Quantum Network Coding

Masahito Hayashi[1], Kazuo Iwama[2], Harumichi Nishimura[3], Rudy Raymond[2] and Shigeru Yamashita[4]

[1] Japan Science and Technology Agency, ERATO-SORST Quantum Computation and Information Project
Tokyo 113-0033, Bunkyo-ku, Hongo 5-28-3, Japan
masahito@qci.jst.go.jp
[2] Kyoto University, Graduate School of Informatics
Kyoto 606-8501, Sakyo-ku, Yoshida-Honmachi, Japan
{iwama, raymond}@kuis.kyoto-u.ac.jp
[3] Osaka Prefecture University, Graduate School of Science
Osaka 599-8531, Sakai, Gakuen-cho 1-1, Japan
hnishimura@mi.s.osakafu-u.ac.jp
[4] Graduate School of Information Science, Nara Institute of Science and Technology
Nara 630-0192, Ikoma, Takayama-cho 8916-5, Japan
ger@is.naist.ac.jp

Abstract. Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this paper is whether or not *quantum* network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow.

Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. Our results for quantum network coding include: (i) We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2. (ii) If one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states. (iv) Several impossibility results including the general upper bound of the fidelity are also given.

Keywords. network coding, quantum communication, quantum computation

1 Introduction

In [3], Ahlswede, Cai, Li and Yeung showed that the fundamental law for network flow, the max-flow min-cut theorem, no longer applies for "digital information

Dagstuhl Seminar Proceedings 06111
Complexity of Boolean Functions
http://drops.dagstuhl.de/opus/volltexte/2006/608

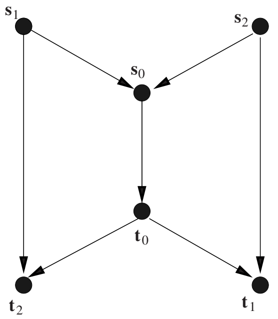

Fig. 1. Butterfly network.

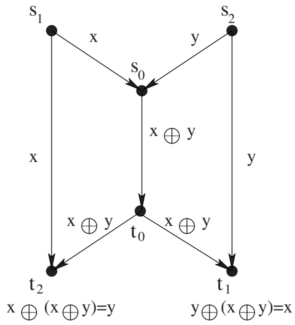

Fig. 2. Coding scheme

flow." The simple, nice example in [3] is called the Butterfly network illustrated in Fig. 1. The capacity of each directed link is all one and there are two source-sink pairs s_1 to t_1 and s_2 to t_2. Notice that both paths have to use the single link from s_0 to t_0 and hence the total amount of (conventional commodity) flow in both paths is bounded by one, say, 1/2 for each. In the case of digital information flow, however, the protocol shown in Fig. 2 allows us to transmit two bits, x and y, simultaneously. Thus, we can effectively achieve larger channel capacity than can be achieved by simple routing. This is known as *network coding* since [3] and has been quite popular (see e.g., [1,18,20,22,23] for recent developments).

The primary question in this paper is whether such a capacity enhancement is also possible for *quantum* information, more specifically, whether we can transmit two qubits from s_1 to t_1 and s_2 to t_2 simultaneously, as with classical network coding. Note that there are (at least) two tricks in the classical case. One is the EX-OR (Exclusive-OR) operation at node s_0; one can see that the bit y is encoded by using x as a key which is sent directly from s_1 to t_2, and vise versa. The other is the exact copy of one-bit information at node t_0. Our answer to the question obviously depends on if we can find quantum counterparts for these key operations.

Neither seems easy: For the copy operation, there is a famous no-cloning theorem [29]. Also, there is no obvious way of encoding a quantum state by a quantum state at s_0. Consider, for example, a simple extension of the classical operation at node s_0, i.e., a controlled unitary transform U as illustrated in Fig. 3. (Note that classical EX-OR is realized by setting $U = X$ "bit-flip.") Then, for any U, there is a quantum state $|\phi\rangle$ (actually an eigenvector of U) such that $|\phi\rangle$ and $U|\phi\rangle$ are identical (up to a global phase). Namely, if $|\psi_2\rangle = |\phi\rangle$, then the quantum state at the output of U is exactly the same for $|\psi_1\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$. This means their difference is completely lost at that position and hence is completely lost at t_1 also.

Thus it is highly unlikely that we can achieve an exact transmission of two quantum states, which forces us to consider an *approximate* transmission. (Now the no-cloning theorem is not an absolute threat since we have the approximated cloning by Bužek and Hillery [11], but the second problem still remains.) As the

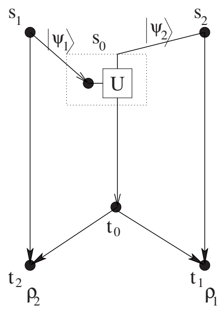

Fig. 3. Network using a controlled unitary operation

similarity measure between the input state $|\psi_1\rangle$ at s_1 ($|\psi_2\rangle$ at s_2, resp.) and the output state $\boldsymbol{\rho}_1$ at t_1 ($\boldsymbol{\rho}_2$ at t_2, resp.) we use the standard one called *fidelity*. Namely, our goal is to design a protocol achieving the best (worst-case) fidelity between input and output states. The fidelity is at most 1.0 by definition. Also, 0.5 is automatically achieved by outputting a completely mixed state. Thus those two values are trivial upper and lower bounds for the performance of such a protocol.

Our Contribution. In this paper, we give nontrivial lower and upper bounds under several different situations. On the positive side, we first consider the most general setting: We give a protocol such that for *any* quantum states $|\psi_1\rangle$ at s_1 and $|\psi_2\rangle$ at s_2, $F(|\psi_1\rangle, \boldsymbol{\rho}_1)$ and $F(|\psi_2\rangle, \boldsymbol{\rho}_2)$ are both strictly greater than 1/2 (Theorem 1), where F is the fidelity. The idea is discretization of (continuous) quantum states. Namely, the quantum state from s_2 is changed into classical two bits by what we call "tetra measurement." Those two bits are then used as a key to encode the state from s_1 at node s_0 ("group operation") and also to decode it at node t_1. Our protocol heavily depends upon the approximate cloning mentioned above, which obviously distorts quantum states. Interestingly, it also has a positive effect by which we can escape the second problem on the state distinguishability ("3D Bell measurement").

Note that the present general lower bound is only slightly better than 1/2 (some 0.52). However, if we impose some restriction, the value becomes much better. For example, if $|\psi_1\rangle$ is a classical state (i.e. either $|0\rangle$ or $|1\rangle$), then the fidelity becomes 2/3 (Theorem 4). Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states, especially if they are so called quantum random access coding states [4]. By using this, we can design an interesting protocol which can send two classical bits from s_1 to t_1 (similarly two bits from s_2 to t_2) but only one of them, determined by adversary, should be recovered. It is shown that the success probability for this protocol is $1/2 + \sqrt{2}/16$ (Theorem 6), but classically the success probability for any protocol is at most 1/2.

On the negative side, our general upper bound (Theorem 2) may not seem very impressive (some 0.983), but once again it is improved under restrictions. In particular, if we impose two restrictions, (i) $|\psi_1\rangle$ at s_1 is classical and (ii) the protocol is *natural*, then we can prove an upper bound of 11/12 (Theorem 5). Here, a natural protocol means that we always use "optimal" (not necessarily Bužek-Hillery) cloning whenever quantum copy is needed, which is quite reasonable. Note that all protocols in this paper are natural. Secondly, we can prove that the two side links (s_1 to t_2 and s_2 to t_1) which are unusable in the conventional multicommodity flow are in fact useful; if we remove them, then we cannot achieve fidelity $p > 1/2$ for crossing two qubits simultaneously (Theorem 3). Thirdly, we give a limit of transmitting random access coding states. Note that Theorem 6 can be extended to the three-bit case (with success probability some 0.525) but that is the limit; no protocol exists for the four-bit transmission with success probability strictly greater than 1/2 (Theorem 8).

Related Work. The study of coding methods on quantum information and computation has been deeply explored for error correction of quantum computation (since [28]) and data compression of quantum sources (since [27]). Recall that their techniques are duplication of data (error correction) and average-case analysis (data compression). Those standard approaches do not seem to help in the core of our problem.

More tricky applications of quantum mechanism are quantum teleportation [6], superdense coding [7], and a variety of quantum cryptosystems including the BB84 key distribution [5]. Probably most related one to this paper is the random access coding by Ambainis, Nayak, Ta-shma, and Vazirani [4], which allows us to encode two or more classical bits into one qubit and decode it to recover any one of the source bits. Our third protocol is a realization of this scheme on the Butterfly network.

Different from the classical world, the quantum mechanics prohibits us from exact manipulation of some fundamental operations such as cloning a qubit [29], deleting one of two copies of a qubit [26], and the universal NOT of a qubit (on the Bloch sphere) [9,12,16]. However, since these operations are so basic ones, it was natural that their approximated or probabilistic versions were investigated. For instance, Bužek and Hillery [11] found a quantum cloning machine which produces two copies of any unknown original state with fidelity 5/6, which was shown to be optimal [8]. Our approximated approach reflects the policy of these studies on manipulations of unknown quantum states.

For applications of coding to computational complexity theory, see e.g., [4,10,21].

Our Model. Our model as a quantum circuit is shown in Fig. 4. The information sources at nodes s_1 and s_2 are pure one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. (It turns out, however, that the result does not change for mixed states because of the joint concavity of the fidelity [24].) Any node does not have prior entanglement with other nodes. At every node, a physically allowable operation, i.e., trace-preserving completely positive map (TP-CP map), is done, and each edge can send only one qubit. They are implemented by unitary operations with

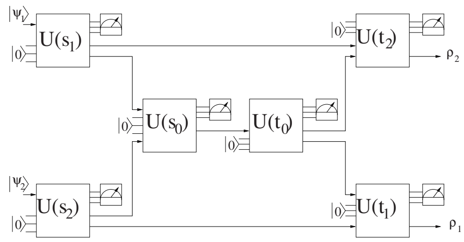

Fig. 4. Quantum circuit for coding on the Butterfly network

additional ancillae and by discarding all qubits except for the output qubits [2,24].

Our goal is to send $|\psi_1\rangle$ to node t_1 and $|\psi_2\rangle$ to node t_2 as well as possible. The quality of data at node t_j is measured by the fidelity between the original state $|\psi_j\rangle$ and the state $\boldsymbol{\rho}_j$ output at node t_j by the protocol. Here, the fidelity between two quantum states $\boldsymbol{\rho}$ and $\boldsymbol{\sigma}$ are defined as $F(\boldsymbol{\sigma},\boldsymbol{\rho}) = \left(\mathrm{Tr}\sqrt{\boldsymbol{\rho}^{1/2}\boldsymbol{\sigma}\boldsymbol{\rho}^{1/2}}\right)^2$ as in [8,13,15]. (The other common definition is $\mathrm{Tr}\sqrt{\boldsymbol{\rho}^{1/2}\boldsymbol{\sigma}\boldsymbol{\rho}^{1/2}}$.) In particular, the fidelity between a pure state $|\psi\rangle$ and a mixed state $\boldsymbol{\rho}$ is $F(|\psi\rangle,\boldsymbol{\rho}) = \langle\psi|\boldsymbol{\rho}|\psi\rangle$. (To simplify the description, for a pure state $|\psi\rangle\langle\psi|$ we often use the vector representation $|\psi\rangle$ and we also use bold fonts for a 2×2 or 4×4 density matrix for exposition.) We call the minimum of $F(|\psi_j\rangle,\boldsymbol{\rho}_j)$ over all one-qubit states $|\psi_j\rangle$ the *fidelity at node* t_j.

2 Protocol for Crossing Two Qubits

In this section we prove the following lower bound.

Theorem 1. *There exists a quantum protocol whose fidelities at nodes t_1 and t_2 are $1/2 + 2/81$ and $1/2 + 2\sqrt{3}/243$, respectively.*

2.1 Overview of the Protocol

Fig. 5 illustrates our protocol, Protocol for Crossing Two Qubits (XQQ). As expected, the approximated cloning is used at nodes s_1, s_2 and t_0. At node s_0, we first apply the tetra measurement to the state of one-qubit system $\mathcal{Q}_3$ and obtain two classical bits r_1r_2. Their different four values suggest which part of the Bloch sphere the state of $\mathcal{Q}_3$ sits in. These four values are then used to choose one of four different operations, the group operations, to encode the state of $\mathcal{Q}_2$. These four operations include identity I, bit-flip X, phase-flip Z, and bit+phase-flip Y. At node t_1, we apply the reverse operations of these four operations (actually the same as the original ones) for the decoding purpose.

At node t_2, we recover the two bits r_1r_2 (actually the corresponding quantum state for the output state) by comparing $\mathcal{Q}_1$ and $\mathcal{Q}_6$. This should be possible

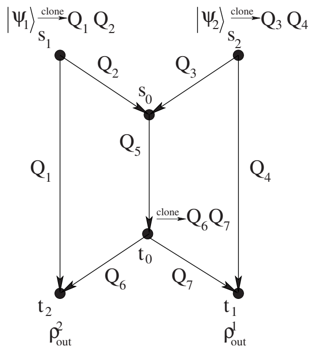

Fig. 5. Protocol XQQ.

since $\mathcal{Q}_2$ ($\approx \mathcal{Q}_1$) is encoded into $\mathcal{Q}_5$ ($\approx \mathcal{Q}_6$) by using $r_1 r_2$ as a key but its implementation is not obvious. It is shown that for this purpose, we can use the Bell measurement together with the fact that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are partially entangled as a result of cloning at node s_1.

Remark. It is not hard to average the fidelities at t_1 and t_2 by mixing the encoding state at t_1 with the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$, implying $1/2 + 2(2-\sqrt{3})/27 \approx 0.52$ at both sinks.

2.2 Building Blocks

Universal Cloning (UC). As the first tool of our protocol, we recall the notion of the approximated cloning by Bužek and Hillery [11], called the *universal cloning*. Let $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Then, it is given by the TP-CP map UC defined by

$$UC(|0\rangle\langle 0|) = \frac{2}{3}|00\rangle\langle 00| + \frac{1}{3}|\Psi^+\rangle\langle\Psi^+|, \quad UC(|0\rangle\langle 1|) = \frac{\sqrt{2}}{3}|\Psi^+\rangle\langle 11| + \frac{\sqrt{2}}{3}|00\rangle\langle\Psi^+|,$$
$$UC(|1\rangle\langle 0|) = \frac{\sqrt{2}}{3}|11\rangle\langle\Psi^+| + \frac{\sqrt{2}}{3}|\Psi^+\rangle\langle 00|, \quad UC(|1\rangle\langle 1|) = \frac{2}{3}|11\rangle\langle 11| + \frac{1}{3}|\Psi^+\rangle\langle\Psi^+|. \tag{1}$$

Let $\boldsymbol{\rho}_1 = \mathrm{Tr}_2 UC(|\psi\rangle)$ and $\boldsymbol{\rho}_2 = \mathrm{Tr}_1 UC(|\psi\rangle)$, where Tr_i is the partial trace over the i-th qubit. Then, easy calculation implies that $\boldsymbol{\rho}_1 = \boldsymbol{\rho}_2 = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}\cdot\frac{\boldsymbol{I}}{2}$, which means $F(|\psi\rangle, \boldsymbol{\rho}_1) = F(|\psi\rangle, \boldsymbol{\rho}_2) = 5/6$. We call its induced map $|\psi\rangle \mapsto \boldsymbol{\rho}_1$ (or $|\psi\rangle \mapsto \boldsymbol{\rho}_2$) the *universal copy*.

Tetra Measurement (TTR). Next, we introduce the tetra measurement. Recall that any measurement is defined by a positive operator-valued measure (POVM) $\{E_i\}_i$, that is, each operator E_i is positive and $\sum_i E_i = I$. We need the following four states $|\chi(00)\rangle = \cos\tilde{\theta}|0\rangle + e^{\imath\pi/4}\sin\tilde{\theta}|1\rangle$, $|\chi(01)\rangle = \cos\tilde{\theta}|0\rangle + e^{-3\imath\pi/4}\sin\tilde{\theta}|1\rangle$, $|\chi(10)\rangle = \sin\tilde{\theta}|0\rangle + e^{-\imath\pi/4}\cos\tilde{\theta}|1\rangle$, and $|\chi(11)\rangle = \sin\tilde{\theta}|0\rangle +$

$e^{3\imath\pi/4}\cos\tilde{\theta}|1\rangle$ with $\cos^2\tilde{\theta} = 1/2 + \sqrt{3}/6$, which form a tetrahedron in the Bloch sphere representation. The *tetra measurement*, denoted by TTR, is the POVM defined by $\{\frac{1}{2}|\chi(00)\rangle\langle\chi(00)|, \frac{1}{2}|\chi(01)\rangle\langle\chi(01)|, \frac{1}{2}|\chi(10)\rangle\langle\chi(10)|, \frac{1}{2}|\chi(11)\rangle\langle\chi(11)|\}$.

Group Operation (GR). In what follows, let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the bit-flip operation, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be the phase-flip operation, and $Y = XZ$. Note that the operations $\{I, X, Y, Z\}$ form the Klein four group operating on one-qubit states. The *group operation under* a two-bit string r_1r_2, denoted by $GR(\boldsymbol{\rho}, r_1r_2)$, is a transformation defined by $GR(\boldsymbol{\rho}, 00) = \boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, 01) = Z\boldsymbol{\rho}$, $GR(\boldsymbol{\rho}, 10) = X\boldsymbol{\rho}$, and $GR(\boldsymbol{\rho}, 11) = Y\boldsymbol{\rho}$. Note that we frequently use simplified expressions like $X\boldsymbol{\rho}$ instead of $X\boldsymbol{\rho}X^\dagger$.

3D Bell Measurement (BM). Moreover, for recovering $|\psi_2\rangle$ at node t_2 we introduce another new operation based on the Bell measurement, $BM(\mathcal{Q}, \mathcal{Q}')$ (or $BM(\boldsymbol{\sigma})$), which applies the following three operations (a), (b), and (c) with probability 1/3 for each, to the state $\boldsymbol{\sigma}$ (a 4×4 density matrix) of the two-qubit system $\mathcal{Q} \otimes \mathcal{Q}'$.

(a) Measure $\boldsymbol{\sigma}$ in the Bell basis

$$\left\{|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, |\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}\right\},$$

and output $|0\rangle$ if the measurement result for $|\Phi^+\rangle$ or $|\Phi^-\rangle$ is obtained, and $|1\rangle$ otherwise.

(b) Measure $\boldsymbol{\sigma}$ similarly, and output $|+\rangle$ if the measurement result for $|\Phi^+\rangle$ or $|\Psi^+\rangle$ is obtained, and $|-\rangle$ otherwise.

(c) Measure $\boldsymbol{\sigma}$ similarly, and output $|+'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \imath|1\rangle)$ if the measurement result for $|\Phi^+\rangle$ or $|\Psi^-\rangle$ is obtained, and $|-'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \imath|1\rangle)$ otherwise.

2.3 Protocol XQQ and Its Performance Analysis

Now here is the formal description of our protocol.

Protocol XQQ: Input $|\psi_1\rangle$ at s_1, and $|\psi_2\rangle$ at s_2; Output $\boldsymbol{\rho}^1_{out}$ at t_1, and $\boldsymbol{\rho}^2_{out}$ at t_2.

Step 1. $(\mathcal{Q}_1, \mathcal{Q}_2) = UC(|\psi_1\rangle)$ at s_1, and $(\mathcal{Q}_3, \mathcal{Q}_4) = UC(|\psi_2\rangle)$ at s_2.

Step 2. $\mathcal{Q}_5 = GR(\mathcal{Q}_2, TTR(\mathcal{Q}_3))$ at s_0.

Step 3. $(\mathcal{Q}_6, \mathcal{Q}_7) = UC(\mathcal{Q}_5)$ at t_0.

Step 4 (Decoding at node t_1 and t_2). $\boldsymbol{\rho}^1_{out} = GR(\mathcal{Q}_7, TTR(\mathcal{Q}_4))$, and $\boldsymbol{\rho}^2_{out} = BM(\mathcal{Q}_1, \mathcal{Q}_6)$.

We give the proof of Theorem 1 by analyzing protocol XQQ. For this purpose, we introduce the notion of shrinking maps (also known as a depolarizing channel [24]), which plays an important role in the following analysis of XQQ: Let $\boldsymbol{\rho}$ be any quantum state. Then, if a map C transforms $\boldsymbol{\rho}$ to $p \cdot \boldsymbol{\rho} + (1-p)\frac{\boldsymbol{I}}{2}$ for some

$0 \le p \le 1$, then C is said to be *p-shrinking*. The following three lemmas are immediate:

Lemma 1. *If C is p-shrinking and C' is p'-shrinking, then $C \circ C'$ is pp'-shrinking.*

Lemma 2. *If C is p-shrinking, $F(\boldsymbol{\rho}, C(\boldsymbol{\rho})) \ge 1/2 + p/2$ for any state $\boldsymbol{\rho}$.*

Lemma 3. *The universal copy is $2/3$-shrinking.*

Computing the Fidelity at Node t_1. We first investigate the quality of the path from s_1 to t_1. Fix $\boldsymbol{\rho}_2 = |\psi_2\rangle\langle\psi_2|$ as an arbitrary state at node s_2 and consider four maps C_1: $|\psi_1\rangle \to \mathcal{Q}_2$, $C_2[\boldsymbol{\rho}_2]$: $\mathcal{Q}_2 \to \mathcal{Q}_5$, C_3: $\mathcal{Q}_5 \to \mathcal{Q}_7$ and $C_4[\boldsymbol{\rho}_2]$: $\mathcal{Q}_7 \to \boldsymbol{\rho}^1_{out}$. We wish to compute the composite map $C_{s_1t_1} = C_4[\boldsymbol{\rho}_2] \circ C_3 \circ C_2[\boldsymbol{\rho}_2] \circ C_1$ and its fidelity. We need two more lemmas before the final one (Lemma 6).

Lemma 4. *$C_3 \circ C_2[\boldsymbol{\rho}_2] = C_2[\boldsymbol{\rho}_2] \circ C_3$.*

Lemma 5. *(Main Lemma) $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$ is $\frac{1}{9}$-shrinking. (See below for the proof.)*

Lemma 6. *For any $|\psi_1\rangle$, $F(|\psi_1\rangle, C_{s_1t_1}(|\psi_1\rangle)) \ge 1/2 + 2/81$.*

Proof. By Lemma 4, $C_{s_1t_1} = C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2] \circ C_3 \circ C_1$. C_3 and C_1 are both 2/3-shrinking by Lemma 3 and $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$ is $\frac{1}{9}$-shrinking by Lemma 5. It then follows that $C_{s_1t_1}$ is $\frac{4}{81}$-shrinking by Lemma 1 and its fidelity is at least $1/2 + 2/81$ by Lemma 2.

Proof of Lemma 5. See Fig. 5 again. Since we are discussing $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2]$, let $\boldsymbol{\rho}_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the state on $\mathcal{Q}_2$, $\boldsymbol{\rho}_2 = |\psi_2\rangle\langle\psi_2| = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be the state at s_2 and assume that $\mathcal{Q}_5 = \mathcal{Q}_7$. We calculate the state on $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$, the state on $\mathcal{Q}_5 \otimes \mathcal{Q}_4$ ($= \mathcal{Q}_7 \otimes \mathcal{Q}_4$) and $\boldsymbol{\rho}^1_{out}$ in this order. For $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$, recall that $\boldsymbol{\rho}_2$ is cloned into $\mathcal{Q}_3$ and $\mathcal{Q}_4$ and so, by Eq.(1) in Sec. 2.2, the state on $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$ is written as

$$\begin{aligned}
&\boldsymbol{\rho}_1 \otimes |0\rangle\langle 0| \otimes \left(\frac{2e}{3}|0\rangle\langle 0| + \frac{f}{3}|0\rangle\langle 1| + \frac{g}{3}|1\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1| \right) \\
&+ \boldsymbol{\rho}_1 \otimes |0\rangle\langle 1| \otimes \left(\frac{1}{6}|1\rangle\langle 0| + \frac{f}{3}\boldsymbol{I} \right) + \boldsymbol{\rho}_1 \otimes |1\rangle\langle 0| \otimes \left(\frac{1}{6}|0\rangle\langle 1| + \frac{g}{3}\boldsymbol{I} \right) \\
&+ \boldsymbol{\rho}_1 \otimes |1\rangle\langle 1| \otimes \left(\frac{1}{6}|0\rangle\langle 0| + \frac{f}{3}|0\rangle\langle 1| + \frac{g}{3}|1\rangle\langle 0| + \frac{2h}{3}|1\rangle\langle 1| \right). \qquad (2)
\end{aligned}$$

Then, we apply the group operation to the first two bits of $\mathcal{Q}_2 \otimes \mathcal{Q}_3 \otimes \mathcal{Q}_4$. In general, for $\mathcal{Q} \otimes \mathcal{Q}'$, $GR(\mathcal{Q}, TTR(\mathcal{Q}'))$ is given as follows.

Lemma 7. *Let $\boldsymbol{\rho}$ be the state on $\mathcal{Q}$. Then, $GR(\mathcal{Q}, TTR(\mathcal{Q}'))$ is the following TP-CP map:*

$$\begin{aligned}
\boldsymbol{\rho}\otimes|0\rangle\langle 0| &\mapsto \frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho} + \left(1-\frac{1}{\sqrt{3}}\right)\cdot\frac{\boldsymbol{I}}{2},\\
\boldsymbol{\rho}\otimes|0\rangle\langle 1| &\mapsto \frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} + \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})),\\
\boldsymbol{\rho}\otimes|1\rangle\langle 0| &\mapsto \frac{1}{2\sqrt{3}}(V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} - \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})),\\
\boldsymbol{\rho}\otimes|1\rangle\langle 1| &\mapsto \frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho} + \left(1-\frac{1}{\sqrt{3}}\right)\cdot\frac{\boldsymbol{I}}{2}.
\end{aligned}$$

Here, $V(I,Z)\boldsymbol{\rho} = \frac{1}{2}(I\boldsymbol{\rho}+Z\boldsymbol{\rho})$, and $V(X,Y)\boldsymbol{\rho}$, $V(I,X)\boldsymbol{\rho}$, $V(Y,Z)\boldsymbol{\rho}$, $V(I,Y)\boldsymbol{\rho}$, and $V(Z,X)\boldsymbol{\rho}$ are similarly defined. Those six operations are $\boldsymbol{I}$-invariant (meaning it maps $\boldsymbol{I}$ to itself) TP-CP maps.

Now the state on $\mathcal{Q}_5\otimes\mathcal{Q}_4$ is obtained by applying Lemma 7 to Eq.(2). From now on, we omit the term for $\frac{\boldsymbol{I}}{2}$. Namely, if the one-qubit state is $\boldsymbol{\rho}+\alpha\frac{\boldsymbol{I}}{2}$, we only describe $\boldsymbol{\rho}$. This is not harmful since any operation in this section is $\boldsymbol{I}$-invariant and hence the $\frac{\boldsymbol{I}}{2}$ term can be recovered at the end by using the trace property. Thus, the state on $\mathcal{Q}_5\otimes\mathcal{Q}_4$ looks like

$$\begin{aligned}
&\frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho}_1\otimes\left(\frac{2e}{3}|0\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1|\right) + \frac{1}{\sqrt{3}}V(I,Z)\boldsymbol{\rho}_1\otimes\left(\frac{f}{3}|0\rangle\langle 1| + \frac{g}{3}|1\rangle\langle 0|\right)\\
&+\frac{1}{2\sqrt{3}}V(I,X;I,Y;+)\boldsymbol{\rho}_1\otimes\frac{1}{6}|1\rangle\langle 0| + \frac{1}{2\sqrt{3}}V(I,X;I,Y;+)\otimes\frac{f}{3}\boldsymbol{I}\\
&+\frac{1}{2\sqrt{3}}V(I,X;I,Y;-)\boldsymbol{\rho}_1\otimes\frac{1}{6}|0\rangle\langle 1| + \frac{1}{2\sqrt{3}}V(I,X;I,Y;-)\otimes\frac{g}{3}\boldsymbol{I}\\
&+\frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho}_1\otimes\left(\frac{1}{6}|0\rangle\langle 0| + \frac{2h}{3}|1\rangle\langle 1|\right) + \frac{1}{\sqrt{3}}V(X,Y)\boldsymbol{\rho}_1\otimes\left(\frac{f}{3}|0\rangle\langle 1| + \frac{g}{3}|1\rangle\langle 0|\right),
\end{aligned} \tag{3}$$

where $V(I,X;I,Y;\pm)\boldsymbol{\rho} = V(I,X)\boldsymbol{\rho} - V(Y,Z)\boldsymbol{\rho} \pm \imath(V(I,Y)\boldsymbol{\rho} - V(Z,X)\boldsymbol{\rho})$, and the terms such that the state of $\mathcal{Q}_5$ is $\frac{\boldsymbol{I}}{2}$ are omitted.

We next transform the state of $\mathcal{Q}_5\otimes\mathcal{Q}_4$ to $\boldsymbol{\rho}^1_{out}$ by using Lemma 7 again. For example, $V(I,Z)\boldsymbol{\rho}_1\otimes|0\rangle\langle 0|$ is transformed to $\frac{1}{\sqrt{3}}V(I,Z)V(I,Z)\boldsymbol{\rho}_1$. To simplify the resulting formula, the following lemma is used.

Lemma 8. *1) $V(I,Z)V(I,Z)\boldsymbol{\rho}_1 = V(X,Y)V(X,Y)\boldsymbol{\rho}_1 = \begin{pmatrix} a & 0\\ 0 & d\end{pmatrix}$.*

2) $V(I,Z)V(X,Y)\boldsymbol{\rho}_1 = V(X,Y)V(I,Z)\boldsymbol{\rho}_1 = \begin{pmatrix} d & 0\\ 0 & a\end{pmatrix}$.

3) $V(I,X)V(I,X)\boldsymbol{\rho}_1 = V(Y,Z)V(Y,Z)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{b+c}{2}\\ \frac{b+c}{2} & \frac{1}{2}\end{pmatrix}$.

4) $V(I,X)V(Y,Z)\boldsymbol{\rho}_1 = V(Y,Z)V(I,X)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & -\frac{b+c}{2}\\ -\frac{b+c}{2} & \frac{1}{2}\end{pmatrix}$.

5) $V(I,Y)V(I,Y)\boldsymbol{\rho}_1 = V(Z,X)V(Z,X)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{1}{2} \end{pmatrix}$.

6) $V(I,Y)V(Z,X)\boldsymbol{\rho}_1 = V(Z,X)V(I,Y)\boldsymbol{\rho}_1 = \begin{pmatrix} \frac{1}{2} & \frac{c-b}{2} \\ \frac{b-c}{2} & \frac{1}{2} \end{pmatrix}$.

7) For any two operators V, V' *taken from any different two sets of* $\{V(I,Z), V(X,Y)\}$, $\{V(I,X), V(Y,Z)\}$, *and* $\{V(I,Y), V(Z,X)\}$, $VV'\boldsymbol{\rho}_1 = \frac{\boldsymbol{I}}{2}$.

Now it is a routine calculation to obtain $\boldsymbol{\rho}^1_{out} = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$ where m_1 through m_4 are equations using a, b, c and d (e, f, g and h disappear). Using the fact that $a + d = 1$, we have $\boldsymbol{\rho}^1_{out} = \frac{1}{9}\boldsymbol{\rho}_1 + \frac{1}{9}\boldsymbol{I}$. Recovering the completely mixed state omitted in our analysis, we obtain $C_4[\boldsymbol{\rho}_2] \circ C_2[\boldsymbol{\rho}_2](\boldsymbol{\rho}_1) = \frac{1}{9}\boldsymbol{\rho}_1 + \frac{8}{9} \cdot \frac{\boldsymbol{I}}{2}$. Thus, the map is $\frac{1}{9}$-shrinking. □

Computing the Fidelity at Node t_2. By analyzing the quality of the path from s_2 to t_2, we have $F(|\psi_2\rangle, \boldsymbol{\rho}^2_{out}) \geq 1/2 + 2\sqrt{3}/243$. Its analysis is different from the previous one, but the notion of shrinking maps also make the analysis easier. Here, we omit the analysis.

2.4 Upper Bounds

The next theorem shows a general upper bound for the fidelity of two crossing qubits over Butterfly. The proof technique is similar to Theorem 5 of the next section.

Theorem 2. *Let q be the fidelity of a protocol for sending two qubits simultaneously. Then, $q < 0.983$.*

Recall that the Butterfly network has links from s_1 to t_2 and s_2 to t_1. They are not on the path from s_1 to t_1 or from s_2 to t_2, but do play an important role. The natural question is how worse the performance becomes if we remove those two links. For this question, we obtain the following result, which means that the two side links are indispensable.

Theorem 3. *Any quantum protocol cannot achieve fidelity larger than* $1/2$ *if both side links are removed from the Butterfly.*

3 Natural Protocols and Their Upper Bounds

In this section, we design a protocol, XQC (crossing a quantum and a classical bits), which assumes that the state at s_2 is only $|0\rangle$ or $|1\rangle$. Before that, however, we introduce the notion of natural protocols. Recall that the Butterfly network has three nodes s_1, s_2 and t_0, where we need some kind of quantum cloning $g(|\phi\rangle)$ to send the information nicely to their two outgoing edges. Let Φ be a set of quantum states. Then g is optimal for Φ if for any g' and $i = 1, 2$ the following condition holds: If $F(\mathrm{Tr}_i g(|\psi\rangle), |\psi\rangle) < F(\mathrm{Tr}_i g'(|\psi\rangle), |\psi\rangle)$ for some $|\psi\rangle \in \Phi$, there

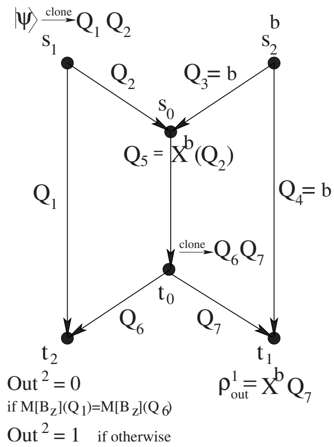

Fig. 6. Protocol XQC

is a $|\psi'\rangle$ such that $F(\mathrm{Tr}_{\bar{i}}g(|\psi'\rangle), |\psi'\rangle) > F(\mathrm{Tr}_{\bar{i}}g'(|\psi'\rangle), |\psi'\rangle)$, where $\bar{i} = 2$ if $i = 1$ and vice versa. If all clonings at s_1, s_2 and t_0 are optimal, then the protocol is called *natural*. If Φ is the set of one-qubit states, then UC is optimal. So, XQQ is natural. If Φ consists of all equatorial states (single qubits whose amplitudes are real), then the so-called phase-covariant cloning [9,13] is optimal (see Sec. 4).

We next consider the case that Φ consists of only two states $|0\rangle$ and $|1\rangle$. Under this condition, the following map, say *simple copy* or SC, is obviously optimal: $SC(|0\rangle) = |00\rangle$ and $SC(|1\rangle) = |11\rangle$. This means that if the state b at s_2 must be in $\{|0\rangle, |1\rangle\}$, any natural protocol is to send this classical bit b to both s_0 and t_1 as it is. Of course there is no nontrivial entanglement between those two nodes. Note also that the fidelity at node t_2 equals to the probability that b can be recovered successfully at t_2. Now our natural XQC protocol is summarized as in Fig. 6, where $M[B_z](\mathcal{Q})$ means that $\mathcal{Q}$ is measured in the basis $B_z = \{|0\rangle, |1\rangle\}$. (A similar notation is also used for the basis $B_x = \{|+\rangle, |-\rangle\}$ in Fig. 8.) Thanks to the restriction, its fidelity is much better than XQQ.

Theorem 4. *XQC achieves the fidelities of $13/18$ and $11/18$ at t_1 and t_2. (By averaging the fidelities at both sinks as before, we can have the same fidelity $2/3$, also.)*

Upper Bound for Natural Protocols. If we restrict ourselves to natural protocols, then we can obtain the following upper bound that is significantly better than Theorem 2.

Theorem 5. *Suppose that under the restriction where one of sources is classical a natural protocol achieves fidelity p. Then, $p < 11/12$.*

Proof. Suppose that there is a natural protocol whose fidelity is $1-\epsilon$, and we wish to show $\epsilon > 1/12$. Here, we give the desired upper bound for the case that the capacity of the link from s_1 to t_2 is unlimited. In this case we can assume that the state sent from s_1 is pure. Let $|\psi\rangle$ and b be the inputs at nodes s_1 and s_2, respectively. By the Schmidt decomposition (see [24]), the state after the operation at s_1 is written as $|\xi\rangle = \alpha|\psi_2\rangle|\psi_1\rangle + \beta|\psi_2^\perp\rangle|\psi_1^\perp\rangle$ where $|\psi_1\rangle$ and $|\psi_1^\perp\rangle$ are single-qubit orthonormal states on the link to s_0 and $|\psi_2\rangle$ and $|\psi_2^\perp\rangle$ are the remaining (possibly multi-qubit) orthonormal states on the link to t_2. Note that α, β, $|\psi_2\rangle$ and $|\psi_1\rangle$ depend on the input $|\psi\rangle$ at s_1. Without loss of generality, we assume $|\alpha| \geq |\beta|$ (and hence $|\beta|^2 \leq 1/2$).

We first investigate the fidelity on the path from s_1 to t_1, which is done by the following sequence of definitions and observations: (i) By the above definition of $|\xi\rangle$, we can write the state on $\mathcal{Q}_2$ (where we use the notations in Fig. 6 again) as $\boldsymbol{\rho} = |\alpha|^2|\psi_1\rangle\langle\psi_1| + |\beta|^2|\psi_1^\perp\rangle\langle\psi_1^\perp|$. (ii) Intuitively, the value of $|\beta|$ shows the strength of entanglement between $\mathcal{Q}_1$ and $\mathcal{Q}_2$; if it is large then the distortion of $\boldsymbol{\rho}$ compared to the original $|\xi\rangle$ must also be large. In other words, β must be small to obtain a small ϵ. (iii) For $b = 0$ and 1, let $C_b : \mathcal{Q}_2 \to \mathcal{Q}_5$ be the TP-CP map at s_0. Let C'_b be its equivalent 3×3 real matrix for Bloch-sphere states. Namely, C'_b maps a Bloch vector $\boldsymbol{r}$ to $O_b^1 \Lambda_b O_b^2 \boldsymbol{r} + \boldsymbol{d}_b$, where O_b^1 and O_b^2 are orthogonal matrices, and Λ_b is a diagonal matrix. (iv) Let U'_b be the map that transforms $\boldsymbol{r}$ to $O_b^1 O_b^2 \boldsymbol{r}$. Then, we can define the map U_b such that its Bloch-sphere equivalence is U'_b. Note that U_b is unitary. (v) Let k_b be the distance between the images of the Bloch sphere by C'_b and U'_b. Note that $||(C_b - U_b)|\phi\rangle\langle\phi|||_{tr} \leq k_b$ for an arbitrary pure state $|\phi\rangle$ (where the trace norm $||\cdot||_{tr}$ is defined by $||A||_{tr} = \sqrt{AA^\dagger}$). By a similar reason as (ii) k_b must be small for a small ϵ. (vi) Now we select the state $\boldsymbol{\rho}$ which is undesirable to achieve a high fidelity, i.e., the one such that $U_0\boldsymbol{\rho} = U_1\boldsymbol{\rho}$ (such $\boldsymbol{\rho}$ exists, which is parallel to the eigenvector of $U_0^{-1}U_1$). Let $\boldsymbol{\rho'} = |\alpha|^2|\psi_1\rangle\langle\psi_1|$, which is an approximation of $\boldsymbol{\rho}$ represented as a product state. (vii) The operation at t_0 is considered to be the two TP-CP maps on the one qubits: One map CP_1 is for t_1 and the other CP_2 is for t_2. Their Bloch-sphere equivalence CP'_1 and CP'_2 have a trade-off on the size of their images. So, the image of CP'_1 must be large for a small ϵ, and then we have a shrinking factor for CP'_2.

Now we are ready to bound both above and below $||(C_0 - C_1)\boldsymbol{\rho'}||_{tr}$, which produces an inequality on ϵ as will be seen soon. For this purpose, we first evaluate the values of β and k_b using geometric properties of the Bloch sphere representation of the TP-CP map on the one qubits: it maps the Bloch sphere (the three dimensional sphere with unit radius) to an ellipsoid within the Bloch sphere. (See [14] for the formal description and more precise characterization of the map.)

Lemma 9. $|\beta|^2 \leq \frac{1}{2}f(\epsilon)$ *and* $k_b \leq f(\epsilon)$ *where*

$$f(\epsilon) = \frac{3}{2} + \epsilon - \sqrt{\frac{9}{4} + \epsilon^2 - 5\epsilon}.$$

$$
\begin{array}{c}
C_0\rho' \approx U_0\rho' \approx U_0\rho \\
\| \\
C_1\rho' \approx U_1\rho' \approx U_1\rho
\end{array}
$$

Fig. 7. Diagram on the closeness between $C_0\boldsymbol{\rho'}$ and $C_1\boldsymbol{\rho'}$

Second, we decompose $||(C_0 - C_1)\boldsymbol{\rho'}||_{tr}$ as follows by the triangle inequality (see Fig. 7), and then bound it from above:

$$
\begin{aligned}
&||(C_0 - C_1)\boldsymbol{\rho'}||_{tr} \\
&\leq ||(C_0 - U_0)\boldsymbol{\rho'}||_{tr} + ||U_0\boldsymbol{\rho'} - U_0\boldsymbol{\rho}||_{tr} + ||U_1\boldsymbol{\rho} - U_1\boldsymbol{\rho'}||_{tr} + ||(U_1 - C_1)\boldsymbol{\rho'}||_{tr} \\
&\leq |\alpha|^2 \cdot k_0 + ||\boldsymbol{\rho} - \boldsymbol{\rho'}||_{tr} \times 2 + |\alpha|^2 \cdot k_1 \\
&\leq (k_0 + k_1)|\alpha|^2 + 2|\beta|^2. \qquad (4)
\end{aligned}
$$

Third, for the shrinking factor by the operation at t_0 the following lemma from [25] is used.

Lemma 10. *(Niu-Griffiths) Let CP_i' be the Bloch sphere representation of CP_i. Let l_1 be the shortest semiaxis length of the image of CP_1', and l_2 be the longest semiaxis length of the image of CP_2'. Then, $l_1 \leq \sqrt{1 - l_2^2}$.*

Since $l_1 \geq 1 - 2\epsilon$ by the fidelity requirement at t_1, Lemma 10 gives us the condition for l_2:

$$l_2 \leq 2\sqrt{\epsilon - \epsilon^2}. \qquad (5)$$

Finally, we bound $||(C_0 - C_1)\boldsymbol{\rho'}||_{tr}$ from below by focusing on the path s_2-t_2. Let M be the TP-CP map done at t_2, and $D = M(I \otimes CP_2)(I \otimes C_0 - I \otimes C_1)$. By the fidelity requirement at t_2, $||D|\xi\rangle\langle\xi|||_{tr} \geq 2 - 4\epsilon$ [2]. On the contrary, using the unnormalized product state $|\chi\rangle = \alpha|\psi_2\rangle|\psi_1\rangle$ we bound $||D|\xi\rangle\langle\xi|||_{tr}$ by

$$||D|\xi\rangle\langle\xi|||_{tr} \leq ||D(|\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|)||_{tr} + ||D|\chi\rangle\langle\chi|||_{tr}.$$

The first term is bounded by $2|||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|||_{tr}$ since D is the difference between two TP-CP maps, each of which has the operator norm at most 1 [2]. Using the monotone decreasing property of the trace distance between two states by TP-CP maps, the second term is bounded by

$$||D|\chi\rangle\langle\chi|||_{tr} \leq ||(I \otimes (CP_2 \cdot (C_0 - C_1)))|\psi_2\rangle\langle\psi_2| \otimes \boldsymbol{\rho'}||_{tr} = ||(CP_2 \cdot (C_0 - C_1))\boldsymbol{\rho'}||_{tr},$$

which is at most $l_2||(C_0 - C_1)\boldsymbol{\rho'}||_{tr}$ since CP_2' maps the Bloch sphere to an ellipsoid within a sphere with radius at most l_2. By a simple calculation of the trace norm, we have the following bound.

Lemma 11. $|||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|||_{tr} \leq 2|\beta|\sqrt{1 - |\beta|^2/2}$.

By Lemma 11 we have

$$2 - 4\epsilon \leq 2|||\xi\rangle\langle\xi| - |\chi\rangle\langle\chi|||_{tr} + l_2||(C_0 - C_1)\boldsymbol{\rho'}||_{tr} \leq 2|\beta|\sqrt{1 - |\beta|^2/2} + l_2||(C_0 - C_1)\boldsymbol{\rho'}||_{tr}. \qquad (6)$$

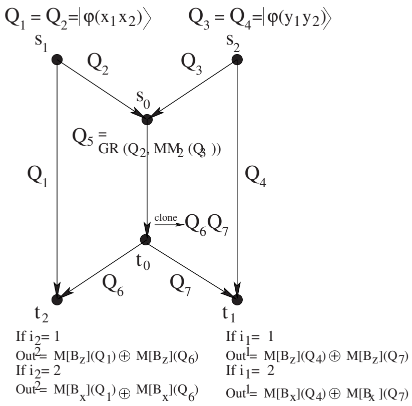

Fig. 8. Protocol $X2C2C$

By Lemma 9, Ineqs.(4), (5) and (6)

$$1 - 2\epsilon \leq 2|\beta|\sqrt{1-|\beta|^2/2} + 2\sqrt{\epsilon-\epsilon^2}\left((1-|\beta|^2)f(\epsilon) + |\beta|^2\right). \tag{7}$$

(Recall that $|\alpha|^2 = 1 - |\beta|^2$.) Note that the right-hand side of Ineq. (7) is monotone increasing on ϵ and $|\beta|$ while its left-hand side is monotone decreasing on ϵ. Therefore, by checking ϵ such that Ineq. (7) holds under the bound of $|\beta|$ from Lemma 9, we obtain $\epsilon > 1/12$.

4 Protocols for Crossing Two Multiple Bits

Protocol $X2C2C$. Consider the case that both sources are restricted to be one of the four $(2, 1, 0.85)$-quantum random access (QRA) coding states [4], where (m, n, p)-QRA coding is the coding of m bits to n qubits such that any one bit chosen from the m bits is recovered with probability at least p. In this case, we can achieve a much better fidelity. As an application, we can consider a more interesting problem where each source node receives two classical bits, namely, $x_1x_2 \in \{0,1\}^2$ at s_1, and $y_1y_2 \in \{0,1\}^2$ at s_2. At node t_1, we output one classical bit Out^1 and similarly Out^2 at t_2. Now an adversary chooses two numbers $i_1, i_2 \in \{1, 2\}$. Our protocol can use the information of i_1 only at node t_1 and that of i_2 only at t_2. Our goal is to maximize $F(x_{i_1}, \mathrm{Out}^1)$ and $F(y_{i_2}, \mathrm{Out}^2)$, where $F(x_{i_1}, \mathrm{Out}^1)$ turns out to be the probability that $x_{i_1} = \mathrm{Out}^1$ and similarly for $F(y_{i_2}, \mathrm{Out}^2)$. Fig. 8 illustrates $X2C2C$ whose key is also how to encode at s_0: we use a measurement MM_2, called the 2D measurement, and the group operation similar to XQQ. Moreover, we use the phase-covariant cloning for the optimal cloning at t_0.

Theorem 6. *$X2C2C$ achieves a fidelity of $1/2 + \sqrt{2}/16$ at both t_1 and t_2.*

By contrast, any classical protocol cannot achieve a success probability greater than $1/2$ for the following reason: Let fix $y_1 = y_2 = 0$. Then the path from s_1 to t_1 is obviously equivalent to the $(2, 1, p)$-classical random access coding, where the success probability p is at most $1/2$ [4].

Furthermore, we can solve the above problem with probability $> 1/2$ for the case that each source node receives three bits ($X3C3C$). This is constructed by extending techniques of $X2C2C$: from the $(2, 1, 0.85)$-QRA coding, the 2D measurement, and group operation to the $(3, 1, 0.79)$-QRA coding, the 3D measurement, and the approximated group operation.

Theorem 7. *$X3C3C$ achieves a fidelity of $1/2 + 2/81$ at both sinks.*

Interestingly, there is no $X4C4C$, which is an immediate corollary of the nonexistence of $(4, 1, p)$-QRA coding such that $p > 1/2$ [19].

Theorem 8. *If an $X4C4C$ protocol achieves fidelity q, then $q \leq 1/2$.*

5 Beyond the Butterfly Network – Concluding Remarks –

Obviously a lot of future work remains. First of all, there is a large gap between the current upper and lower bounds for the achievable fidelity, which should be narrowed. Equally important is to consider more general networks. To this direction, it might be interesting to study the network G_k as shown in Fig. 9, introduced in [17]. Note that there are k source-sink pairs (s_i, t_i) all of which share a single link from s_0 to t_0. For this network G_k, we can design the protocol XQ^k by a simple extension of XQQ. The idea is to decompose the node s_0 (similarly for t_0) into a sequence of nodes of indegree two. At each of those nodes, we do exactly the same thing as before, i.e., encoding one state by the classical two bits obtained from the other state. It is not hard to see that such a protocol achieves a fidelity strictly better than $1/2$. A similar extension is also possible for the recursively constructed network based on the Butterfly network in [1].

References

1. M. Adler, N. J. Harvey, K. Jain, R. D. Kleinberg, and A. R. Lehman. On the capacity of information networks. *Proc. 17th ACM-SIAM SODA*, pp.241–250, 2006.
2. D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *Proc. 30th ACM STOC*, pp. 20–30, 1998.
3. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory* **46** (2000) 1204–1216.
4. A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM* **49** (2002) 496–511.

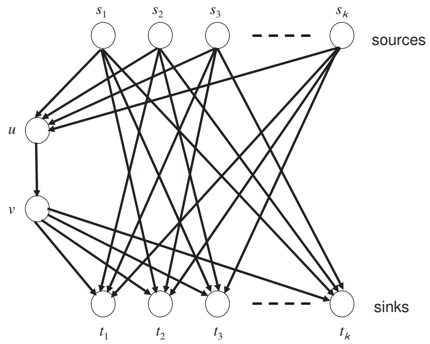

Fig. 9. Network G_k

5. C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.
6. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum states via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70** (1993) 1895–1899.
7. C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69** (1992) 2881–2884.
8. D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Phys. Rev. A* **57** (1998) 2368–2378.
9. D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello. Phase-covariant quantum cloning. *Phys. Rev. A* **62** (2000) 012302.
10. H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.* **87** (2001) 167902.
11. V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A* **54** (1996) 1844–1852.
12. V. Bužek, M. Hillery, and R. F. Werner. Optimal manipulation with qubits: universal NOT gate. *Phys. Rev. A* **60** (1999) 2626–2629.
13. H. Fan, K. Matsumoto, X.-B. Wang, and H. Imai. Phase-covariant quantum cloning. *J. Phys. A: Math. Gen.* **35** (2002) 7415–7423.
14. A. Fujiwara and P. Algoet. One-to-one parametrization of quantum channels. *Phys. Rev. A* **59** (1999) 3290–3294.
15. N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.* **79** (1997) 2153–2156.
16. N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Phys. Rev. Lett.* **83** (1999) 432–435.
17. N. J. Harvey, R. D. Kleinberg, and A. R. Lehman. Comparing network coding with multicommodity flow for the k-pairs communication problem. MIT LCS Technical Report 964, September 2004.
18. N. J. Harvey, D. R. Karger, and K. Murota. Deterministic network coding by matrix completion. *Proc. 16th ACM-SIAM SODA*, pp. 489–498, 2005.

19. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. $(4,1)$-quantum random access coding does not exist. Preprint available at http://arxiv.org/quant-ph/0604061, April 2006.
20. S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, L. M. G. M. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory* **51** (2005) 1973–1982.
21. I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *J. Comput. Syst. Sci.* **69** (2004) 395–420.
22. A. R. Lehman and E. Lehman. Complexity classification of network information flow problems. *Proc. 15th ACM-SIAM SODA*, pp. 142–150, 2004.
23. A. R. Lehman and E. Lehman. Network coding: does the model need tuning? *Proc. 16th ACM-SIAM SODA*, pp. 499–504, 2005.
24. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*, Cambridge, 2000.
25. C.-S. Niu and R. B. Griffiths. Optimal copying of one quantum bit. *Phys. Rev. A* **58** (1998) 4377–4393.
26. A. K. Pati and S. L. Braunstein. Impossibility of deleting an unknown quantum state. *Nature* **404** (2000) 164–165.
27. B. Schumacher. Quantum coding. *Phys. Rev. A* **51** (1995) 2738–2747.
28. P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52** (1995) 2493–2496.
29. W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature* **299** (1982) 802–803.