) the new protocol does not put any condition on the underlying classical coding scheme, that is, it can simulate nonlinear communication protocols as well, and (ii) the amount of classical communication sent in the protocol is significantly reduced.

1 Introduction

The idea of *network coding*, proposed in the seminal paper by Ahlswede, Cai, Li and Yeung [1], opened up a new communication-efficient way of sending information through networks. The key idea is to allow coding and replication of information locally at any intermediate node of the network. For instance, this allows one to send two bits simultaneously between two source-target pairs over several networks for which the same task cannot be solved by routing. A simple, yet instructive, example is the butterfly network described in Fig. 1. We refer to Refs. [4, 8, 18, 19] for extensive treatments of the topic of classical network coding.

In quantum information processing, it is often desirable to manipulate quantum states by applying local operations only, rather than applying global operations that require to send quantum information between different places. This in particular applies to the situation of communication tasks involving quantum information where it is quite natural to assume that whenever quantum information is sent over a channel, there is a high chance that it will be corrupted, whereas classical information can be sent very reliably. In this context a natural question is whether the concept of network coding can be applied to quantum networks in order to reduce the amount of *quantum communication*. There have been several studies working on "quantum" network coding [6, 7, 12, 16]. These papers deal with the challenge to send quantum information over a network as well as possible, a task that is greatly hampered by the fact due to the no-cloning theorem that unknown quantum information cannot be replicated. A natural target problem that has crystallized out from the prior works [6, 7, 12] as being at the core of the issue is the following quantum k-pair problem: Given a directed acyclic graph G with k source-target pairs (where we assume all the edges, which represent quantum channels, have unit capacities), is there a way of sending k quantum messages between the k pairs? Note that the classical k-pair problem, in which the channels and messages

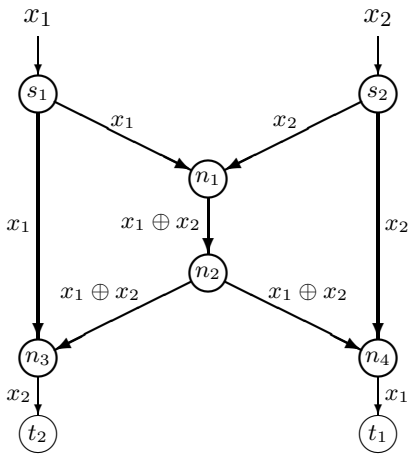

Figure 1: The butterfly network and a classical linear coding protocol. The node s_1 (resp. s_2) has for input a bit x_1 (resp. x_2). The task is to send x_1 to t_1 and x_2 to t_2. The capacity of each edge is assumed to be one bit.

are classical, is one of the most important network coding problems (for instance, see Refs. [3, 5, 9, 13, 17]). The butterfly network described in Fig. 1 is an instance of the two-pair problem.

Unfortunately, in the early stage of studying quantum network coding it was shown that there exist networks for which the classical k-pair problem is solvable but the quantum k-pair problem is not perfectly solvable [6, 7, 12]. For instance, two quantum states cannot be sent simultaneously and perfectly (i.e., with fidelity one) between the two source-target pairs in the butterfly network. However, the situation changes dramatically if classical communication is allowed freely (which seems to be reasonable since classical communication is much cheaper than quantum communication and does not increase the amount of entanglement of the system). Indeed, the authors of the present paper established that any linear classical network coding protocol over $\mathbb{F}_2$ (i. e., a scheme where the encoding operation at each node is a linear function of its inputs) for the multi-cast problem can be turned into a perfect quantum network coding protocol [11]. This was generalized to the k-pair case [10] where it was shown that if the classical k-pair problem is solvable using a *linear* coding scheme (or even just a vector-linear coding scheme over a finite field or a finite ring) then the quantum k-pair problem is also solvable using free classical communication. This result gives rise to two natural questions.

The first question is whether the linearity condition on the coding schemes of the classical k-pair problem can be removed. Indeed, there exist classical k-pair problems that are solvable with nonlinear coding schemes, but cannot be solved with linear coding schemes [2, 15]. This question is closely related to the following open problem: can we construct an instance of the k-pair problem for which there is a (nonlinear) solution to the classical version of the problem, but for which no perfect solution to the corresponding quantum version exists, even with free classical communication? Note that the techniques used in Ref. [10] rely on the linearity of the classical encoding scheme, and hence they cannot be used directly when simulating classical nonlinear coding schemes.

The second question is how much amount of classical communication is sufficient. The protocol in Ref. [10] essentially uses the fact that classical information can be sent (for free) between any two nodes, i.e., there exists a classical two-way channel between any two nodes, and their capacities are unlimited. Obviously, it would be desirable to find a weaker requirement on the classical communication, and to reduce the amount of classical communication as much as possible. This second question is closely related to the work of Leung, Oppenheim and Winter [12]. They investigated various settings of quantum network coding assisted with supplied resources such as free classical communication or entanglement. Among others, they considered the case where classical communication can be sent only between each pair of nodes connected by a quantum channel and only in the direction of that quantum channel. Unfortunately again, they found that the quantum two-pair problem on the

butterfly network cannot be solved even under this model. One open problem is thus to clarify which types of assistance of classical communication enable us to construct a quantum network coding protocol for a given k-pair problem, and show the minimal amount of classical communication necessary under such a model.

Our contribution. This paper provides solutions to both of the above two questions. We present a quantum protocol solving, if there is some help of classical communication, any instance of the k-pair problem for which the corresponding classical version is solvable (under *any* coding scheme). In other words, our result shows that whenever an instance of the classical k-pair problem is solvable, the quantum version of the same problem is solvable when assisted with classical communication. Furthermore, classical communication is only sent between two nodes linked by quantum channels, and more precisely one unit of classical communication is sent in the direction of each quantum channel, and one unit is sent in the reverse direction of each quantum channel. When considering two-dimensional quantum states (qubits), each classical communication unit consists of one bit, and thus, at most two bits are sent between adjacent nodes: one in the direction of the quantum channel and the other in the reverse direction. The total amount of classical communication bits sent is then at most twice the number of edges in the graph. This significantly improves the bound given in Ref. [10], in which the amount of classical communication going through every edge could depend on the number of nodes.

The starting point of our protocol is the method proposed in Ref. [10]. We first simulate a classical protocol by applying a quantum operator at each node in order to simulate the classical encoding performed at this node. This simulation introduces intermediate registers that are entangled with the quantum state we want to send to the targets, and thus have to be "properly disentangled." All the difficulties come from this latter crucial part. The technique used in Ref. [10] was to measure these intermediate registers in the Fourier basis, and then to send the measurement outcomes to the target nodes, who then correct locally the phase introduced by the measurements. However, this technique relies on the fact that the classical protocol being simulated is linear, namely that the exponent in the phase introduced is a linear function of the input — this is why the phase could be corrected locally at the targets. In our new protocol, we consider a different way of successfully disentangling the intermediate registers. The registers are again measured in the Fourier basis, but the measurement outcomes are then sent to the nodes to which the current node has incoming edges (instead of to the target nodes). We then show that, when these operations are done in a proper order (a reverse topological order of the nodes), then the phase introduced by the measurements can be corrected locally at these nodes. Repeating this process for each internal node of the graph enables us to disentangle almost all the intermediate registers. The remaining intermediate registers are those owned by the k source nodes, which can be disentangled by measuring them in the Fourier basis, but now sending the measurement outcomes through the graph to the targets. The point is that this can be done in a very communication-efficient way since this becomes precisely an instance of the classical k-pair problem for which a solution is available.

In our new protocol, the classical coding scheme we simulate then appears three times. First, this scheme is simulated quantumly, which introduces the intermediate registers — this uses one unit of quantum communication for each edge (in the original direction of the edge). Second, it is used when removing the internal intermediate registers to correct the phase — this uses one unit of classical communication for each edge (in the reverse direction of the edge). Third, it is used explicitly in order to remove, at the last part of the protocol, the intermediate registers owned by the source nodes — this uses one unit of classical communication for each edge (in the original direction of the edge).

Actually, our techniques can also be used to create EPR-pairs between the sources and the targets of an instance of the k-pair problem, whenever the associated classical k-pair problem is solvable, using one qubit of quantum communication and only one bit of classical communication per edge, as will be discussed in Section 5. Note that once EPR-pairs are shared, the quantum k-pair problem can be solved using teleportation. However, this would require three bits per edge in total, while the protocol described above (designed specifically for the k-pair problem) uses only two bits per edge.

Related work. The restriction of classical communication in this paper was also studied before by Leung, Oppenheim and Winter [12] (who called this the two-way assisted case with free two-way classical communication). As mentioned in Ref. [12], this enables us to send a qubit in a reverse direction to the quantum channel by sending

two bits (via quantum teleportation). Hence some examples of the k-pair problem are shown to be solvable by routing (i.e., without using any coding) when *time sharing* is allowed (i.e., when the rate of transmission is studied under the assumption that the network can be used more than once): see Ref. [12] for the butterfly network. It is open, however, whether every instance is solvable by routing. Our method suggests a different way of solving the quantum k-pair problem, which requires some coding but does not require time sharing, and works for any solvable classical instance.

2 The k-pair problem

The classical k-pair problem.

We recall the statement of the k-pair problem in the classical case (often called the multiple unicast problem), and the definition of a solution to this problem. The reader is referred to, for example, Ref. [3] for further details. We use the same setting as in Ref. [10], but some conventions differ in order to facilitate the exposition of our new protocol.

An instance of a k-pair problem is a directed acyclic graph $G = (V, E)$ and k pairs $(s_1, t_1), \ldots, (s_k, t_k)$ of nodes in V. We suppose, without loss of generality, that the nodes $s_1, \ldots, s_k$ have fan-in zero, and the nodes $t_1, \ldots, t_k$ have fan-in one and fan-out zero. We denote by $\overline{E}$ the set of *internal edges*, i.e., the edges in E with no extremity in $\{t_1, \ldots, t_k\}$. The k edges with an extremity in $\{t_1, \ldots, t_k\}$ are called the *output edges*. For each node v in V, we fix an arbitrary ordering of the incoming edges of v, and an arbitrary ordering of the outgoing edges of v.

For each $i \in \{1, \ldots, k\}$, a message x_i is given at the source s_i, and has to be sent to the target t_i through G under the condition that each edge has unit capacity. For convenience, the following convention is assumed when describing a classical coding scheme. Each source s_i is supposed to have a "virtual" incoming edge from which it receives its input x_i (each source node has thus fan-in at least one, but these virtual edges are not included in E). In this way, the source nodes perform coding operations on their inputs, and this convention enables one to ignore the distinction between source nodes and internal nodes. These conventions are illustrated in Fig. 1.

Let Σ be a finite set. A *coding scheme* over Σ is a choice of operations for each node in V with nonzero fan-in and nonzero fan-out: for each node $v \in V$ with fan-in $m \geq 1$ and fan-out $n \geq 1$, the operation at v is written as n functions $f_{v,1}, \ldots, f_{v,n}$, each from Σ^m to Σ, where the value $f_{v,i}(z_1, \ldots, z_m)$ represents the message sent through the i-th outgoing edge of v when the inputs of the m incoming edges are $z_1, \ldots, z_m$. Since the graph G is acyclic, we can fix a topological ordering of the nodes of the graphs, i.e., an ordering in which each node comes before all nodes to which it has outgoing edges. The coding scheme can then be explicitly implemented by applying the encoding functions in the order in which the nodes appear. A *solution* over Σ to an instance of the k-pair problem is a coding scheme over Σ that enables one to send simultaneously k messages $x_i \in \Sigma$ from s_i to t_i, for all $i \in \{1, \ldots, k\}$. For example, the coding scheme in Fig. 1 is a solution over $\{0, 1\}$ to the two-pair problem associated with the butterfly graph.

The quantum k-pair problem.

We suppose that the reader is familiar with the basics of quantum information theory and refer to Ref. [14] for a good reference. In this paper we use the same model for the quantum k-pair problem as in Ref. [10] except restricting the classical communication to be allowed.

An instance of a quantum k-pair problem is, as in the classical case, a directed acyclic graph $G = (V, E)$ and k pairs of nodes $(s_1, t_1), \ldots, (s_k, t_k)$. Let $\mathcal{H}$ be a Hilbert space. A (quantum) solution for $\mathcal{H}$ to the instance is a quantum coding scheme, i.e., a choice of quantum operations over all nodes, allowing us to send a quantum state $|\psi\rangle \in \mathcal{H}^{\otimes k}$ supported on the source nodes $s_1, \ldots, s_k$ (in this order) to the target nodes $t_1, \ldots, t_k$ (in this order). We consider the model where each edge of G can transmit one quantum state over $\mathcal{H}$. In this paper, classical

communication is only allowed between any two adjacent nodes: if $(v_1, v_2) \in E$ then classical communication is possible from v_1 to v_2 and from v_2 to v_1. (Note that in Ref. [10] classical communication was allowed between any two nodes of G.) For a positive integer d, an instance of the quantum k-pair problem is said to be *solvable* over $\mathbb{C}^d$ if there exists a protocol solving this problem for $\mathcal{H} = \mathbb{C}^d$.

3 Main result

The main result of this paper is the following theorem.

Theorem 1. *Let $G = (V, E)$ be a directed acyclic graph and $(s_1, t_1), \ldots, (s_k, t_k)$ be k pairs of nodes in V. Let Σ be a finite set. Suppose that there exists a solution over Σ to the associated classical k-pair problem. Then the corresponding quantum k-pair problem is solvable over $\mathbb{C}^{|\Sigma|}$. Moreover, there exists a quantum protocol for this task that sends at most two elements of Σ per edge as classical communication (one in each direction of the edge), i.e., at most $2|E|\lceil \log_2 |\Sigma| \rceil$ bits of classical communication in total.*

The amount of free classical communication used in the protocol of our previous work [10] was $km|V|\lceil \log_2 |\Sigma| \rceil$ bits, where m denotes the maximal fan-in over all nodes in G (note that $|E|$ is at most $O(m|V|)$ in the worst case, and is much smaller than $m|V|$ in most cases). The bound in Ref. [10] actually supposes that classical information can be sent between any two nodes of the graph. If the classical communication is restricted to adjacent nodes, then the amount of communication can increase by a factor corresponding to the length of the longest path from an internal node to a target node, and, in general, the number of elements of Σ that are sent through a given edge depends on k, $|V|$ and m. In comparison, Theorem 1 enables us to perform quantum network coding by sending at most two elements of Σ between adjacent nodes.

Notice that the classical communication bound of Theorem 1 is described independently of the original classical coding scheme. In fact, if there exists a coding scheme on a subgraph (V, E') of G, where $E' \subset E$ (e.g., if a part of the graph is not involved in the original classical encoding scheme), then the factor $|E|$ can be improved in a straightforward way. We can then also describe the complexity of a quantum k-pair problem in term of the complexity of the best classical protocol for the corresponding classical task (i.e., in term of the smallest subset $E' \subseteq E$ such that a solution over (V, E') exists). A specific statement of this observation for the case $|\Sigma| = 2$ follows.

Corollary 2. *Let $G = (V, E)$ be a directed acyclic graph and $(s_1, t_1), \ldots, (s_k, t_k)$ be k pairs of nodes in V. Suppose that there exists a solution over $\{0, 1\}$ to the associated classical k-pair problem using a total amount of C bits of communication. Then there exists a quantum protocol over $\mathbb{C}^2$ for the corresponding quantum k-pair problem that sends in total C qubits of communication and $2C$ bits of classical communication.*

4 Protocol

As in Ref. [10], the basic strategy for proving Theorem 1 is to perform a quantum simulation of the classical coding scheme, while the simulation method is more elaborated. Before presenting the proof, we need some preliminaries.

4.1 Quantum operators

Let Σ be a finite set. In the quantum setting, we suppose that each register contains a quantum state over $\mathcal{H} = \mathbb{C}^{|\Sigma|}$, and denote by $\{|z\rangle\}_{z \in \Sigma}$ an orthonormal basis of $\mathcal{H}$. We use the notation $|0_{\mathcal{H}}\rangle$ to refer to an arbitrary vector of the basis that will be used to initialize registers. Let σ be an arbitrary bijection from Σ to the set of integers $\{0, \ldots, |\Sigma| - 1\}$. For convenience we denote $\overline{x} = \sigma(x)$ for any element $x \in \Sigma$.

We define a unitary operator W over the Hilbert space $\mathcal{H}$ as follows: for any $y \in \Sigma$, the operator W maps the basis state $|y\rangle$ to the state

$$\frac{1}{\sqrt{|\Sigma|}} \sum_{z \in \Sigma} \exp\Big(\frac{2\pi\iota \overline{y} \cdot \overline{z}}{|\Sigma|}\Big)|z\rangle.$$

Note that W is basically the quantum Fourier transform over the cyclic group of order $|\Sigma|$.

A measurement of a quantum state over the Hilbert space $\mathcal{H}$ in the Fourier basis consists in applying the operator W to the quantum state, and then measuring it in the basis $\{|z\rangle\}_{z \in \Sigma}$. The measurement outcome is an element of Σ. Notice that, if the quantum state measured in the Fourier basis is $|y\rangle$, for some $y \in \Sigma$, and the measurement outcome is $z \in \Sigma$, then the state after measurement becomes $\exp\big(\frac{2\pi\iota \overline{y} \cdot \overline{z}}{|\Sigma|}\big)|z\rangle$.

Let m and n be two positive integers and $f_1, \ldots, f_n$ be n functions from Σ^m to Σ. Let $U_{f_1,\ldots,f_n}$ be a unitary operator over the Hilbert space $\mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n}$ such that, for any elements $y_1, \ldots, y_m$ in Σ, the operator $U_{f_1,\ldots,f_n}$ maps the basis state $|y_1, \ldots, y_m\rangle|0_{\mathcal{H}}, \ldots, 0_{\mathcal{H}}\rangle$ to the state $|y_1, \ldots, y_m\rangle|f_1(y_1, \ldots, y_m), \ldots, f_n(y_1, \ldots, y_m)\rangle$.

4.2 Global encoding functions

A coding scheme over a directed acyclic graph $G = (V, E)$ naturally induces a *global encoding function* associated with each edge in E. Let $\vec{e}$ be an edge in E. Then the global encoding function $g_{\vec{e}}\colon \Sigma^k \to \Sigma$ associated with the edge $\vec{e}$ is the function of the variables $x_1, \ldots, x_k$ representing the message sent through this edge by the coding scheme when the input is $x_1, \ldots, x_k$. Since G is acyclic, the global encoding functions can be defined directly as follows.

Definition 3. Let $G = (V, E)$ be a directed acyclic graph and (s_i, t_i) be k pairs of nodes in V, for $i \in \{1, \ldots, k\}$. Consider an encoding scheme for this k-pair problem defined by, for each node $v \in V$ with fan-in m and fan-out n, functions $f_{v,1}, \ldots, f_{v,n}$ from Σ^m to Σ representing the encoding performed at v. Then the global encoding function $g_{\vec{e}}\colon \Sigma^k \to \Sigma$ associated with this encoding scheme, for each $\vec{e} \in E$, is inductively defined as follows.

(a) Suppose that $\vec{e}$ is an edge in E of the form (s_i, u), with $i \in \{1, \ldots, k\}$ and $u \in V$. Suppose that $\vec{e}$ is the ℓ-th outgoing edge of s_i. Then $g_{\vec{e}}(x_1, \ldots, x_k) = f_{s_i,\ell}(x_i)$ for any $x_1, \ldots, x_k \in \Sigma$.

(b) Suppose that $\vec{e}$ is an edge in E of the form (v, w) with $v \notin \{s_1, \ldots, s_k\}$. Suppose that $\vec{e}$ is the ℓ-th outgoing edge of v and denote by $(u_1, v), \ldots, (u_m, v)$ the incoming edges of node v (see Fig. 2). Then, for any $x_1, \ldots, x_k \in \Sigma$,

$$g_{(v,w)}(x_1, \ldots, x_k) = f_{v,\ell}(g_{(u_1,v)}(x_1, \ldots, x_k), \ldots, g_{(u_m,v)}(x_1, \ldots, x_k)). \tag{1}$$

4.3 Proof of Theorem 1

Now we are ready to give the proof of Theorem 1 (see Appendix for an illustration of our strategy on the butterfly graph).

Proof of Theorem 1. Let $G = (V, E)$ be a graph on which there exists a solution to the classical k-pair problem associated with the pairs (s_i, t_i). Without loss of generality, we suppose that all nodes in $V \backslash \{t_1, \ldots, t_k\}$ have nonzero fan-in and nonzero fan-out (remember that each source node s_i has one virtual incoming edge). For each node $V \backslash \{t_1, \ldots, t_k\}$ with fan-in $m \geq 1$ and fan-out $n \geq 1$, let $f_{v,1}, \ldots, f_{v,n}$ be the coding operations performed at node v in the solution, where each function $f_{v,i}$ is from Σ^m to Σ.

Suppose that the input state of the quantum task is

$$|\psi_S\rangle_{(\mathsf{S}_1,\ldots,\mathsf{S}_k)} = \sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k} |x_1\rangle_{\mathsf{S}_1} \otimes \cdots \otimes |x_k\rangle_{\mathsf{S}_k},$$

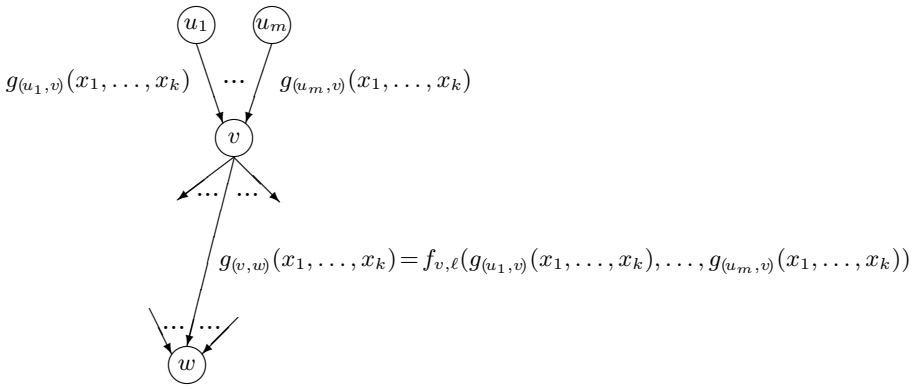

Figure 2: Illustration of the notion of global encoding functions. Here node v has m incoming edges labelled in increasing order $(u_1, v), \cdots, (u_m, v)$, and edge (v, w) is the ℓ-th outgoing edge of v.

where the $\alpha_{x_1,\ldots,x_k}$'s are complex numbers such that $\sum_{x_1,\ldots,x_k\in\Sigma} |\alpha_{x_1,\ldots,x_k}|^2 = 1$. Here, for each $i \in \{1,\ldots,k\}$, S_i is a register received by the node s_i from its incoming virtual edge. Our protocol consists of the three parts that are described in details below.

Part 1. First, we simulate the solution to the associated classical task node by node. In our simulation, each node in V will receive one quantum register along each incoming edge (remember that each source s_i receives S_i from its incoming virtual edge). Each node in $V\backslash\{t_1,\ldots,t_k\}$ will perform, in the same order as in the classical protocol (e.g., any topological order of the nodes of G), a quantum operation on the registers it receives, and send new registers through its outgoing edges.

More precisely, let $v \in V\backslash\{t_1,\ldots,t_k\}$ be a node of G with fan-in m and fan-out n. Let $\mathsf{Q}_1,\ldots,\mathsf{Q}_m$ denote the quantum registers received by the incoming edges. The coding performed at node v is simulated as follows: n quantum registers $\mathsf{Q}'_1,\ldots,\mathsf{Q}'_n$, each initialized to $|0_{\mathcal{H}}\rangle$, are introduced, and then the operator $U_{f_1,\ldots,f_n}$ is applied to the registers $(\mathsf{Q}_1,\ldots,\mathsf{Q}_m,\mathsf{Q}'_1,\ldots,\mathsf{Q}'_n)$. The registers $\mathsf{Q}'_1,\ldots,\mathsf{Q}'_n$ are then sent along the n outgoing edges of v (i.e., Q'_i is sent along the i-th outgoing edge of v), and the registers $\mathsf{Q}_1,\ldots,\mathsf{Q}_m$ are kept at node v.

Such a simulation is done for all the nodes in $V\backslash\{t_1,\ldots,t_k\}$. Notice that exactly one register is introduced per edge in E. These registers can then be indexed by the edges in E: the register associated with an edge of the form $(u, v) \in E$ is created at node u, then sent from u to v through edge (u, v) in the procedure described above, and is finally owned by node v. We will denote the registers associated with the output edges (and owned by the target nodes) by $\mathsf{T}_1,\ldots,\mathsf{T}_k$ and the other registers by $\mathsf{R}_{\vec{e}}$ for each $\vec{e} \in \overline{E}$. Remember that, additionally, each source s_i owns the input register S_i, for $i \in \{1,\ldots,k\}$. Then the overall quantum state consists of $|E| + k$ registers and, since the coding scheme under consideration solves the classical task, is of the form

$$\sum_{x_1,\ldots,x_k\in\Sigma} \alpha_{x_1,\ldots,x_k} |x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots \otimes |x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k} \otimes \Big(\bigotimes_{\vec{e}\in\overline{E}} |g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\Big),$$

where $g_{\vec{e}}$'s are the global encoding functions associated with the considered coding scheme, as defined in Definition 3.

Part 2. Second, we remove all the intermediate registers $\mathsf{R}_{\vec{e}}$. Consider an edge $(v, w) \in \overline{E}$ and the register $\mathsf{R}_{(v,w)}$ associated with it. This register is owned by the internal node w at the end of the procedure described in Part 1. Node w first measures register $\mathsf{R}_{(v,w)}$ in the Fourier basis. Suppose that the outcome of the measurement is

$a_{(v,w)} \in \Sigma$. The quantum state then becomes

$$\sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k} \exp\Big(2\pi\iota \frac{\overline{a_{(v,w)}} \cdot \overline{g_{(v,w)}(x_1,\ldots,x_k)}}{|\Sigma|}\Big) \times |x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots$$
$$\cdots \otimes |x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k} \otimes |a_{(v,w)}\rangle_{\mathsf{R}_{(v,w)}} \otimes \Big(\bigotimes_{\vec{e} \in \overline{E} \setminus \{(v,w)\}} |g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\Big).$$

Register $\mathsf{R}_{(v,w)}$ is not anymore entangled with the other registers, and can then be disregarded. Node w then sends the element $a_{(v,w)}$ of Σ to the node v using classical communication. Now suppose that (v,w) is the ℓ-th outgoing edge of v and denote by $(u_1,v),\ldots,(u_m,v)$ the incoming edges of node v (see Fig. 2). Node v then applies the map Y_v to its registers $(\mathsf{R}_{(u_1,v)},\ldots,\mathsf{R}_{(u_m,v)})$, where Y_v is defined as

$$Y_v\colon |z_1,\ldots,z_m\rangle \quad \mapsto \quad \exp\Big(-2\pi\iota \frac{\overline{a_{(v,w)}} \cdot \overline{f_{v,\ell}(z_1,\ldots,z_m)}}{|\Sigma|}\Big)|z_1,\ldots,z_m\rangle$$

for any $z_1,\ldots,z_m \in \Sigma$. From Equation (1), this implies that the quantum state becomes

$$\sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots \otimes |x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k} \otimes \Big(\bigotimes_{\substack{\vec{e} \in \overline{E} \\ \vec{e} \neq (v,w)}} |g_{\vec{e}}(x_1,\ldots,x_k)\rangle_{\mathsf{R}_{\vec{e}}}\Big),$$

where the register $\mathsf{R}_{(v,w)}$ has been disregarded. Notice that only one element of Σ has been sent (from w to v, i.e., in the reverse direction of the edge (v,w)).

The above procedure is performed by each internal node (i.e., each node in $V \setminus \{s_1,\ldots,s_k,t_1,\ldots,t_k\}$) in a reverse topological order (i.e., an ordering in which each node comes before all nodes from which it has incoming edges) — this latter condition is crucial for the correctness of the technique. The final state is

$$\sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots \otimes |x_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k}. \tag{2}$$

The total number of elements of Σ sent as classical communication in Part 2 is $|\overline{E}|$. More precisely, one element of Σ is sent per edge, in the reverse direction of the edge.

Part 3. Finally, we remove the registers $\mathsf{S}_1,\ldots,\mathsf{S}_k$. Remember that each register S_i is owned by node s_i, for $i \in \{1,\ldots,k\}$. Each node s_i then measures its register S_i in the Fourier basis, obtaining an element $b_i \in \Sigma$. The state then becomes

$$\sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k} \exp\Big(2\pi\iota \frac{\overline{b_1} \cdot \overline{x_1} + \cdots + \overline{b_k} \cdot \overline{x_k}}{|\Sigma|}\Big)|b_1\rangle_{\mathsf{S}_1}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots \otimes |b_k\rangle_{\mathsf{S}_k}|x_k\rangle_{\mathsf{T}_k}.$$

The registers $\mathsf{S}_1,\ldots,\mathsf{S}_k$ can then be disregarded. Each source s_i now sends b_i to the target t_i using classical communication. Notice that this is precisely an instance of the classical k-pair problem we are considering, and hence the assumed classical network coding protocol is available. Therefore, this can be done by sending at most one element of Σ per edge. As the last step, each target node t_i for $i \in \{1,\ldots,k\}$ applies the map Z_i to its register T_i, where Z_i maps the basis state $|x\rangle$ to the state $\exp\big(-2\pi\iota\frac{\overline{b_i}\cdot\overline{x}}{|\Sigma|}\big)|x\rangle$, for any $x \in \Sigma$. This corrects the phase and the resulting state is

$$\sum_{x_1,\ldots,x_k \in \Sigma} \alpha_{x_1,\ldots,x_k}|x_1\rangle_{\mathsf{T}_1} \otimes \cdots \otimes |x_k\rangle_{\mathsf{T}_k} = |\psi_S\rangle_{(\mathsf{T}_1,\ldots,\mathsf{T}_k)}.$$

The amount of classical communication sent in Part 3 is at most one element of Σ per edge (in the direction of the edge), i.e., at most $|E|$ elements of Σ in total.

This concludes the proof of Theorem 1. □

5 Sharing EPR-pairs

In this section we describe how our techniques can be used to create EPR-pairs between the sources and the targets of an instance of the k-pair problem using one qubit of quantum communication and only one bit of classical communication per edge.

Let $\mathcal{H}$ be a Hilbert space of dimension 2 with orthonormal basis $\{|0\rangle, |1\rangle\}$. Let A and B be two registers over $\mathcal{H}$. Remember that an EPR-pair over (A, B), denoted by $|\Psi\rangle_{(\mathsf{A},\mathsf{B})}$, is the quantum state $\frac{1}{\sqrt{2}}(|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}} + |1\rangle_{\mathsf{A}}|1\rangle_{\mathsf{B}})$.

Let $G = (V, E)$ be a directed acyclic graph and $(s_1, t_1), \ldots, (s_k, t_k)$ be k pairs of nodes. The corresponding *EPR-pair sharing problem* asks to create k EPR-pairs $|\Psi\rangle_{(\mathsf{S}_i\mathsf{T}_i)}$ where, for $i \in \{1, \ldots, k\}$, each S_i is a register owned by the source s_i and each T_i is a register owned by the target t_i. We consider the model where each edge of G can transmit one qubit and classical communication is only allowed between any two adjacent nodes.

Suppose that the classical k-pair problem associated to G and the k pairs (s_i, t_i) has a solution over $\{0, 1\}$. Each source node s_i creates a register S_i initialized to the state $|0\rangle_{\mathsf{S}_i}$, and applies a Hadamard transform on it. The quantum state obtained is

$$|\psi\rangle_{(\mathsf{S}_1,\ldots,\mathsf{S}_k)} = \frac{1}{\sqrt{2^k}}(|0\rangle_{\mathsf{S}_1} + |1\rangle_{\mathsf{S}_1}) \otimes \cdots \otimes (|0\rangle_{\mathsf{S}_k} + |1\rangle_{\mathsf{S}_k}).$$

Now consider the quantum k-pair problem associated to G and the k pairs (s_i, t_i) on the input $|\psi\rangle_{(\mathsf{S}_1,\ldots,\mathsf{S}_k)}$. Applying Part 1 and Part 2 of the protocol described in Section 4 gives (see Formula (2)) the state

$$\frac{1}{\sqrt{2^k}}(|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{T}_1} + |1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{T}_1}) \otimes \cdots \otimes (|0\rangle_{\mathsf{S}_k}|0\rangle_{\mathsf{T}_k} + |1\rangle_{\mathsf{S}_k}|1\rangle_{\mathsf{T}_k}) = |\Psi\rangle_{(\mathsf{S}_1,\mathsf{T}_1)} \otimes \cdots \otimes |\Psi\rangle_{(\mathsf{S}_k,\mathsf{T}_k)},$$

while only one bit of classical communication is sent per edge in $\overline{E}$, in the reverse direction of the edge. Here T_i denotes a register owned by the target node t_i, for $i \in \{1, \ldots, k\}$. We thus obtain the following result.

Theorem 4. *Let $G = (V, E)$ be a directed acyclic graph and $(s_1, t_1), \ldots, (s_k, t_k)$ be k pairs of nodes in V. Suppose that there exists a solution over $\{0, 1\}$ to the associated classical k-pair problem. Then there exists a quantum protocol that solves the corresponding EPR-pair sharing problem using only one bit of classical communication per edge (in the reverse direction of the edge).*

Acknowledgments

The authors are grateful to Kazuo Iwama for helpful comments on this work.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.

[2] R. Dougherty, C. F. Freiling, and K. Zeger. Insufficiency of linear coding in network information flow. *IEEE Transactions on Information Theory*, 51(8):2745–2759, 2005.

[3] R. Dougherty and K. Zeger. Nonreversibility and equivalent constructions of multiple-unicast networks. *IEEE Transactions on Information Theory*, 52(11):5067–5077, 2006.

[4] C. Fragouli and E. Soljanin. *Network coding fundamentals*. Now Publishers Inc., 2007.

[5] N. Harvey, R. Kleinberg, and A. Lehman. On the capacity of information networks. *IEEE Transactions on Information Theory*, 52(6):2345–2364, 2006.

[6] M. Hayashi. Prior entanglement between senders enables perfect quantum network coding with modification. *Physical Review A*, 76(4):040301(R), 2007.

[7] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Quantum network coding. In *STACS 2007*, volume 4393 of *Lecture Notes in Computer Science*, pages 610–621, 2007.

[8] T. Ho and D. S. Lun. *Network coding: an introduction*. Cambridge University Press, 2008.

[9] K. Iwama, H. Nishimura, M. Paterson, R. Raymond, and S. Yamashita. Polynomial-time construction of linear network coding. In *ICALP 2008*, volume 5125 of *Lecture Notes in Computer Science*, pages 271–282, 2008.

[10] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler. General scheme for perfect quantum network coding with free classical communication. In *ICALP 2009*, volume 5555 of *Lecture Notes in Computer Science*, pages 622–633, 2009. See also arXiv preprint 0908.1457, August 2009.

[11] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler. Perfect Quantum Network Communication Protocol Based on Classical Network Coding. In *IEEE International Symposium on Information Theory*, pages 2686–2690, 2010. See also arXiv preprint 0902.1299, February 2009.

[12] D. Leung, J. Oppenheim, and A. Winter. Quantum network communication — the butterfly and beyond. *IEEE Transactions on Information Theory*, 56(7):3478–3490, 2010. See also arXiv preprint quant-ph/0608223, August 2006.

[13] Z. Li and B. Li. Network coding in undirected networks. In *38th Annual Conference on Information Sciences and Systems*, pages 257–262, 2004.

[14] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[15] S. Riis. Linear versus non-linear boolean functions in network flow. In *38th Annual Conference on Information Sciences and Systems*, 2004.

[16] Y. Shi and E. Soljanin. On multicast in quantum networks. In *40th Annual Conference on Information Sciences and Systems*, pages 871–876, 2006.

[17] C.-C. Wang and N. B. Shroff. Beyond the butterfly – a graph-theoretic characterization of the feasibility of network coding with two simple unicast sessions. In *IEEE International Symposium on Information Theory*, pages 121–125, 2007.

[18] R. W. Yeung. *Information Theory and Network Coding*. Springer-Verlag, 2007.

[19] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang. *Network coding theory*. Now Publishers Inc., 2006.

Appendix: Example for our protocol

We illustrate in this appendix the techniques developed in this paper for the butterfly network shown in Figure 3. Our task is to send a quantum state $|\psi_S\rangle$ from the source nodes s_1 and s_2 to the target nodes t_1 and t_2. The task can be achieved using the quantum protocol given in Theorem 1. We give the explicit details for this example. More precisely, we describe how the protocol simulates the classical linear coding scheme over $\Sigma = \mathbb{F}_2$ (the finite field of size 2) presented in Fig. 1. Notice that this example does not require nonlinear coding, but we prefer to explain our protocol on this simple example rather than on known instances of the k-pair problem that require nonlinear coding (e.g., the networks proposed in Refs. [2, 15]) since the latter are rather complex. Moreover, we believe that this choice enables the reader to better compare our new protocol to the one proposed in our previous work [10].

Hereafter, all the registers are assumed to be single-qubit registers, i.e., $\mathcal{H} = \mathbb{C}^2$. We denote by $\{|z\rangle\}_{z\in\mathbb{F}_2}$ an orthonormal basis of $\mathcal{H}$. All the registers are supposed to be initialized to $|0\rangle$.

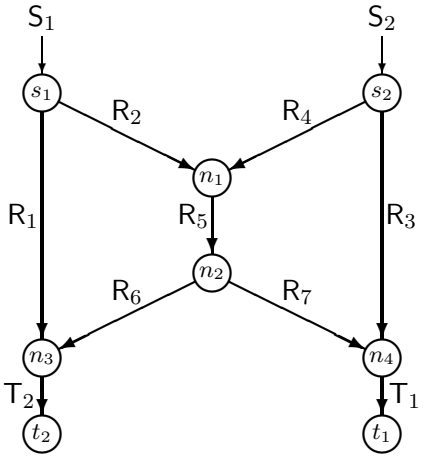

Figure 3: Quantum network coding through the butterfly network. Each edge has quantum capacity one. The task is to send a given input quantum state $|\psi_S\rangle$ in $(\mathsf{S}_1, \mathsf{S}_2)$ to $(\mathsf{T}_1, \mathsf{T}_2)$ in this order of registers. Here, the quantum register S_1 (resp. S_2) is possessed by the source node s_1 (resp. s_2), while the quantum register T_1 (resp. T_2) is possessed at the end of the protocol by the target node t_1 (resp. t_2). The protocol given in Theorem 1 realizes perfect quantum transmission of $|\psi_S\rangle$. Each R_i or T_i indicates the quantum register to be sent along the corresponding edge in the protocol.

In this example, the unitary operator U_{f_I,f_I} is applied at nodes s_1, s_2 and n_2, where f_I denotes the identity map over $\mathbb{F}_2$. The operator U_{f_I,f_I} maps each basis state $|y\rangle|z_1, z_2\rangle$ to the state $|y\rangle|z_1 + y, z_2 + y\rangle$. The quantum unitary operator U_{f_+} is applied at nodes n_1, n_3 and n_4, where $f_+ \colon (\mathbb{F}_2)^2 \to \mathbb{F}_2$ is the function mapping (y_1, y_2) to $y_1 + y_2$. The operator U_{f_+} maps $|y_1, y_2\rangle|z\rangle$ to $|y_1, y_2\rangle|z + y_1 + y_2\rangle$. Notice that both U_{f_I,f_I} and U_{f_+} can be implemented by using controlled-NOT operators.

Now we present our protocol for the example of Fig. 3. Let

$$|\psi_S\rangle_{(\mathsf{S}_1,\mathsf{S}_2)} = \alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{S}_2} + \alpha_{01}|0\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{S}_2} + \alpha_{10}|1\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{S}_2} + \alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{S}_2}$$

be the state that has to be sent from the source nodes to the target nodes. Here S_1 (resp. S_2) is a register received by the source s_1 (resp. s_2) through its virtual incoming edge.

Part 1. Node s_1 (resp. s_2) introduces two registers R_1 and R_2 (resp. R_3 and R_4), and applies the operator U_{f_I,f_I}

over the registers $(\mathsf{S}_1, \mathsf{R}_1, \mathsf{R}_2)$ (resp. over the registers $(\mathsf{S}_2, \mathsf{R}_3, \mathsf{R}_4)$). The resulting state is

$$\begin{aligned}
&\alpha_{00}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}\\
+&\alpha_{01}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}\\
+&\alpha_{10}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}\\
+&\alpha_{11}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}.
\end{aligned}$$

Hereafter, let $\mathbf{0}$ and $\mathbf{1}$ denote strings of all-zero and all-one, respectively, of appropriate length (three here). Then R_1 and R_2 are sent to n_3 and n_1, respectively, while R_3 and R_4 are sent to n_4 and n_1, respectively.

Then the protocol proceeds with the simulation of the coding operation performed at node n_1 in the classical coding scheme of Fig. 1: node n_1 prepares a new register R_5 and applies the operator U_{f_+} on registers $(\mathsf{R}_2, \mathsf{R}_4, \mathsf{R}_5)$. The resulting state is

$$\begin{aligned}
&\alpha_{00}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}\\
+&\alpha_{01}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}\\
+&\alpha_{10}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}\\
+&\alpha_{11}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}.
\end{aligned}$$

The register R_5 is then sent to n_2.

The node n_2 now prepares two registers R_6 and R_7, and applies the operator U_{f_I,f_I} on the registers $(\mathsf{R}_5, \mathsf{R}_6, \mathsf{R}_7)$. The resulting state is

$$\begin{aligned}
&\alpha_{00}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{0}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}\\
+&\alpha_{01}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{1}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}\\
+&\alpha_{10}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{1}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}\\
+&\alpha_{11}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{0}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)},
\end{aligned}$$

and the registers R_6 and R_7 are sent to n_3 and n_4, respectively.

In the last step of the simulation, node n_3 (resp. n_4) prepares one register T_2 (resp. T_1), and applies the U_{f_+} to registers $(\mathsf{R}_1, \mathsf{R}_6, \mathsf{T}_2)$ (resp. $(\mathsf{R}_3, \mathsf{R}_7, \mathsf{T}_1)$). The resulting state is

$$\begin{aligned}
&\alpha_{00}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{0}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{01}|\mathbf{0}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{1}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+&\alpha_{10}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{1}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{11}|\mathbf{1}\rangle_{(\mathsf{S}_1,\mathsf{R}_1,\mathsf{R}_2)}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|\mathbf{0}\rangle_{(\mathsf{R}_5,\mathsf{R}_6,\mathsf{R}_7)}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2},
\end{aligned}$$

and registers T_1 and T_2 are sent to nodes t_1 and t_2, respectively.

At this point of our protocol, node s_1 owns register S_1, node s_2 owns register S_2, node n_1 owns registers R_2 and R_4, node n_2 owns register R_5, node n_3 owns register R_1 and R_6, node n_4 owns registers R_3 and R_7, node t_1 owns register T_1, and node t_2 owns register T_2.

Part 2. Let us take a reverse topological order of the internal nodes of the graph, for example (n_3, n_4, n_2, n_1).

Node n_3 first measures its registers R_1 and R_6 in the Hadamard basis (i.e., the Fourier basis for $|\Sigma| = 2$), giving outcomes a_1 and a_2 respectively. The resulting state is

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|a_1\rangle_{\mathsf{R}_1}|0\rangle_{\mathsf{R}_2}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}|a_2\rangle_{\mathsf{R}_6}|0\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&(-1)^{a_2}\alpha_{01}|0\rangle_{\mathsf{S}_1}|a_1\rangle_{\mathsf{R}_1}|0\rangle_{\mathsf{R}_2}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}|a_2\rangle_{\mathsf{R}_6}|1\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+&(-1)^{a_1+a_2}\alpha_{10}|1\rangle_{\mathsf{S}_1}|a_1\rangle_{\mathsf{R}_1}|1\rangle_{\mathsf{R}_2}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}|a_2\rangle_{\mathsf{R}_6}|1\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&(-1)^{a_1}\alpha_{11}|1\rangle_{\mathsf{S}_1}|a_1\rangle_{\mathsf{R}_1}|1\rangle_{\mathsf{R}_2}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}|a_2\rangle_{\mathsf{R}_6}|0\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2},
\end{aligned}$$

and R_1 and R_6 can be disregarded. Node n_3 then sends the bit a_1 to s_1, and the bit a_2 to n_2, using classical communication along the edges (s_1, n_3) and (n_2, n_3) but in the reverse direction. Node s_1 then applies on its register S_1 the quantum operator mapping, for each $x \in \mathbb{F}_2$, the state $|x\rangle$ to $(-1)^{-a_1 x}|x\rangle$. Node n_2 applies on its register R_5 the quantum operator mapping, for each $x \in \mathbb{F}_2$, the state $|x\rangle$ to $(-1)^{-a_2 x}|x\rangle$. The quantum state becomes

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{01}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+&\alpha_{10}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|\mathbf{0}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|1\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|\mathbf{1}\rangle_{(\mathsf{S}_2,\mathsf{R}_3,\mathsf{R}_4)}|0\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2},
\end{aligned}$$

where R_1 and R_6 have been disregarded.

Similarly, node n_4 measures its registers R_3 and R_7 in the Hadamard basis, giving outcomes b_1 and b_2 respectively. The resulting state is

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|b_1\rangle_{\mathsf{R}_3}|0\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{R}_5}|b_2\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+(-1)^{b_1+b_2}&\alpha_{01}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|b_1\rangle_{\mathsf{R}_3}|1\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{R}_5}|b_2\rangle_{\mathsf{R}_7}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+(-1)^{b_2}&\alpha_{10}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|b_1\rangle_{\mathsf{R}_3}|0\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{R}_5}|b_2\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+(-1)^{b_1}&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|b_1\rangle_{\mathsf{R}_3}|1\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{R}_5}|b_2\rangle_{\mathsf{R}_7}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}.
\end{aligned}$$

Node n_4 then sends b_1 to node s_2, and b_2 to node n_2 using classical communication. Node s_1 then applies on its register S_2 the quantum operator mapping, for each $x \in \mathbb{F}_2$, the state $|x\rangle$ to $(-1)^{-b_1 x}|x\rangle$. Node n_2 applies on its register R_5 the quantum operator mapping, for each $x \in \mathbb{F}_2$, the state $|x\rangle$ to $(-1)^{-b_2 x}|x\rangle$. The quantum state becomes

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{01}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+&\alpha_{10}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2},
\end{aligned}$$

where R_3 and R_7 have been disregarded.

Node n_2 then measures its registers R_5 in the Hadamard basis, giving outcomes c. The state becomes

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|c\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+(-1)^{c}&\alpha_{01}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|c\rangle_{\mathsf{R}_5}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+(-1)^{c}&\alpha_{10}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|c\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|c\rangle_{\mathsf{R}_5}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}.
\end{aligned}$$

The value c is then sent to node n_1. The register R_5 can be disregarded, and the phase introduced is corrected in the following way: node n_1 applies on its registers $(\mathsf{R}_2, \mathsf{R}_4)$ the unitary operator mapping, for any $x, y \in \mathbb{F}_2$, the state $|x, y\rangle$ to the state $(-1)^{-c f_+(x,y)}|x, y\rangle = (-1)^{-c(x+y)}|x, y\rangle$. The resulting state is

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{01}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}\\
+&\alpha_{10}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2}\\
+&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{R}_2}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{R}_4}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}.
\end{aligned}$$

Notice that the same procedure to remove register R_5 would have worked even if f_+ is not a linear function. This is the crucial observation that enables us to simulate nonlinear classical protocols as well.

Finally, node n_1 measures its registers R_2 and R_4 in the Hadamard basis, giving outcomes d_1 and d_2 respectively. It sends d_1 to node s_1, and d_2 to node s_2, respectively. The registers R_2 and R_4 can then be disregarded, and the phase introduced is corrected in the following way: node s_1 (resp. s_2) applies on its register S_1 (resp. S_2) the unitary operator mapping, for any $x \in \mathbb{F}_2$, the state $|x\rangle$ to the state $(-1)^{-d_1 x}|x\rangle$ (resp. to $(-1)^{-d_2 x}|x\rangle$). The quantum state becomes

$$\begin{aligned}
&\alpha_{00}|0\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} \\
+&\alpha_{01}|0\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2} \\
+&\alpha_{10}|1\rangle_{\mathsf{S}_1}|0\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} \\
+&\alpha_{11}|1\rangle_{\mathsf{S}_1}|1\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}.
\end{aligned}$$

Part 3. Node s_1 (resp. s_2) measures its quantum register S_1 (resp. S_2) in the Hadamard basis, giving outcomes e_1 (resp. e_2). The state becomes

$$\begin{aligned}
&\alpha_{00}|e_1\rangle_{\mathsf{S}_1}|e_2\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} \\
+&(-1)^{e_2}\alpha_{01}|e_1\rangle_{\mathsf{S}_1}|e_2\rangle_{\mathsf{S}_2}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2} \\
+&(-1)^{e_1}\alpha_{10}|e_1\rangle_{\mathsf{S}_1}|e_2\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} \\
+&(-1)^{e_1+e_2}\alpha_{11}|e_1\rangle_{\mathsf{S}_1}|e_2\rangle_{\mathsf{S}_2}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2}.
\end{aligned}$$

The registers S_1 and S_2 can then be disregarded. Then e_1 is sent from the sources s_1 to the target t_1 using classical communication and, similarly, e_2 is sent from s_2 to t_2. This is done using one bit of communication per edge by using the original coding protocol for the butterfly graph: the bit e_1 is sent through edges (s_1, n_1) and (s_1, n_3), the bit e_2 is sent through edges (s_2, n_1) and (s_2, n_4), and the bit $e_1 + e_2$ is sent through edges (n_1, n_2), (n_2, n_3) and (n_2, n_4). The bit e_1 can then be recovered at node t_1 and the bit e_2 can be recovered at node t_2.

Node t_1 (resp. t_2) finally applies on its register T_1 (resp. T_2) the unitary operator mapping, for any $x \in \mathbb{F}_2$, the state $|x\rangle$ to the state $(-1)^{-e_1 x}|x\rangle$ (resp. to $(-1)^{-e_2 x}|x\rangle$). Now the quantum state becomes the desired state

$$\alpha_{00}|0\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} + \alpha_{01}|0\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2} + \alpha_{10}|1\rangle_{\mathsf{T}_1}|0\rangle_{\mathsf{T}_2} + \alpha_{11}|1\rangle_{\mathsf{T}_1}|1\rangle_{\mathsf{T}_2} = |\psi_S\rangle_{(\mathsf{T}_1,\mathsf{T}_2)}.$$

This concludes our protocol.