

# Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols (3pages Abstract)

HIROTADA KOBAYASHI<sup>1</sup>   FRANCOIS LE GALL<sup>2</sup>   HARUMICHI NISHIMURA<sup>3</sup>   MARTIN RÖTTELER<sup>4</sup>

<sup>1</sup>National Institute of Informatics, Tokyo, Japan; hirokada@nii.ac.jp

<sup>2</sup>The University of Tokyo, Tokyo, Japan; legall@is.s.u-tokyo.ac.jp

<sup>3</sup>Osaka Prefecture University, Japan; hnishimura@mi.s.osakafu-u.ac.jp

<sup>4</sup>NEC Laboratories America, Inc., Princeton, NJ, USA; mroetteler@nec-labs.com

The idea of *network coding*, proposed in the seminal paper by Ahlswede, Cai, Li and Yeung in 2000, 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.

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. 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 [Hay07, HINRY07, LOW10] 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 are classical, is one of the most important network coding problems. 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 [Hay07, HINRY07, LOW10]. 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 [KLN09a]. This was generalized to the  $k$ -pair case [KLN09b] 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. 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

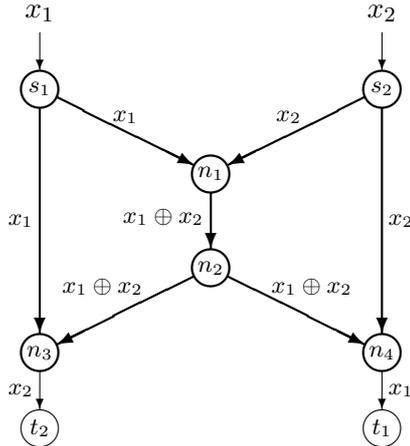


Figure 1: The butterfly network and a classical linear coding protocol. The node  $s_1$  (resp.  $s_2$ ) has for input a bit  $x_1$  (resp.  $x_2$ ). The task is to send  $x_1$  to  $t_1$  and  $x_2$  to  $t_2$ . The capacity of each edge is assumed to be one bit.

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. [KLN09b] 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. [KLN09b] 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 [LOW10]. 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. [KLN09b], 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. [KLN09b]. 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. [KLN09b] 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. 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.

#### References.

- [Hay07] M. Hayashi. *Phys. Rev. A* **76**(4) (2007) 040301(R).
- [HINRY07] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. In *Proc. STACS07*, LNCS4393, pp. 610–621, 2007.
- [KLN09a] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler. In *Proc. ISIT10*, pp. 2686–2690, 2010. See also arXiv:0902.1299, February 2009.
- [KLN09b] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler. In *Proc. ICALP09*, LNCS 5555, pp. 622–633, 2009. See also arXiv:0908.1457, August 2009.
- [LOW10] D. Leung, J. Oppenheim, and A. Winter. *IEEE Trans. Info. Theo.* **56**(7) (2010) 3478–3490.