Broadcast Classical-Quantum Capacity Region of Two-Phase Bidirectional Relaying Channel

Holger Boche, Minglai Cai, Christian Deppe

January 22, 2014

Abstract

We study a three-node quantum network which enables bidirectional communication between two nodes with a half-duplex relay node, the classical version of which has been introduced in [13]. A decode-and-forward protocol is used to perform the communication in two phases. In the first phase, the messages of two nodes are transmitted to the relay node. In the second phase, the relay node broadcasts a re-encoded composition to the two nodes. We determine the capacity region of the broadcast phase.

1 Introduction

The study of quantum channels networks has become more and more important in the last few years. In this paper we analyze a quantum channel network model which was introduced by Oechtering, Schnurr, Bjelaković, and Boche in [13] for a classical channels network. It is called the two-phase bidirectional relaying channel (Figure 1). In this model we consider a three-node quantum network with two message sets $M_1$ and $M_2$, which is called a two-user bidirectional quantum channel. The message $m_2 \in M_2$ is located at node 1, and the message $m_1 \in M_1$ is located at node 2, respectively, while a relay node enables the bidirectional communication between two other nodes. Our goal is that after the transmission the message $m_2 \in M_2$ is known at node 2, and the message $m_1 \in M_1$ is known at node 1, respectively. We simplify the problem by assuming an a priori separation of the communication into two phases. The relay node’s task is to decoding the messages which it receives in the first phase and forwards the information to its destinations in the second phase. Thus we assume that $M_1$ and $M_2$ are classical message sets due to the No-Cloning Theorem (cf. [18]).

Considering the capacity of quantum channels carrying classical information is equivalent to considering the capacity of classical-quantum channels, where a classical-quantum channel is a quantum channel whose sender’s inputs are classical variables. The capacity of classical-quantum channels has been determined in [8], [9], and [17].
Channel networks with relay nodes have been studied extensively in the context of classical information theory (cf. [10] and [5]). The study of quantum channels with relay nodes has just recently begun (cf. [16]).

With the separation of the communication we end up with a multiple access phase, where node 1 and node 2 transmit messages $m_2$ and $m_1$ to the relay node, and a broadcast phase, where the relay forwards the messages to node 2 and node 1, respectively. We look at the two phases separately.

In the multiple access phase we have a classical-quantum multiple access channel. The multiple access channel is a channel such that two (or more) senders send information to a common receiver via this channel. The optimal coding strategies and capacity regions for classical multiple access channels have been given in [2] and [11]. The optimal coding strategies and capacity regions for multiple access quantum channels have been given in [20] and [21].
In the broadcast phase we have a broadcast quantum channel. The broadcast channel is a channel such that one single sender sends information to two (or more) receivers via this channel. The optimal coding strategies and capacity regions for classical broadcast channels have been given in [12], [3], and [6]. An optimal coding strategy and a capacity region for a broadcast quantum channel has been given in [15].

For the broadcast phase we assume that the relay node has successfully decoded the messages \( m_1 \) and \( m_2 \) in the multiple access phase. Then we have a broadcast quantum channel where the message \( m_2 \) is known at node 1 and at the relay node, while the message \( m_2 \) is known at node 2 and at the relay node. The mission of the relay node is to broadcast a message to node 1 and node 2 which allows both nodes to recover the unknown source. This means that node 1 wants to recover message \( m_2 \) and node 2 wants to recover message \( m_2 \).

## 2 Basic Definitions

For finite-dimensional complex Hilbert spaces \( G \) and \( G' \) a quantum channel \( N: S(G) \to S(G') \) is represented by a positive trace preserving map which accepts input quantum states in \( S(G) \) and produces output quantum states in \( S(G') \). Here \( S(G) \) and \( S(G') \) stand for the space of density operators on \( G \) and \( G' \), respectively.

If the sender wants to transmit a classical message \( m \in M \) to the receiver using a quantum channel \( N \), his encoding procedure will include a classical-to-quantum encoder \( M \to S(G) \) to prepare a quantum message state \( \rho \in S(G) \) as an input for the channel. If the sender’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states \( \{\rho_x : x \in A\} \subset S(G) \), then we can consider the choice of the signal quantum states \( \rho_x \) as a component of the channel. Thus, we obtain a channel \( \sigma_x := N(\rho_x) \) with classical inputs \( x \in A \) and quantum outputs, which we call a classical-quantum channel. This is a map \( \mathbb{N}: A \to S(G') \), \( A \ni x \to \mathbb{N}(x) \in S(G') \) which is represented by the set of \( [A] \) possible output quantum states \( \{\sigma_x = \mathbb{N}(x) := N(\rho_x) : x \in A\} \subset S(G') \), meaning that each classical input of \( x \in A \) leads to a distinct quantum output \( \sigma_x \in S(G') \). In view of this, we have the following definition.

Let \( A \) be a finite set. Let \( H \) be a finite-dimensional complex Hilbert space. A classical-quantum channel is a map \( N: A \to S(H) \), \( A \ni a \to N(a) \in S(H) \).

For a probability distribution \( P \) on a finite set \( A \) a conditional stochastic matrix \( \Lambda \), and a positive constant \( \delta \), we denote the set of typical sequences by \( T^P_{\Lambda, \delta} \) and the set of conditionally typical sequences by \( T^P_{\Lambda, \delta}(x^n) \) (here we use the strong condition) (cf. [18]).

Let \( n \in \mathbb{N} \). For a finite set \( A \) we define \( A^n := \{(a_1, \cdots , a_n) : a_i \in A \ \forall i \in \{1, \cdots , n\}\} \). For a finite-dimensional complex Hilbert space \( H \) the space which the vectors \( \{v_1 \otimes \cdots \otimes v_n : v_i \in H \ \forall i \in \{1, \cdots , n\}\} \) span is defined by \( H^{\otimes n} \). We also write \( a^n \) and \( v^{\otimes n} \) for the elements of \( A^n \) and \( H^{\otimes n} \), respectively.

Associated to a classical quantum channel \( N: A \to S(H) \) is the channel map on the \( n \)-block \( N^{\otimes n}: A^n \to S(H^{\otimes n}) \) such that for \( a^n = (a_1, \cdots , a_n) \in A^n \) we have \( N^{\otimes n}(a^n) = N(a_1) \otimes \cdots \otimes N(a_n) \).
For a quantum state $\rho \in S(G)$ we denote the von Neumann entropy of $\rho$ by

$$S(\rho) = -\text{tr}(\rho \log \rho).$$

Let $\mathcal{V} : A \to S(G)$ be a classical-quantum channel. For $P \in P(A)$ the conditional entropy of the channel for $\mathcal{V}$ with input distribution $P$ is denote by

$$S(\mathcal{V}|P) := \sum_{x \in A} P(x) S(\mathcal{V}(x)).$$

**Remark 2.1.** The following definition is a more general definition of conditional entropy in quantum information theory. Let $\mathcal{P}$ and $\Omega$ be quantum systems. We denote the Hilbert space of $\mathcal{P}$ and $\Omega$ by $G^\mathcal{P}$ and $G^\Omega$, respectively. Let $\phi^{G^\Omega}$ be a bipartite quantum state in $S(G^\mathcal{P}G^\Omega)$. We denote $S(\mathcal{P} | \Omega)_\pi := S(\phi^{G^\mathcal{P}G^\Omega}) - S(\phi^G)$. Here $\phi^G = \text{tr}_\Omega(\phi^{G^\Omega}).$

Let $\Phi := \{\rho_x : x \in A\}$ be a set of quantum states labeled by elements of $A$. For a probability distribution $P$ on $A$ the Holevo $\chi$ quantity is defined as

$$\chi(P; \Phi) := S \left( \sum_{x \in A} P(X) \rho_x \right) - \sum_{x \in A} P(X) S(\rho_x).$$

We denote the identity operator on a space $G$ by $\text{id}_G$.

A two-user multiple access quantum channel $N_{BC-A} : H^{BC} \to H^A$ has two senders $B, C$, and a single receiver $A$. It is defined as a map $N : H^{BC} \to H^A$.

An $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information for a two-user quantum multiple access channel $N_{BC-A} : H^{BC} \to H^A$ consists of a family of vectors $\{w(m_1) : m_1 = 1, \cdots, J_n^{(1)}\} \subset S(H^B)$, vectors $\{v(m_2) : m_2 = 1, \cdots, J_n^{(2)}\} \subset S(H^C)$, and a family of semi-definite operators $\{D_{m_1,m_2} : m_1 \in \{1, \cdots, J_n^{(1)}\}, m_2 \in \{1, \cdots, J_n^{(2)}\}\}$ on $H^A$ such that $\{D_{m_1,m_2} : m_1, m_2\}$ is less or equal to the partition of the identity, i.e.

$$\sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} D_{m_1,m_2} \leq \text{id}_{H^A}. $$

**Remark 2.2.** In some literature, codes for quantum multiple access channels are defined in such a way that $\{D_{m_1,m_2} : m_1, m_2\}$, the collection of positive semi-definite operators, is equal to the partition of the identity, i.e.

$$\sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} D_{m_1,m_2} = \text{id}_{H^A}.$$ This definition is equivalent to our definition, since if $\sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} D_{m_1,m_2} < \text{id}_{H^A}$ holds we can add $\text{id}_{H^A} - \sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} D_{m_1,m_2}$ to an arbitrary operator in the set $\{D_{m_1,m_2} : m_1, m_2\}$.

A pair of non-negative numbers $(R_1, R_2)$ is an achievable secrecy rate pair with classical inputs for the quantum multiple access channel $N_{BC-A} : H^{BC} \to H^A$ with average error, if for every positive $\varepsilon$, $\delta$, and a sufficiently large $n$ there is an $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information $(\{w(m_1) : m_1 = 1, \cdots, J_n^{(1)}\}, \{v(m_2) : m_2 = 1, \cdots, J_n^{(2)}\}, \{D_{m_1,m_2} : m_1 \in \{1, \cdots, J_n^{(1)}\}, m_2 \in \{1, \cdots, J_n^{(2)}\}\})$ such that $\frac{1}{n} \log J_n^{(1)} \geq R_1 - \delta$, $\frac{1}{n} \log J_n^{(2)} \geq R_2 - \delta$ and

$$\frac{1}{J_n^{(1)} J_n^{(2)}} \sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} \text{tr}((\text{id}_{H^A} - D_{m_1,m_2})N_{BC-A}((w(m_1), v(m_2))) \leq \varepsilon. \ (1)$$
The two-user broadcast quantum channel $N_{A-BC} = (W_1, W_2) : H^A \to H^{BC}$ is a quantum channel from a single sender $A$ to two independent receivers $B$ and $C$. The quantum channel from $A$ to $B$ is obtained by tracing out $C$ from the channel map, i.e., $W_1 = N_{A-B} : H^A \to H^B$, which is the quantum channel from $A$ to $B$, is defined as $W_1(\sigma) = \text{tr}_C(N_{A-BC}(\sigma))$. Furthermore, $W_2 = N_{A-C} : H^A \to H^B$, which the quantum channel from $A$ to $C$, is defined as $W_2(\sigma) = \text{tr}_B(N_{A-BC}(\sigma))$.

An $(n, j_n^{(1)}, j_n^{(2)})$ code carrying classical information for a two-user broadcast quantum channel $(W_1, W_2) : H^A \to H^{BC}$ consists of a family of vectors $\{w((m_1, m_2)) : m_1 = 1, \ldots, j_n^{(1)}, m_2 = 1, \ldots, j_n^{(2)}\} \subset S(A^{\otimes n})$, a collection of positive semi-definite operators $\{D_{m_1}^{(1)} : m_1 \in \{1, \ldots, j_n^{(1)}\}\}$ on $H^{C^{\otimes n}}$, and a collection of positive semi-definite operators $\{D_{m_2}^{(2)} : m_2 \in \{1, \ldots, j_n^{(2)}\}\}$ on $H^{B^{\otimes n}}$. The capacity regions of multiple-access quantum channels and broadcast quantum channels are convex by the time sharing principle: let $B$ and $C$ be rate tuples of $m$ and $n$ block codes, respectively, with error probabilities $\epsilon_1$ and $\epsilon_2$, respectively. We get an $(m+n)$ block code with error probability at most $\epsilon_1 + \epsilon_2$ and with rates $\left(\frac{m}{m+n}R_1 + \frac{n}{m+n}R_1', \frac{m}{m+n}R_2 + \frac{n}{m+n}R_2'\right)$ by concatenating the codewords to $(m+n)$ blocks and tensoring the corresponding decoding observables.

3 The Classical-Quantum Capacity Region of the Bidirectional Relaying Quantum Channel

For the multiple-access phase the optimal coding strategy is well known from [20], where the following lemma for the classical-quantum rate region of multiple-access quantum channels was given.

Lemma 3.1. Let $N$ be a two-user multiple-access quantum channel. Let $H^{Y_1}$ be the Hilbert space whose unit vectors correspond to the pure states of node 1's
quantum system, $H^Y_2$ be the Hilbert space whose unit vectors correspond to the pure states of node 2’s quantum system, and $H^X$ be the Hilbert space whose unit vectors correspond to the pure states of the relay node’s quantum system.

We assume node 1’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_1 \subset H^Y_1$.

We assume node 2’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_2 \subset H^Y_2$.

The classical-quantum capacity region of the multiple-access quantum channel with average error is given by the set of all rate pairs $(R_2, R_1)$, satisfying

\[ R_2 \leq \chi(Q_1; \sigma^X) , \] (4)

\[ R_1 \leq \chi(Q_2; \sigma^X) , \] (5)

and

\[ R_2 + R_1 \leq \chi(Q_{1,2}; \sigma^X) \] (6)

for any joint probability distribution $Q_{1,2}$ on $Y_1 \times Y_2$. Here, $Q_1$ is the marginal probability distribution of $Q_{1,2}$ on $Y_1$, $Q_2$ is the marginal probability distribution of $Q_{1,2}$ on $Y_2$, and $\sigma^X$ is the resulting quantum state at the outcome of the relay node.

Thus, if $n$ is sufficiently large, and if for $M_1$ and $M_2$ it holds

\[ |M_2| \leq 2^{n(\chi(Q_1; \sigma^X) - \epsilon)} \]

\[ |M_1| \leq 2^{n(\chi(Q_2; \sigma^X) - \epsilon)} \]

and

\[ |M_2| + |M_1| \leq 2^{n(\chi(Q_{1,2}; \sigma^X) - \epsilon)} \]

for some positive $\epsilon$, we can assume the following statement for the multiple-access phase. After receiving $n$ quantum states, the relay node has successfully decoded the messages $m_1 \in M_1$ and $m_2 \in M_2$.

For the broadcast phase since node 1 already knows the message $m_2 \in M_2$, it can use this knowledge as a support for the choice of its decoding strategy to decode $m_1$. Since node 2 already knows the message $m_1 \in M_1$, it can use this knowledge as a support for the choice of its decoding strategy to decode $m_2$. In view of these facts we have the following Theorem 3.2.

**Theorem 3.2.** Let $N$ be a two-user bidirectional quantum channel. Let $H^Y_1$ be the Hilbert space whose unit vectors correspond to the pure states of node 1’s quantum system, $H^Y_2$ be the Hilbert space whose unit vectors correspond to the pure states of node 2’s quantum system, and $H^X$ be the Hilbert space whose unit vectors correspond to the pure states of the relay node’s quantum system. Let $N_{X-Y_1Y_2} = (W_1, W_2)$ be the broadcast quantum channel in the broadcast phase.

We assume that the relay node’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $\{\phi_x : x \in X\} \subset H^X$.

For all probability distribution $P$ on $X$ the capacity region of the bidirectional broadcast quantum channel during the broadcast phase for transmitting classical
information with average error is given by the set of all rate pairs \((R_1, R_2)\), satisfying
\[
R_1 \leq \limsup_{n \to \infty} \chi(P^n; \sigma^{Y_1 \otimes n})
\]  
(7)
and
\[
R_2 \leq \limsup_{n \to \infty} \chi(P^n; \sigma^{Y_2 \otimes n}) .
\]  
(8)
Here, \(\sigma^{Y_1}\) is the resulting quantum state at the outcome of node 1, while \(\sigma^{Y_2}\) is the resulting quantum state at the outcome of node 2.

Proof. It is easy to verify that every achievable rate pair cannot exceed \(\frac{7}{2}\) and \(\frac{8}{2}\). \(R_1\) cannot exceed \(\limsup_{n \to \infty} \chi(P^n; \sigma^{Y_1 \otimes n})\) (cf. \(\frac{9}{2}\)), even if the relay node only sends a message to node 1 without sending any message to node 2. For the same reason, \(R_2\) cannot exceed \(\limsup_{n \to \infty} \chi(P^n; \sigma^{Y_2 \otimes n})\) either. Now we will prove the achievability of the extremal point of the rate region given by \(\frac{7}{2}\) and \(\frac{8}{2}\), since then every rate pair in the rate region is achievable by the time sharing principle.

At first we present some tools which will be used for our proof:

Let \(H\) be a Hilbert space. For \(\rho \in \mathcal{S}(H)\) and \(\alpha > 0\) there exists an orthogonal subspace projector \(\Pi_{\rho, \alpha}\) commuting with \(\rho^{\otimes n}\) and satisfying
\[
\text{tr} \left( \rho^{\otimes n} \Pi_{\rho, \alpha} \right) \geq 1 - \frac{d}{4n\alpha^2} ,
\]  
(9)
\[
\text{tr} \left( \Pi_{\rho, \alpha} \right) \leq 2^{nS(\rho) + Kd\alpha\sqrt{n}} ,
\]  
(10)
\[
\Pi_{\rho, \alpha} : \rho^{\otimes n} : \Pi_{\rho, \alpha} \leq 2^{-nS(\rho) + Kd\alpha\sqrt{n}} \Pi_{\rho, \alpha} ,
\]  
(11)
where \(d := \dim H\) and \(K\) is a positive constant (cf. \(\frac{10}{2}\)). Let \(A\) be a finite set and let \(V : A \to \mathcal{S}(H)\) be a classical-quantum channel. For a probability distribution \(P\) on \(A\), \(\alpha > 0\), and \(x^n \in \mathcal{T}^n_P\) there exists an orthogonal subspace projector \(\Pi_{\psi, \alpha}(x^n)\) commuting with \(\psi^{\otimes n}\) and satisfying
\[
\text{tr} \left( \psi^{\otimes n} \Pi_{\psi, \alpha}(x^n) \right) \geq 1 - \frac{ad}{4n\alpha^2} ,
\]  
(12)
\[
\text{tr} \left( \Pi_{\psi, \alpha}(x^n) \right) \leq 2^{nS(\psi) + Kd\alpha\sqrt{n}} ,
\]  
(13)
\[
\Pi_{\psi, \alpha}(x^n) : \psi^{\otimes n}(x^n) : \Pi_{\psi, \alpha}(x^n) \leq 2^{-nS(\psi) + Kd\alpha\sqrt{n}} \Pi_{\psi, \alpha}(x^n) ,
\]  
(14)
where \(a := \#\{A\}\) and \(K\) is a positive constant (cf. \(\frac{11}{2}\)). Let \(V : A \to \mathcal{S}(H)\) be a classical-quantum channel. Then every probability distribution \(P\) on \(A\) defines a quantum state \(PV\) on \(\mathcal{S}(H)\), which is the resulting quantum state at the output of \(V\) when the input is sent according to \(P\). Thus for \(\alpha' > 0\) we can define an orthogonal subspace projector \(\Pi_{\psi, \alpha', \sqrt{n}}\) which fulfills \(\frac{12}{2}\), \(\frac{13}{2}\), and \(\frac{14}{2}\) (here we set \(\rho = PV\) and \(\alpha = \alpha' \sqrt{n}\)). Furthermore, for \(\Pi_{\psi, \alpha', \sqrt{n}}\) we have the following inequality
\[
\text{tr} \left( \psi^{\otimes n} \Pi_{\psi, \alpha', \sqrt{n}} \right) \geq 1 - \frac{ad}{4n\alpha'^2} ,
\]  
(15)
where $K$ is a positive constant (cf. [18]).

**Lemma 3.3 (Measurement on Approximately Close States, cf. [18]).**

Let $\sigma$ and $\rho$ be two quantum states, and let $\Pi$ be a positive operator such that $\Pi \leq \text{id}$, then

$$\text{tr}(\Pi \sigma) \geq \text{tr}(\Pi \rho) - ||\sigma - \rho||_1.$$  

**Lemma 3.4 (Tender Operator, cf. [19] and [14]).** Let $\rho$ be a quantum state. Let $X$ be a positive operator such that $X \leq \text{id}$ and $1 - \text{tr}(\rho X) \leq \lambda \leq 1$, then

$$||\rho - \sqrt{X} \rho \sqrt{X}|| \leq \sqrt{8\lambda}.$$  

**Lemma 3.5 (Hayashi-Nagaoka Operator Inequality, cf. [7]).** For any positive operators $S$ and $T$ such that $S \leq \text{id}$ we have

$$\text{id} - (S + T)^{-\frac{1}{2}} S (S + T)^{-\frac{1}{2}} \leq (\text{id} - S) + 4T.$$  

For any positive $\epsilon$ let $M'_1$ be a message set such that $|M'_1| \leq 2^{n(\chi(P, \sigma^{Y_1}) - 2\epsilon)}$, and let $M'_2$ be a message set such that $|M'_2| \leq 2^{n(\chi(P, \sigma^{Y_2}) - 2\epsilon)}$. We generate $|M'_1||M'_2|$ independent random variables

$$\{X^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}$$

taking values in $X^n$ i.i.d. according to the product distribution $P(x^n) = \prod_{i=1}^{n} P(x_i)$.

For all $x^n \in X^n$ we define $\Pi_{PW_1, \alpha \sqrt{\sigma}}$ on $H_{Y_1}^{\otimes n}$, $\Pi_{PW_2, \alpha \sqrt{\sigma}}$ on $H_{Y_2}^{\otimes n}$, $\Pi_{W_1^{\otimes n}(x^n), \alpha}$ on $H_{Y_1}^{\otimes n}$, and $\Pi_{W_2^{\otimes n}(x^n), \alpha}$ on $H_{Y_2}^{\otimes n}$ as in (12), (13), (14), and (15). Here we set $P = P$, $\forall = W_1$, and $= W_2$, respectively. $\alpha$ is some positive constant which we will choose later. We define

$$D'_{x^n}^{(1)} := \Pi_{PW_1, \alpha \sqrt{\sigma}} \Pi_{W_1^{\otimes n}(x^n), \alpha} \Pi_{PW_1, \alpha \sqrt{\sigma}},$$

and

$$D'_{x^n}^{(2)} := \Pi_{PW_2, \alpha \sqrt{\sigma}} \Pi_{W_2^{\otimes n}(x^n), \alpha} \Pi_{PW_1, \alpha \sqrt{\sigma}}.$$  

For all $(m_1, m_2) \in M'_1 \times M'_2$ and any realization $x^n(m_1, m_2)$ of $X^n(m_1, m_2)$ we have

$$\text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) D'_{x^n}^{(1)} \right)$$

$$= \text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha \sqrt{\sigma}} \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \Pi_{PW_1, \alpha \sqrt{\sigma}} \right)$$

$$= \text{tr} \left((\Pi_{PW_1, \alpha \sqrt{\sigma}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha \sqrt{\sigma}}) \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \right)$$

$$\geq \text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \right)$$

$$- \|\Pi_{PW_1, \alpha \sqrt{\sigma}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha \sqrt{\sigma}} - W_1^{\otimes n}(x^n(m_1, m_2))\|_1$$

$$\geq 1 - \frac{d}{4n^2} \text{tr} \left(\Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \right)$$

$$- \|\Pi_{PW_1, \alpha \sqrt{\sigma}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha \sqrt{\sigma}} - W_1^{\otimes n}(x^n(m_1, m_2))\|_1.$$
\[ \geq 1 - \frac{d}{4m\alpha^2} - \sqrt{8 \frac{ad}{4m\alpha^2}}. \]  

(18)

The first inequality holds because of Lemma 3.3, the second inequality holds because of (12), and the third inequality holds because of Lemma 3.4 and (15).

Similarly, we have

\[
\text{tr} \left( W_2^{\otimes n}(x^n(m_1, m_2)) D_x^{(2)}(m_1, m_2) \right) \geq 1 - \frac{d}{4m\alpha^2} - \sqrt{8 \frac{ad}{4m\alpha^2}}. 
\]

(19)

We define \( \rho_2 := PW_2 = \sum_{x \in X} P(X)W_2(\phi_x) \), then \( \rho_2^{\otimes n} = \rho_2 \) if any realization of \( X^n \) is used to decode the input message. Let us fix \((m_1, m_2), (m_1', m_2') \in M' \times M'\) such that \( m_2 \not= m_2' \). Node 2 would make an error if \((m_1, m_2)\) has been sent, but node 2’s decoding results in the message \( m_2' \). We now consider the expected value of the probability of this case if we use the random encoder \( X^n \) to decode the input message. We have

\[
E \left[ \text{tr} \left( W_2^{\otimes n}(X^n(m_1, m_2)) D_x^{(2)}(X^n(m_1, m_2)) \right) \right] = \text{tr} \left[ E \left( W_2^{\otimes n}(X^n(m_1, m_2)) \right) \cdot D_x^{(2)}(X^n(m_1, m_2)) \right] \\
= \text{tr} \left[ \rho_2^{\otimes n} E \left( D_x^{(2)}(X^n(m_1, m_2)) \right) \right] \\
= \text{tr} \left[ \rho_2^{\otimes n} E \left( \Pi_{PW_2, \alpha \sqrt{\sigma}} \Pi_{W_2^{\otimes n}(X^n(m_1, m_2)), \alpha} \Pi_{PW_2, \alpha \sqrt{\sigma}} \right) \right] \\
= \text{tr} \left[ E \left( \Pi_{PW_2, \alpha \sqrt{\sigma}} \rho_2^{\otimes n} \Pi_{PW_2, \alpha \sqrt{\sigma}} \Pi_{W_2^{\otimes n}(X^n(m_1, m_2)), \alpha} \right) \right] \\
= \text{tr} \left[ \Pi_{PW_2, \alpha \sqrt{\sigma}} \rho_2^{\otimes n} \Pi_{PW_2, \alpha \sqrt{\sigma}} E \left( \Pi_{W_2^{\otimes n}(X^n(m_1, m_2)), \alpha} \right) \right] \\
\leq 2^{-n[S(\rho_2) - \frac{1}{2} \epsilon]} \text{tr} \left[ \Pi_{PW_2, \alpha \sqrt{\sigma}} E \left( \Pi_{W_2^{\otimes n}(X^n(m_1, m_2)), \alpha} \right) \right] \\
\leq 2^{-n[S_X(\text{tr}(PW_2(\phi_x))) - \frac{1}{2} \epsilon] - n[S(\rho_2) - \frac{1}{2} \epsilon]} \text{tr} \left[ \Pi_{PW_2, \alpha \sqrt{\sigma}} \right] \\
= 2^{-n[S_X(\text{tr}(PW_2(\phi_x))) - S(\sum_{x \in X} P(X)W_2(\phi_x)) - \epsilon]} \text{tr} \left[ \Pi_{PW_2, \alpha \sqrt{\sigma}} \right] \\
= 2^{-n[\chi(P, \rho^{\otimes 2}) - \epsilon]} \text{tr} \left[ \Pi_{PW_2, \alpha \sqrt{\sigma}} \right] \\
\leq 2^{-n[\chi(P, \rho^{\otimes 2}) - \epsilon]} . 
\]

(20)

The first equality hold because \( X^n(m_1, m_2) \) and \( X^n(m_1, m_2) \) are independent, the first inequality holds because of (11), and the second inequality holds because of (13).

Similarly, let us fix \((m_1', m_2), (m_1, m_2) \in M' \times M'\) such that \( m_1 \not= m_1' \). Node 1 would make an error if \((m_1, m_2)\) has been sent, but node 1’s decoding results in the message \( m_1' \). We now consider the expected value of the probability of this case if we use the random encoder \( X^n \) to decode the input message. We have

\[
E \left[ \text{tr} \left( W_1^{\otimes n}(X^n(m_1, m_2)) D_x^{(2)}(X^n(m_1, m_2)) \right) \right] \leq 2^{-n[\chi(P, \rho^{\otimes 2}) - \epsilon]} . 
\]

(21)
For all \((m_1, m_2) \in M'_1 \times M'_2\) we define

\[
D^{(1)}_{X^n(m_1, m_2)} := \left( \sqrt{ \sum_{m_1^2 \in M'_1} D^{(1)}_{X^n(m_1', m_2)} } \right)^{-1} D^{(1)}_{X^n(m_1, m_2)} \left( \sqrt{ \sum_{m_1^2 \in M'_1} D^{(1)}_{X^n(m_1', m_2)} } \right)^{-1},
\]

and

\[
D^{(2)}_{X^n(m_1, m_2)} := \left( \sqrt{ \sum_{m_2^2 \in M'_2} D^{(2)}_{X^n(m_1, m_2^2)} } \right)^{-1} D^{(2)}_{X^n(m_1, m_2)} \left( \sqrt{ \sum_{m_2^2 \in M'_2} D^{(2)}_{X^n(m_1, m_2^2)} } \right)^{-1},
\]

which depends on the random outcome of \(X^n\). By construction, for any realization \(\{x^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}\) of \(\{X^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}\) we have for every \(m_1 \in M'_1\),

\[
\sum_{m_1 \in M'_1} D^{(1)}_{x^n(m_1, m_2)} \leq \text{id}_{H \otimes \sigma_n},
\]

and for every \(m_2 \in M'_2\)

\[
\sum_{m_2 \in M'_2} D^{(2)}_{x^n(m_1, m_2)} \leq \text{id}_{H \otimes \sigma_n}.
\]

We combine \((18)\) and \((20)\), for all \((m_1, m_2) \in M'_1 \times M'_2\) we have

\[
E \left[ \text{tr} \left( D^{(1)}_{X^n(m_1, m_2)} W_1^\otimes n(X^n(m_1, m_2)) \right) \right] \\
\geq E \left[ \text{tr} \left( D^{(1)}_{X^n(m_1, m_2)} W_1^\otimes n(X^n(m_1, m_2)) \right) \right] \\
- 4E \left[ \text{tr} \left( \sum_{m_1^2 \neq m_1} D^{(1)}_{X^n(m_1', m_2)} W_1^\otimes n(X^n(m_1, m_2)) \right) \right] \\
\geq 1 - \frac{d}{4na^2} - \sqrt{8\frac{ad}{4na^2}} \\
- 4E \left[ \text{tr} \left( \sum_{m_1^2 \neq m_1} D^{(1)}_{X^n(m_1', m_2)} W_1^\otimes n(X^n(m_1, m_2)) \right) \right] \\
\geq 1 - \frac{d}{4na^2} - \sqrt{8\frac{ad}{4na^2}} - 4|M'_1|2^{-n|\chi(P, \sigma^n) - e|} \\
\geq 1 - \frac{d}{4na^2} - \sqrt{8\frac{ad}{4na^2}} - 2^{-2n}.
\]

The first inequity holds because of Lemma \(3.5\).

Similarly, if we combine \((18)\) and \((21)\) we have for all \((m_1, m_2) \in M'_1 \times M'_2\)

\[
E \left[ \text{tr} \left( D^{(2)}_{X^n(m_1, m_2)} W_2^\otimes n(X^n(m_1, m_2)) \right) \right] \\
\geq 1 - \frac{d}{4na^2} - \sqrt{8\frac{ad}{4na^2}} - 2^{-2n}.
\]
Since (22) and (23) hold for all \((m_1, m_2) \in M'_1 \times M'_2\), for any positive \(\omega\), choosing a suitable \(\alpha\), if \(n\) is sufficiently large we have

\[
\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} E \left[ \text{tr} \left( D^{(1)}_{X^n(m_1, m_2)} W_1^{\otimes n} (X^n(m_1, m_2)) \right) \right] \geq 1 - \omega
\]

and

\[
\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} E \left[ \text{tr} \left( D^{(2)}_{X^n(m_1, m_2)} W_2^{\otimes n} (X^n(m_1, m_2)) \right) \right] \geq 1 - \omega .
\]

By the law of large numbers, if \(n\) is sufficiently large, for any positive \(\delta\) and \(\gamma\) we have

\[
p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(1)}_{X^n(m_1, m_2)} W_1^{\otimes n} (X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \geq 1 - \gamma
\]

and

\[
p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(2)}_{X^n(m_1, m_2)} W_2^{\otimes n} (X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \geq 1 - \gamma .
\]

Thus

\[
p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(1)}_{X^n(m_1, m_2)} W_1^{\otimes n} (X^n(m_1, m_2)) \right) \geq 1 - \delta \right. \quad \text{and} \quad \left. \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(2)}_{X^n(m_1, m_2)} W_2^{\otimes n} (X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \geq 1 - 2\gamma .
\]

If \(n\) is sufficiently large, with a positive probability, we can find a realization \(x^n(m_1, m_2)\) of \(X^n(m_1, m_2)\) such that

\[
\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(1)}_{x^n(m_1, m_2)} W_1^{\otimes n} (x^n(m_1, m_2)) \right) \geq 1 - \delta ,
\]

and

\[
\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left( D^{(2)}_{x^n(m_1, m_2)} W_2^{\otimes n} (x^n(m_1, m_2)) \right) \geq 1 - \delta .
\]

Assume

\[
\left| \left\{ m_2 \in M'_2 : \sum_{m_2 \in M'_2} \frac{1}{|M'_2|} \text{tr} \left( D^{(1)}_{x^n(m_1, m_2)} W_1^{\otimes n} (x^n(m_1, m_2)) \right) < 1 - 2\delta \right\} \right| > \frac{1}{2} |M'_2| .
\]
We have in this case,
\[
\sum_{m_1 \in M_1'} \sum_{m_2 \in M_2'} \frac{1}{|M_1'||M_2'|} \text{tr} \left( D_{x^n(m_1,m_2)}^{(1)} W_1^\otimes n(x^n(m_1,m_2)) \right) < 1 - \delta ,
\]
but this is a contradiction to the result above.

Thus there exists a set \( M_2 \in M_2' \) such that \( |M_2| = \left\lceil \frac{1}{2} |M_2'| \right\rceil \) and for every \( m_2 \in M_2 \) we have
\[
\sum_{m_1 \in M_1'} \frac{1}{|M_1'|} \text{tr} \left( D_{x^n(m_1,m_2)}^{(1)} W_1^\otimes n(x^n(m_1,m_2)) \right) \geq 1 - 2\delta . \tag{24}
\]

Similarly, there exists a set \( M_1 \in M_1' \) such that \( |M_1| = \left\lceil \frac{1}{2} |M_1'| \right\rceil \) and for every \( m_1 \in M_1 \) we have
\[
\sum_{m_2 \in M_2'} \frac{1}{|M_2'|} \text{tr} \left( D_{x^n(m_1,m_2)}^{(2)} W_2^\otimes n(x^n(m_1,m_2)) \right) \geq 1 - 2\delta . \tag{25}
\]

For every \((m_1, m_2) \in M_1 \times M_2\) we define
\[
w((m_1, m_2)) := x^n(m_1, m_2) , \tag{26}
\]
and
\[
D_{m_2}^{(m_1)} := D_{x^n(m_1,m_2)}^{(1)} , \tag{27}
\]
and
\[
D_{m_1}^{(m_2)} := D_{x^n(m_1,m_2)}^{(2)} . \tag{28}
\]

\( \{ D_{m_1}^{(m_2)} : m_1 \in M_1 \} \) is less or equal to the partition of the identity for every \( m_2 \in M_2 \). \( \{ D_{m_2}^{(m_1)} : m_2 \in M_2 \} \) is less or equal to the partition of the identity for every \( m_1 \in M_1 \).

Since node 1 already knows the message \( m_2 \in M_2 \), it chooses the corresponding decoding set
\[
\{ D_{m_2}^{(m_2)} : m_2 \in M_2 \}
\]
to decode \( m_1 \in M_1 \). Since node 2 already knows the message \( m_1 \in M_1 \), it chooses the corresponding decoding set
\[
\{ D_{m_1}^{(m_1)} : m_1 \in M_1 \}
\]
to decode \( m_2 \in M_2 \).

By (24) and (25) for every \( m_2 \in M_2 \) we have
\[
\sum_{m_1 \in M_1} \frac{1}{|M_1|} \text{tr} \left( D_{m_1}^{(m_2)} W_1^\otimes n(x^n(m_1,m_2)) \right) \geq 1 - 4\delta , \tag{29}
\]
and for every \( m_1 \in M_1 \) we have
\[
\sum_{m_2 \in M_2} \frac{1}{|M_2|} \text{tr} \left( D_{m_2}^{(m_1)} W_2^\otimes n(x^n(m_1,m_2)) \right) \geq 1 - 4\delta . \tag{30}
\]
Thus, for all sufficiently large $n \in \mathbb{N}$ any rate pairs satisfying
\[ R_1 \leq \chi(P; \sigma^{Y_1}) - 2\epsilon - \frac{1}{n} \]
and
\[ R_2 \leq \chi(P; \sigma^{Y_2}) - 2\epsilon - \frac{1}{n} \]
are achievable.

If we combine Lemma 3.1 and Theorem 3.2, we obtain

**Corollary 3.6.** Let $N$ be a two-phase bidirectional relaying quantum channel. Let $H^{Y_1}$ be the Hilbert space whose unit vectors correspond to the pure states of node 1’s quantum system, $H^{Y_2}$ be the Hilbert space whose unit vectors correspond to the pure states of node 2’s quantum system, and $H^{X}$ be the Hilbert space whose unit vectors correspond to the pure states of the relay node’s quantum system.

We assume that the relay node’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $X \subset H^{X}$.

We assume that node 1’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_1 \subset H^{Y_1}$.

We assume that node 2’s encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_2 \subset H^{Y_2}$.

The classical-quantum capacity region of the two-phase bidirectional relaying quantum channel with average error is the intersection of two rate regions, Region 1 and Region 2, which are defined as follows:

1: Region 1 is the set of all rate pairs $(R_1, R_2)$ such that
\[ R_2 \leq \chi(Q_1; \sigma^X) \]  
\[ R_1 \leq \chi(Q_2; \sigma^X) \]  
and
\[ R_2 + R_1 \leq \chi(Q_{1,2}; \sigma^X) \]
for any joint probability distribution $Q_{1,2}$ on $Y_1 \times Y_2$. Here $Q_1$ is the marginal probability distribution of $Q_{1,2}$ on $Y_1$, $Q_2$ is the marginal probability distribution of $Q_{1,2}$ on $Y_2$, and $\sigma^X$ is the resulting quantum state at the outcome of the relay node.

2: Region 2 is the set of all rate pairs $(R_1, R_2)$ such that
\[ R_1 \leq \limsup_{n \to \infty} \chi(P^n; \sigma^{Y_1 \otimes n}) \]  
\[ R_2 \leq \limsup_{n \to \infty} \chi(P^n; \sigma^{Y_2 \otimes n}) \]
for all probability distribution $P$ on $X$. Here $\sigma^{Y_1}$ is the resulting quantum state at the outcome of node 1, while $\sigma^{Y_2}$ is the resulting quantum state at the outcome of node 2.
Remark 3.7. We consider only average errors, but not maximal errors in Theorem 3.2 and Corollary 3.6, since Lemma 3.1 only considered average errors for the multiple-access phase. It is well-known from the classical multiple-access channels that the capacity region of a multiple-access channel with average errors is not equal to its capacity region with maximal errors (cf. [1]).

Remark 3.8. Without loss of generality we assume that \( \chi(P; \sigma^X) \geq \chi(Q_2; \sigma^X) \) holds, i.e., \( W_2 \), the channel which connects the relay node and node 2, has a lower capacity than \( W_1 \) in the broadcast phase. If additionally \( \chi(Q_2; \sigma^X) = \chi(P; \sigma^Y) \) holds, i.e., the capacities of \( W_2 \) in both directions are identical, then \( R_1 \) cannot exceed \( \chi(P; \sigma^Y) \) in the multiple-access phase. In this case we may assume that in the broadcast phase, the message sets \( M_1 = \{1, \cdots, |M_1|\} \) and \( M_2 = \{1, \cdots, |M_2|\} \), which the relay node sends to node 1 and node 2, satisfy \( |M_1| \leq 2^n\chi(P; \sigma^Y) - \epsilon \) and \( |M_2| \leq 2^n\chi(P; \sigma^Y) - \epsilon \) for a positive \( \epsilon \).

In this case, we have a very simple coding strategy for the broadcast phase. The common message set which the relay node sends to both node 1 and node 2 in the broadcast phase is a set \( M' = \{1, \cdots, |M'|\} \) which satisfies \( |M'| = \lfloor 2^n\chi(P; \sigma^Y) - \epsilon \rfloor \).

We consider the case that the relay node wants to send \( (m_1, m_2) \in M_1 \times M_2 \), where node 1 shall detect \( m_1 \), while node 2 shall detect \( m_2 \). Then the relay node sends \( m_1 + m_2 \mod |M'| \) as a common message to both node 1 and node 2. By the HSW Random Coding Theorem (cf. [17] and [9]) node 1 and node 2 can decode the common message if the size of the message set is less than \( 2^n\chi(P; \sigma^Y) \).

Since node 1 already knows \( m_2 \), it can obtain \( m_1 \) by simply subtracting \( m_2 \) from \( m_1 + m_2 \mod |M'| \). Since node 2 already knows \( m_1 \), it can obtain \( m_2 \) by subtracting \( m_1 \) from \( m_1 + m_2 \mod |M'| \).

References

[1] R. Ahlswede, On two-way communication channels and a problem by Zarankiewicz, Sixth Prague Conf. on Inf. Th., Stat. Dec. Fct’s and Rand. Proc., Publ. House Chechosl. Academy of Sc., Prague, pp. 23-37, 1973.

[2] R. Ahlswede, Multi-way communication channels, Proceedings of 2nd International Symposium on Information Theory, Thakadsor, Armenian SSR, 1971, Akademiai Kiado, Budapest, pp. 23-52, 1973.

[3] P. P. Bergmans, Random coding theorem for broadcast channels with degraded components, IEEE Trans. Inf. Theory, Vol. IT-19, No. 2, pp. 197-207, 1973.

[4] T. M. Cover, Comments on broadcast channels, IEEE Trans. Inf. Theory, Vol. IT-44, pp. 2524-2530, 1998.

[5] T. M. Cover and A. El Gamal, Capacity theorems for the relay channel, IEEE Trans. Inf. Theory, Vol. IT-25, No. 5, pp. 572-584, 1979.

[6] A. El Gamal and E. Van der Meulen, A proof of marton’s coding theorem for the discrete memoryless broadcast channel, IEEE Trans. Inf. Theory, Vol. IT-27, pp. 120-122, 1981.
[7] M. Hayashi and H. Nagaoka, General formulas for capacity of classical-quantum channels, IEEE Trans. Inf. Theory, Vol. 49, No. 7, pp. 1753-1768, 2003.

[8] A. Holevo, Statistical problems in quantum physics, Proceedings of the second Japan-USSR Symposium on Probability Theory, ser. Lecture Notes in Mathematics, G. Maruyama and J. V. Prokhorov, Eds., Vol. 330, pp. 104-119, Springer-Verlag, Berlin, 1973.

[9] A. S. Holevo, The capacity of the quantum channel with general signal states, IEEE Trans. Inf. Theory, Vol. 44, pp. 269-273, 1998.

[10] G. Kramer, M. Gastpar, and P. Gupta, Cooperative strategies and capacity for relay networks, IEEE Trans. Inf. Theory, Vol. 51, No. 9, pp. 3037-3063, 2005.

[11] H. Liao, Multiple access channels, Ph.D. dissertation, Department of Electrical Engineering, University of Hawai‘i, Honolulu, 1972.

[12] K. Marton, A coding theorem for the discrete memoryless broadcast channel, IEEE Trans. Inf. Theory, Vol. IT-25, pp. 306-311, 1979.

[13] T. J. Oechtering, C. Schmurr, I. Bjelaković, and H. Boche, Broadcast capacity region of two-phase bidirectional relaying, IEEE Trans. Inf. Theory, Vol. 54, No. 1, pp. 454-458, 2008.

[14] T. Ogawa and H. Nagaoka, Making good codes for classical-quantum channel coding via quantum hypothesis testing, IEEE Trans. Inform. Theory, Vol. 53, No. 6, 2261-2266, 2007.

[15] I. Savov, M. Wilde, Classical codes for quantum broadcast channels, Proceedings of ISIT 2012, pp. 721-725, 2012.

[16] I. Savov, M. Wilde, and M. Vu, Partial decode-forward for quantum relay channels, Proceedings of ISIT 2012, pp. 731-735, 2012.

[17] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev. A, Vol. 56, pp. 131-138, 1997.

[18] M. Wilde, Quantum Information Theory, Cambridge University Press, 2013.

[19] A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inf. Theory, Vol. 45, No. 7, pp. 2481-2485, 1999.

[20] A. Winter, The capacity of the quantum multiple-access channel, IEEE Trans. Inf. Theory, Vol. 47, No. 7, pp. 3059-3065, 2001.

[21] J. Yard, P. Hayden, and I. Devetak, Capacity theorems for quantum multiple access channels — classical-quantum and quantum-quantum capacity regions, IEEE Trans. Inf. Theory, Vol. 54, No. 7, pp. 3091-3113, 2008.