Measurement compression with quantum side information using shared randomness

Anurag Anshu∗ Rahul Jain† Naqueeb Ahmad Warsi‡

Abstract

We consider the problem of measurement compression with side information in the one-shot setting with shared randomness. We provide a protocol based on convex split and position based decoding with its communication upper bounded in terms of smooth-max and hypothesis testing divergences.

1 Introduction

Measurement compression is a fundamental problem in quantum information theory first considered in a seminal work by Winter [1]. It has found important applications in the task of distilling pure states from bi-partite mixed states [2, 3, 4, 5]. Subsequently its extension with quantum side information was considered by Wilde, Hayden, Buscemi and Hsieh [7] which is as follows: Alice (AC), Bob (B) and Referee (R) share a joint pure state

\[ |\Psi_{RACB}\rangle = \sum_c \sqrt{p(c)} |c\rangle_C |\psi^c\rangle_{RAB}. \]

The register \( C \) is to be viewed as outcome of a POVM performed by Alice coherently (given that any measurement can be realized coherently). Due to the copy of \( C \) in \( \bar{C} \), the register \( C \) is a classical register. The state on registers \( RACB \) can be written as

\[ |\Psi_{RACB}\rangle = \sum_c p(c) |c\rangle_C \otimes |\psi^c\rangle_{RAB}, \]

for some probability distribution \( p(c) \) and pure quantum states \( |\psi^c\rangle_{RAB} \). The objective is that using shared randomness, Alice should communicate register \( C \) to Bob. That is, Bob should produce a register \( C' \) such that the state in registers \( RBCC' \) after the protocol is \( |\Phi_{RBCC'}\rangle \) satisfying

\[ \mathbb{P}(\Phi_{RBCC'}, \sum_c p(c) |c\rangle_C \otimes |\psi^c\rangle_{RAB}) \leq \varepsilon, \]

where \( \varepsilon > 0 \) is error parameter and \( \mathbb{P}(\cdot, \cdot) \) represents purified distance.

∗Centre for Quantum Technologies, National University of Singapore, Singapore. a0109169@u.nus.edu
†Centre for Quantum Technologies, National University of Singapore and MajuLab, UMI 3654, Singapore. rahul@comp.nus.edu.sg
‡Centre for Quantum Technologies, National University of Singapore and School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore and IIITD, Delhi. warsi.naqueeb@gmail.com
The work [7] gave optimal communication required to achieve this task in the asymptotic setting given by $I(R : C | B)_p$. We consider this task in the one-shot setting and present a protocol with communication upper bounded by

$$\min_{\sigma_C} \left( D_{\text{max}}(\Psi_{RBC} \| \Psi_{RB} \otimes \sigma_C) - D_H^2(\Psi_{BC} \| \Psi_B \otimes \sigma_C) \right) + O \left( \log \left( \frac{1}{\varepsilon} \right) \right),$$

where $\sigma_C$ is a classical state (that is, it commutes with $\Psi_C$). We note that this bound converges to $I(R : C | B)_p$ in the asymptotic setting. Some one-shot converse bounds for this task appear in [8].

## 2 Preliminaries

### Quantum information theory

Consider a finite dimensional Hilbert space $H$ endowed with an inner product $\langle \cdot, \cdot \rangle$. (In this paper, we only consider finite dimensional Hilbert-spaces). The $\ell_1$ norm of an operator $X$ on $H$ is $\|X\|_1 := \text{Tr}\sqrt{X^\dagger X}$ and $\ell_2$ norm is $\|X\|_2 := \sqrt{\text{Tr}X^\dagger X}$. A quantum state (or a density matrix or a state) is a positive semi-definite matrix on $H$ with trace equal to 1. It is called pure if and only if its rank is 1. A sub-normalized state is a positive semi-definite matrix on $H$ with trace less than or equal to 1. Let $|\psi\rangle$ be a unit vector on $H$, that is $\langle \psi, \psi \rangle = 1$. With some abuse of notation, we use $\psi$ to represent the state and also the density matrix $|\psi\rangle\langle \psi|$, associated with $|\psi\rangle$. Given a quantum state $\rho$ on $H$, support of $\rho$, called supp$(\rho)$ is the subspace of $H$ spanned by all eigen-vectors of $\rho$ with non-zero eigenvalues.

A quantum register $A$ is associated with some Hilbert space $H_A$. Define $|A\rangle := \dim(H_A)$. Let $L(A)$ represent the set of all linear operators on $H_A$. We denote by $D(A)$, the set of quantum states on the Hilbert space $H_A$. State $\rho$ with subscript $A$ indicates $\rho_A \in D(A)$. If two registers $A, B$ are associated with the same Hilbert space, we shall represent the relation by $A \equiv B$. Composition of two registers $A$ and $B$, denoted $AB$, is associated with Hilbert space $H_A \otimes H_B$. For two quantum states $\rho, \sigma \in D(B)$, $\rho \otimes \sigma \in D(AB)$ represents the tensor product (Kronecker product) of $\rho$ and $\sigma$. The identity operator on $H_A$ (and associated register $A$) is denoted $I_A$.

Let $\rho_{AB} \in D(AB)$. We define

$$\rho_B := \text{Tr}_A \rho_{AB} := \sum_i (|i\rangle \otimes I_B) \rho_{AB} (|i\rangle \otimes I_B),$$

where $\{|i\rangle\}_i$ is an orthonormal basis for the Hilbert space $H_A$. The state $\rho_B \in D(B)$ is referred to as the marginal state of $\rho_{AB}$. Unless otherwise stated, a missing register from subscript in a state will represent partial trace over that register. Given a $\rho_A \in D(A)$, a purification of $\rho_A$ is a pure state $\rho_{AB} \in D(AB)$ such that $\text{Tr}_B \rho_{AB} = \rho_A$. Purification of a quantum state is not unique.

A quantum map $E : L(A) \to L(B)$ is a completely positive and trace preserving (CPTP) linear map (mapping states in $D(A)$ to states in $D(B)$). A unitary operator $U_A : H_A \to H_A$ is such that $U_A^\dagger U_A = U_A U_A^\dagger = I_A$. An isometry $V : H_A \to H_B$ is such that $V^\dagger V = I_A$ and $VV^\dagger = I_B$. The set of all unitary operations on register $A$ is denoted by $U(A)$.

**Definition 1.** We shall consider the following information theoretic quantities. Reader is referred to [9] [10] [11] [12] for many of these definitions. We consider only normalized states in the definitions below. Let $\varepsilon \geq 0$.

1. **Fidelity.** For $\rho_A, \sigma_A \in D(A)$,

$$F(\rho_A, \sigma_A) \overset{\text{def}}{=} \| \sqrt{\rho_A} \sqrt{\sigma_A} \|_1.$$ 

For classical probability distributions $P = \{p_i\}, Q = \{q_i\}$,

$$F(P, Q) \overset{\text{def}}{=} \sum_i \sqrt{p_i q_i}.$$
2. **Purified distance.** For \( \rho_A, \sigma_A \in D(A) \),
\[
P(\rho_A, \sigma_A) = \sqrt{1 - F^2(\rho_A, \sigma_A)}.
\]

3. **\( \varepsilon \)-ball.** For \( \rho_A \in D(A) \),
\[
B^\varepsilon(\rho_A) = \{ \rho'_A \in D(A) \mid P(\rho_A, \rho'_A) \leq \varepsilon \}.
\]

4. **Von-neumann entropy.** For \( \rho_A \in D(A) \),
\[
S(\rho_A) \overset{\text{def}}{=} -\text{Tr}(\rho_A \log \rho_A).
\]

5. **Relative entropy.** For \( \rho_A, \sigma_A \in D(A) \) such that \( \text{supp}(\rho_A) \subset \text{supp}(\sigma_A) \),
\[
D(\rho_A\|\sigma_A) \overset{\text{def}}{=} \text{Tr}(\rho_A \log \rho_A) - \text{Tr}(\rho_A \log \sigma_A).
\]

6. **Max-relative entropy.** For \( \rho_A, \sigma_A \in D(A) \) such that \( \text{supp}(\rho_A) \subset \text{supp}(\sigma_A) \),
\[
D_{\text{max}}(\rho_A\|\sigma_A) \overset{\text{def}}{=} \inf\{ \lambda \in \mathbb{R} : 2^\lambda \sigma_A \geq \rho_A \}.
\]

7. **Smooth max-relative entropy.** For \( \rho_A, \sigma_A \in D(A) \) such that \( \text{supp}(\rho_A) \subset \text{supp}(\sigma_A) \),
\[
D^\varepsilon_{\text{max}}(\rho_A\|\sigma_A) \overset{\text{def}}{=} \inf_{\rho'_A \in B^\varepsilon(\rho_A)} D_{\text{max}}(\rho'_A\|\sigma_A).
\]

8. **Smooth min-relative entropy.** For \( \rho_A, \sigma_A \in D(A) \),
\[
D^\varepsilon_H(\rho_A\|\sigma_A) \overset{\text{def}}{=} \sup_{0 < \eta < I, \text{Tr}(\eta \rho_A) \geq 1 - \varepsilon} \log\left(\frac{1}{\text{Tr}(\eta \sigma_A)}\right).
\]

We will use the following facts.

**Fact 1** (Triangle inequality for purified distance, [11]). For states \( \rho_A, \sigma_A, \tau_A \in D(A) \),
\[
P(\rho_A, \sigma_A) \leq P(\rho_A, \tau_A) + P(\tau_A, \sigma_A).
\]

**Fact 2** ([13]). (Stinespring representation) Let \( \mathbb{E}(\cdot) : \mathcal{L}(A) \rightarrow \mathcal{L}(B) \) be a quantum operation. There exists a register \( C \) and an unitary \( U \in U(ABC) \) such that \( \mathbb{E}(\omega) = \text{Tr}_{A,C}(U(\omega \otimes |0\rangle\langle 0|^{B,C})U^\dagger) \). Stinespring representation for a channel is not unique.

**Fact 3** (Monotonicity under quantum operations, [13], [15]). For quantum states \( \rho, \sigma \in D(A) \), and quantum operation \( \mathbb{E}(\cdot) : \mathcal{L}(A) \rightarrow \mathcal{L}(B) \), it holds that
\[
\|\mathbb{E}(\rho) - \mathbb{E}(\sigma)\|_1 \leq \|\rho - \sigma\|_1 \text{ and } F(\mathbb{E}(\rho), \mathbb{E}(\sigma)) \geq F(\rho, \sigma) \text{ and } D(\rho\|\sigma) \geq D(\mathbb{E}(\rho)\|\mathbb{E}(\sigma)).
\]

In particular, for bipartite states \( \rho_{AB}, \sigma_{AB} \in D(AB) \), it holds that
\[
\|\rho_{AB} - \sigma_{AB}\|_1 \geq \|\rho_A - \sigma_A\|_1 \text{ and } F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A) \text{ and } D(\rho_{AB}\|\sigma_{AB}) \geq D(\rho_A\|\sigma_A).
\]

**Fact 4** (Uhlmann’s Theorem, [14]). Let \( \rho_A, \sigma_A \in D(A) \). Let \( \rho_{AB} \in D(AB) \) be a purification of \( \rho_A \) and \( \sigma_{AC} \in D(AC) \) be a purification of \( \sigma_A \). There exists an isometry \( V : C \rightarrow B \) such that,
\[
F(|\theta\rangle\langle AB, |\rho\rangle\langle AB|) = F(\rho_A, \sigma_A),
\]
where \( |\theta\rangle_{AB} = (I_A \otimes V)|\sigma\rangle_{AC} \).
Following is a well known fact about fidelity of classical quantum states.

**Fact 5.** Let $\rho_{X_A}, \sigma_{X_A}$ be two c-q states of the form $\rho_{X_A} = \sum_x p(x) |x\rangle\langle x| \otimes \rho^x_A$ and $\sigma_{X_A} = \sum_x q(x) |x\rangle\langle x| \otimes \sigma^x_A$. Then

$$F(\rho_{X_A}, \sigma_{X_A}) = \sum_x \sqrt{p(x)q(x)} F(\rho^x_A, \sigma^x_A).$$

**Proof.** We have that

$$F(\rho_{X_A}, \sigma_{X_A}) = \text{Tr} \left( \sqrt{\sum_x p(x) |x\rangle\langle x| \otimes \rho^x_A} \sum_x q(x) |x\rangle\langle x| \otimes \sigma^x_A} \sqrt{\sum_x p(x) |x\rangle\langle x| \otimes \rho^x_A} \right)^{1/2}$$

$$= \text{Tr} \left( \left( \sum_x \sqrt{p(x)} |x\rangle\langle x| \otimes \sqrt{\rho^x_A} \right) \left( \sum_x q(x) |x\rangle\langle x| \otimes \sigma^x_A \right) \left( \sum_x \sqrt{p(x)} |x\rangle\langle x| \otimes \sqrt{\rho^x_A} \right) \right)^{1/2}$$

$$= \text{Tr} \left( \sum_x \sqrt{p(x)q(x)} |x\rangle\langle x| \otimes \sqrt{\rho^x_A \sigma^x_A} \right)^{1/2}$$

$$= \sum_x \sqrt{p(x)q(x)} \text{Tr} \left( \sqrt{\rho^x_A \sigma^x_A} \right)$$

$$= \sum_x \sqrt{p(x)q(x)} F(\rho^x_A, \sigma^x_A)$$

Following is an immediate application of Uhlmann’s Theorem.

**Fact 6.** Let $\rho_{X_AB}, \sigma_{X_AC}$ be two c-q states of the form $\rho_{X_AB} = \sum_x p(x) |x\rangle\langle x| \otimes |\rho^x|_{AB}$ and $\sigma_{X_AC} = \sum_x q(x) |x\rangle\langle x| \otimes |\sigma^x|_{AC}$. Then there exists a set of isometries $\{U^x : B \to C\}$ such that

$$F \left( \sum_x |x\rangle\langle x| \otimes I_A \otimes U^x \right) \rho_{X_AB} \left( \sum_x |x\rangle\langle x| \otimes I_A \otimes U^x \right)^\dagger, \sigma_{X_AC} \right) = F(\rho_{X_A}, \sigma_{X_A}).$$

**Proof.** For every $x$, there exists an isometry $U_x : B \to C$, as guaranteed by Uhlmann’s Theorem \cite{uhlmann1976}, such that

$$F \left( (I_A \otimes U^x)|\rho^x|_{AB}(I_A \otimes U^x)^\dagger, |\sigma^x\rangle\langle \sigma^x|_{AC} \right) = F(\rho^x_A, \sigma^x_A).$$

The fact follows from the expression (Fact 5)

$$F(\rho_{X_A}, \sigma_{X_A}) = \sum_x \sqrt{p(x)q(x)} F(\rho^x_A, \sigma^x_A),$$

and the relation

$$F \left( \sum_x |x\rangle\langle x| \otimes I_A \otimes U^x \right) \rho_{X_AB} \left( \sum_x |x\rangle\langle x| \otimes I_A \otimes U^x \right)^\dagger, \sigma_{X_AC} \right)$$

$$= \sum_x \sqrt{p(x)q(x)} F \left( (I_A \otimes U^x)|\rho^x|_{AB}(I_A \otimes U^x)^\dagger, |\sigma^x\rangle\langle \sigma^x|_{AC} \right).$$

\(\square\)
Fact 7 (Gentle measurement lemma, [17][18]). Let \( \rho \) be a quantum state and \( 0 < A < I \) be an operator. Then
\[
F(\rho, A\rho A / \text{Tr}(A^2\rho)) \geq \sqrt{\text{Tr}(A^2\rho)}.
\]

Proof. Let \( |\rho\rangle \) be a purification of \( \rho \). Then \( (I \otimes A)|\rho\rangle \) is a purification of \( A\rho A \). Now applying monotonicity of fidelity under quantum operations (Fact 3), we find
\[
F(\rho, A\rho A / \text{Tr}(A^2\rho)) \geq F(|\rho\rangle\langle\rho|, (I \otimes A)|\rho\rangle\langle\rho|(I \otimes A^\dagger)) = \sqrt{\text{Tr}(A^2\rho)}.
\]
In last inequality, we have used \( A \geq A^2 \).

Following fact is an extension of the Gentle measurement lemma.

Fact 8. Consider a quantum state \( \rho_A = \sum_i p_i \rho^i_A \) and a map \( \mathcal{A}(X) = \sum_j P_j X P_j \otimes |i\rangle \langle i|_O \), such that \( 0 < P_i < I, \sum_i P_i^2 = I \) (\( O \) is considered the output register for the measurement \( \mathcal{A} \)). Define the state \( \rho'_{AO} \coloneqq \sum_i p_i \rho^i_A \otimes |i\rangle \langle i|_O \) and let \( q_i \coloneqq \text{Tr}(P_i^2 \rho^i_A) \). Then it holds that
\[
F(\rho'_{AO}, \mathcal{A}(\rho_A)) \geq (\sum_i p_i q_i)^{3/2}.
\]

Proof. We abbreviate \( \sigma_{AO} \coloneqq \mathcal{A}(\rho_A) \). This implies that
\[
\sigma_{AO} = \sum_{i,j} p_i P_j \rho^i_A P_j \otimes |j\rangle \langle j|_O.
\]
Define
\[
\sigma_{AO}^{\text{good}} \coloneqq \frac{1}{\sum_i p_i q_i} \sum_i p_i P_j \rho^i_A P_j \otimes |j\rangle \langle j|_O \quad \text{and} \quad \sigma_{AO}^{\text{bad}} \coloneqq \frac{1}{1 - \sum_i p_i q_i} \sum_{i \neq j} p_i P_j \rho^i_A P_j \otimes |j\rangle \langle j|_O.
\]
Then we can decompose \( \sigma_{AO} \) as
\[
\sigma_{AO} = (\sum_i p_i q_i) \sigma_{AO}^{\text{good}} + (1 - \sum_i p_i q_i) \sigma_{AO}^{\text{bad}}.
\]
From concavity of fidelity, this gives us
\[
F(\sigma_{AO}, \rho'_{AO}) \geq (\sum_i p_i q_i) F(\sigma_{AO}^{\text{good}}, \rho'_{AO})
\]
\[
= (\sum_i p_i q_i) \left( \frac{1}{\sqrt{\sum_i p_i q_i}} \sum_i p_i \sqrt{q_i} \cdot F\left( \frac{P_i \rho^i_A P_i}{q_i}, \rho^i_A \right) \right).
\]
Now employing Gentle measurement lemma (Fact 7), we conclude that
\[
F(\sigma_{AO}, \rho'_{AO}) \geq \sqrt{\sum_i p_i q_i (\sum_i p_i \sqrt{q_i} \cdot \sqrt{q_i})} = (\sum_i p_i q_i)^{3/2}.
\]

Fact 9 (Hayashi-Nagaoka inequality, [19]). Let \( 0 < S < I, T \) be positive semi-definite operators. Then
\[
(S + T)^{-\frac{1}{2}} T (S + T)^{-\frac{1}{2}} \leq 2(I - S) + 4T.
\]
Fact 10. For a quantum state $\rho_{AB}$, it holds that

$$\inf_{\rho' \in B^{\epsilon}(\rho_{PQ})} D_{\max}(\rho'_{PQ} \| \rho_P \otimes \rho_Q) \leq D_{\max}(\rho_{AB} \| \rho_A \otimes \rho_B) + 3 \log_2 \frac{2}{\epsilon}.$$  

Proof. The proof is similar to the proof given in [20], and has been explicitly given as Lemma 1 in [21].

Following is a variant of convex-split lemma (22).

Lemma 1 (Variation of convex-split lemma, [21]). For any $\epsilon > 0$. Let $\rho_{PQ} \in D(PQ)$ and $\sigma_Q \in D(Q)$ be quantum states such that $\text{supp}(\rho_Q) \subset \text{supp}(\sigma_Q)$. Let $k \overset{\text{def}}{=} \inf_{\rho' \in B^{\epsilon}(\rho_{PQ})} D_{\max}(\rho'_{PQ} \| \rho_P \otimes \sigma_Q)$. Define the following state

$$\tau_{PQ_1 \ldots Q_n} \overset{\text{def}}{=} \frac{1}{n} \sum_{j=1}^{n} \rho_{PQ_j} \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \cdots \sigma_{Q_{j-1}} \otimes \sigma_{Q_{j+1}} \cdots \sigma_{Q_n}$$

on $n + 1$ registers $P, Q_1, Q_2, \ldots, Q_n$, where $\forall j \in [n] : \rho_{PQ_j} = \rho_{PQ}$ and $\sigma_{Q_j} = \sigma_Q$. For $\delta > 0$ and $n \geq \lceil \frac{2^k}{\epsilon^2} \rceil$,

$$P(\tau_{PQ_1 \ldots Q_n}, \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \cdots \otimes \sigma_{Q_n}) \leq 2\epsilon + \delta.$$  

We will use the following corollary.

Corollary 1 (Corollary of convex-split lemma). For any $\epsilon > 0$. Let $\rho_{PQ} \in D(PQ)$. Let $k \overset{\text{def}}{=} D_{\max}(\rho_{PQ} \| \rho_P \otimes \rho_Q)$. Define the following state

$$\tau_{PQ_1 \ldots Q_n} \overset{\text{def}}{=} \frac{1}{n} \sum_{j=1}^{n} \rho_{PQ_j} \otimes \rho_{Q_1} \otimes \rho_{Q_2} \cdots \rho_{Q_{j-1}} \otimes \rho_{Q_{j+1}} \cdots \otimes \rho_{Q_n}$$

on $n + 1$ registers $P, Q_1, Q_2, \ldots, Q_n$, where $\forall j \in [n] : \rho_{PQ_j} = \rho_{PQ}$ and $\rho_{Q_j} = \rho_Q$. For $\delta > 0$ and $n = \lceil 8 \cdot 2^k \rceil$,  

$$P(\tau_{PQ_1 \ldots Q_n}, \tau_P \otimes \rho_{Q_1} \otimes \rho_{Q_2} \cdots \otimes \rho_{Q_n}) \leq 4\epsilon + \delta.$$  

Proof. Let $k' \overset{\text{def}}{=} \inf_{\rho' \in B^{2\epsilon}(\rho_{PQ})} D_{\max}(\rho'_{PQ} \| \rho_P \otimes \rho_Q)$. From Fact 10 we have that $k' \leq k + 3 \log_2 \frac{2}{\epsilon}$. Thus, the choice of $n$ ensures that $n \geq \lceil \frac{2^{k'}}{\epsilon^2} \rceil$. Now, using Lemma 1, this corollary follows.

3 An achievability bound

We prove the following theorem.

Theorem 1. Let

$$|\Psi\rangle_{RAC\hat{C}B} = \sum_c \sqrt{p(c)} |c\rangle_C |c\rangle_{\hat{C}} |\psi^c\rangle_{RAB}.$$  

There exists a randomness assisted one-way protocol $P$, which takes as input pure state $|\Psi\rangle_{RAC\hat{C}},$ shared between three parties Referee ($R$), Bob ($B$) and Alice ($AC\hat{C}$) and outputs a state $\Phi_{RAB\hat{C}}$ shared between Referee ($R$), Bob ($BC\hat{C}$) and Alice ($AC\hat{C}$) such that

$$\Phi_{RAB\hat{C}} \in B^{10 \epsilon} \left( \sum_c p(c) |c\rangle_C \otimes |c\rangle_{\hat{C}} \otimes |\psi^c\rangle_{RAB} \right).$$
and the number of bits communicated by Alice to Bob in $\mathcal{P}$ is upper bounded by:

$$\min_{\sigma_C} \left( D_{\max}^\epsilon (\Psi_{RBC} \parallel \Psi_{RB} \otimes \sigma_C) - D_\mathcal{H}^2 (\Psi_{BC} \parallel \Psi_B \otimes \sigma_C) \right) + 6 \log \left( \frac{1}{\epsilon} \right),$$

where $\sigma_C$ is a classical state.

Proof. Let $\sigma_C$ be the classical state achieving the optimum in the statement of the theorem and let it be of the form $\sigma_C = \sum_c q(c) |c\rangle \langle c|$. Let $k \overset{\text{def}}{=} D_{\max}^\epsilon (\Psi_{RBC} \parallel \Psi_{RB} \otimes \sigma_C)$, $n \overset{\text{def}}{=} \lceil 8 \cdot \frac{2^k}{\epsilon^2} \rceil$ and $b \overset{\text{def}}{=} \lceil \epsilon^2 \cdot 2 D_{\mathcal{H}}^2 (\Psi_{BC} \parallel \Psi_B \otimes \sigma_C) \rceil$. By definition of $D_\mathcal{H}^2 (\Psi_{BC} \parallel \Psi_B \otimes \sigma_C)$, there exists a projector $\Pi_{BC}$ such that $\text{Tr}(\Pi_{BC} \Psi_{BC}) \geq 1 - \epsilon^2$ and $\text{Tr}(\Pi_{BC} \Psi_B \otimes \sigma_C) \leq \epsilon^2 / b$. Let $\sigma_{CC'} \overset{\text{def}}{=} \sum_c q(c) |c\rangle \langle c| \otimes |c\rangle \langle c|$, be an extension of $\sigma_C$. Consider the state,

$$\mu_{RBC_1 C'_1 ... C_n C'_n} \overset{\text{def}}{=} \frac{1}{n} \sum_{j=1}^n \Psi_{RBC_j C'_j} \otimes \sigma_{C_1 C'_1} \otimes ... \otimes \sigma_{C_{j-1} C'_{j-1}} \otimes \sigma_{C_{j+1} C'_{j+1}} \otimes ... \otimes \sigma_{C_n C'_n},$$

where we have written

$$\Psi_{RABC_j C'_j} \overset{\text{def}}{=} \sum_c p(c) |c\rangle \langle c|_j \otimes |c\rangle \langle c|_{C'_j} \otimes \psi_{RAB}^{c_j}.$$ 

Note that $\Psi_{RB} = \mu_{RB}$. From the definition $\Psi_{RACB} = \sum_c p(c) |c\rangle \langle c| \otimes \psi_{RAB}^{c}$, this state can be rewritten as

$$\mu = \sum_{c_1, ... , c_n} q(c_1) ... q(c_n) |c_1 ... c_n\rangle |c_1 ... c_n\rangle \otimes |c_1 ... c_n\rangle |c_1 ... c_n\rangle |c_1 ... c_n\rangle |c'_1 ... c'_n \otimes \left( \frac{1}{n} \sum_{j=1}^n \frac{p(c_j)}{q(c_j)} \psi_{RAB}^{c_j} \right).$$

Define $\gamma(c_1, c_2, ... , c_n) = \frac{1}{n} \sum_{j=1}^n \frac{p(c_j)}{q(c_j)}$. Introducing a new register $J$, define the following state, for every $c_1, c_2 ... , c_n$:

$$|\theta^{c_1, c_2, ... , c_n}\rangle_{RAB} \overset{\text{def}}{=} \frac{1}{\sqrt{\gamma(c_1, c_2, ... , c_n)}} \sum_{j=1}^n \frac{1}{\sqrt{n}} \sqrt{\frac{p(c_j)}{q(c_j)}} |c_j\rangle |\psi_{RAB}^{c_j}\rangle |J\rangle.$$

Now, consider the following extension of $\mu_{RBC_1 C'_1 ... C_n C'_n}$,

$$\mu_{RBC_1 C'_1 ... C_n C'_n} \overset{\text{def}}{=} \sum_{c_1, ... , c_n} \gamma(c_1, ... , c_n) \cdot q(c_1) ... q(c_n) |c_1 ... c_n\rangle |c_1 ... c_n\rangle \otimes |c_1 ... c_n\rangle |c_1 ... c_n\rangle |c'_1 ... c'_n \otimes |\theta^{c_1 ... c_n}\rangle |\theta^{c_1 ... c_n}\rangle_{RAB}.$$ 

Consider the following fictitious protocol $\mathcal{P}_1$.

1. Alice, Bob and Referee start by sharing the state $\mu_{RBAJC_1 C'_1 ... C_n C'_n}$ between themselves where Alice holds registers $A JC_1 ... C_n$, Referee holds the register $R$ and Bob holds the registers $BC'_1 C'_2 ... C'_n$.
2. Alice measures the register $J$ and obtains the measurement outcome $j \in [n]$. She sends the integer $\lceil (j - 1) / b \rceil$ to Bob using classical communication.
3. Bob swaps registers $C'_b \lceil (j - 1) / b \rceil + 1, C'_b \lceil (j - 1) / b \rceil + 2, ... , C'_b \lceil (j - 1) / b \rceil + b$ with the set of registers $C'_1, C'_2, ... , C'_b$ in that order. In the same fashion, Alice swaps registers $C_b \lceil (j - 1) / b \rceil + 1, C_b \lceil (j - 1) / b \rceil + 2, ... , C_b \lceil (j - 1) / b \rceil + b$.
with the set of registers $C_1, C_2, \ldots, C_b$ in that order. At this step of the protocol, the joint state in the registers $RBAC_1C_1 \ldots C_b$ is
\[
\mu_{RBAC_1C_1 \ldots C_b}(2) = \sum_{c_1, \ldots, c_b} q(c_1) \ldots q(c_b) |c_1 \ldots c_b\rangle \langle c_1 \ldots c_b|_{C_1 \ldots C_b} \otimes |c_1 \ldots c_b\rangle \langle c_1 \ldots c_b|_{C_1 \ldots C_b} \otimes \left( \frac{1}{b} \sum_{j=1}^b p(c_j) \right) |\psi^{C_j}\rangle |RAB\rangle
\]
\[
= \frac{1}{b} \sum_{j=1}^b \Psi_{RBAC_1C_1} \otimes \sigma_{C_1} \otimes \ldots \otimes \sigma_{C_{j-1}} \otimes \sigma_{C_{j+1}} \otimes \ldots \otimes \sigma_{C_b}.
\]
4. Define,
\[
\Pi_j \overset{\text{def}}{=} I_{C_1} \otimes \ldots I_{C_{j-1}} \otimes \Pi_{BC_j} \otimes I_{C_{j+1}} \otimes \ldots \otimes I_{C_b} \quad \text{and} \quad \Pi := \sum_j \Pi_j.
\]
Bob applies the measurement
\[
\mathcal{A}(X) = \sum_j \sqrt{\Pi_j \Pi_j} \sqrt{\Pi_j} \Pi_j \Pi_j \otimes |j\rangle \langle j|_O,
\]
where $O$ is the outcome register, and upon obtaining the outcome $j$, swaps $C_j$, $C_j'$.
5. Alice, who already knows the correct value of $j$, swaps $C_j$ with $C_1$.
6. Final state is obtained in the registers $RABC_1C_1'$. We call it $\Phi^{1}_{RABC_1C_1'}$.

We have the following claim.

**Claim 1.** It holds that $P(\Phi^{1}_{RABC_1C_1'}, \Psi_{RABC_1C_1'}) \leq \sqrt{16\varepsilon}$.

**Proof.** Applying the measurement $\mathcal{A}$ to the state $\mu_{RABC_1C_1 \ldots C_b}(2)$, we obtain the state $\mathcal{A}(\mu_{RABC_1C_1 \ldots C_b}(2))$. Let $p_{i,j}$ be defined as follows:
\[
p_{i,j} \overset{\text{def}}{=} \text{Tr}(\Pi_j \Pi_j \Pi_{j-1} \Pi_{j+1} \ldots \Pi_{b}) \Psi_{RBAC_1C_1} \otimes \sigma_{C_1} \otimes \ldots \otimes \sigma_{C_{j-1}} \otimes \sigma_{C_{j+1}} \otimes \ldots \otimes \sigma_{C_b}.
\]
Define the state
\[
\mu^{(4)} = \frac{1}{b} \sum_i \Psi_{RBAC_1C_1} \otimes \sigma_{C_1} \otimes \ldots \otimes \sigma_{C_{i-1}} \otimes \sigma_{C_{i+1}} \otimes \ldots \otimes \sigma_{C_b} |i\rangle \langle i|_O.
\]
From Fact[8] we find that
\[
F(\mathcal{A}(\mu^{(2)}), \mu^{(4)}) \geq \left( \frac{1}{b} \sum_i p_{i,i} \right)^{3/2}.
\]
Now using Hayashi-Nagaoka inequality (Fact[9]), we obtain
\[
\frac{1}{b} \sum_{i \neq j} p_{i,j} \leq \frac{1}{b} \sum_j 4 \text{Tr}((I - \Pi_j) \Psi_{BC_j} \otimes \sigma_{C_1} \otimes \ldots \otimes \sigma_{C_{j-1}} \otimes \sigma_{C_{j+1}} \otimes \ldots \otimes \sigma_{C_b})
\]
\[+ \frac{1}{b} \sum_j 2 \text{Tr}((\sum_{i \neq j} \Pi_i) \Psi_{BC_j} \otimes \sigma_{C_1} \otimes \ldots \otimes \sigma_{C_{j-1}} \otimes \sigma_{C_{j+1}} \otimes \ldots \otimes \sigma_{C_b})
\]
\[= \frac{2}{b} \sum_j \text{Tr}((I - \Pi_j) \Psi_{BC_j}) + \frac{4}{b} \sum_j \text{Tr}((\sum_{i \neq j} \Pi_i) \Psi_{B} \otimes \sigma_{C_j})
\]
\[\leq 2\varepsilon^2 + 4(b - 1) \frac{\varepsilon^2}{b} \leq 6\varepsilon^2.
\]
Consider the following protocol $P$. Notice that in registers $\Phi$. Let

Thus, this implies using Claim 1 and triangle inequality for purified distance 1 that

\[
F^2(\mu^4, A(\mu^2)) \geq (1 - 6\varepsilon^2)^3 \geq 1 - 18\varepsilon^2.
\]

Swapping register $C_j^\prime$ and $C_1$, controlled on value $j$ in register $O$, on the state $\mu^4$ gives the state $\Psi_{RABC_1}^\prime$ in registers $RABC_1$. Moreover, Alice has already swapped $C_j, C_1$ which are classical copies of $C_j^\prime, C_1^\prime$. Thus, the claim follows.

This shows that protocol $P_1$ succeeds with fidelity as given in the claim. Now we proceed to construct the actual protocol. Consider the state,

\[
\xi_{RBC_1C_1^\prime \ldots C_nC_n^\prime} \overset{\text{def}}{=} \Psi_{RB} \otimes \sigma_{C_1C_1^\prime} \ldots \otimes \sigma_{C_nC_n^\prime}.
\]

Define the state

\[
\xi_{RABC_1C_1^\prime \ldots C_nC_n^\prime} \overset{\text{def}}{=} |\Psi\rangle\langle \Psi|_{RABC_1C_1^\prime \ldots C_nC_n^\prime} \otimes \sigma_{C_1C_1^\prime} \ldots \otimes \sigma_{C_nC_n^\prime}.
\]

Using the corollary of convex-split lemma (Corollary 1) and choice of $n$ we have,

\[
P(\xi_{RBC_1C_1^\prime \ldots C_nC_n^\prime}, \mu_{RBC_1C_1^\prime \ldots C_nC_n^\prime}) \leq 5\varepsilon.
\]

Notice that $\xi_{C_1C_1^\prime \ldots C_nC_n^\prime} = \mu_{C_1C_1^\prime \ldots C_nC_n^\prime}$. Thus, using Fact 1 we find that there exists an isometry depending on $c_1, c_2, \ldots, c_n$: $U^{c_1 \ldots c_n}: ACC \rightarrow AJ$ such that,

\[
P\left(\left(\sum_{c_1 \ldots c_n} |c_1 \ldots c_n\rangle\langle c_1 \ldots c_n| \otimes U^{c_1 \ldots c_n} \right)\xi_{RACC_1C_1^\prime \ldots C_nC_n^\prime} \left(\sum_{c_1 \ldots c_n} |c_1 \ldots c_n\rangle\langle c_1 \ldots c_n| \otimes U^{c_1 \ldots c_n}\right)^\dagger, \right)
\]

\[
\nu_{RABC_1C_1^\prime \ldots C_nC_n^\prime} = P(\xi_{RBC_1C_1^\prime \ldots C_nC_n^\prime}, \mu_{RBC_1C_1^\prime \ldots C_nC_n^\prime}) \leq 5\varepsilon.
\]

Consider the following protocol $\mathcal{P}$.

1. Alice, Bob share $n$ copies of the state $\sigma_{CC_1^\prime}$ as $\sigma_{C_1C_1^\prime} \otimes \ldots \otimes \sigma_{C_nC_n^\prime}$. Alice, Bob and Referee share the state $|\Psi\rangle_{RABC_1}$ between themselves where Alice holds registers $ACC$, Referee holds the register $R$ and Bob holds the registers $B$.

2. Conditioned on the values $c_1, c_2, \ldots, c_n$ in registers $C_1C_2 \ldots C_n$, Alice applies the isometry $U^{c_1 \ldots c_n}$ on her register $ACC$.

3. Alice and Bob simulate protocol $P_1$ from Step 2. onwards.

Let $\Phi'_{RABC_1C_1^\prime}$ be the output of protocol $\mathcal{P}$. Since quantum maps (the entire protocol $P_1$ can be viewed as a quantum map from input to output) do not decrease fidelity (monotonicity of fidelity under quantum operation, Fact 1), we have,

\[
P(\Phi'_{RABC_1C_1^\prime}, \Phi'_{RABC_1C_1^\prime}) \leq 5\varepsilon.
\]

This implies using Claim 1 and triangle inequality for purified distance 1 that

\[
P(\Phi'_{RABC_1C_1^\prime}, \Psi_{RABC_1C_1^\prime}) \leq 10\varepsilon.
\]

That is, $\Phi'_{RABC_1C_1^\prime} \in \mathcal{B}_{10\varepsilon}(\Psi_{RABC_1C_1^\prime})$. The number of bits communicated by Alice to Bob in $\mathcal{P}$ is equal to the number of bits communicated in $P_1$ and is upper bounded by:

\[
\log(n/b) \leq D_{\text{max}}^\varepsilon(\Psi_{RBC} \parallel \Psi_{RB} \otimes \sigma_C) - D_{H}^\varepsilon(\Psi_{BC} \parallel \Psi_B \otimes \sigma_C) + 6 \log \left(\frac{1}{\varepsilon}\right).
\]

\[\square\]
Acknowledgement

We thank Mark M. Wilde for introducing us to this problem and for many helpful comments. We also thank Eneet Kaur for helpful feedback on our manuscript.

This work is supported by the Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant Random numbers from quantum processes MOE2012-T3-1-009.

References

[1] A. Winter, “‘extrinsic’ and ‘intrinsic’ data in quantum measurements: Asymptotic convex decomposition of positive operator valued measures,” *Communications in Mathematical Physics*, vol. 244, no. 1, pp. 157–185, 2004.

[2] I. Devetak, “Distillation of local purity from quantum states,” *Phys. Rev. A*, vol. 71, p. 062303, Jun 2005.

[3] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, “Local information as a resource in distributed quantum systems,” *Phys. Rev. Lett.*, vol. 90, p. 100402, Mar 2003.

[4] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke, “Local versus nonlocal information in quantum-information theory: Formalism and phenomena,” *Phys. Rev. A*, vol. 71, p. 062307, Jun 2005.

[5] I. Devetak, A. W. Harrow, and A. J. Winter, “A resource framework for quantum shannon theory,” *IEEE Transactions on Information Theory*, vol. 54, pp. 4587–4618, Oct 2008.

[6] H. Krovi and I. Devetak, “Local purity distillation with bounded classical communication,” *Phys. Rev. A*, vol. 76, p. 012321, Jul 2007.

[7] M. M. Wilde, P. Hayden, F. Buscemi, and M.-H. Hsieh, “The information-theoretic costs of simulating quantum measurements,” *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 45, p. 453001, 2012.

[8] F. Leditzky, M. M. Wilde, and N. Datta, “Strong converse theorems using rnyi entropies,” *Journal of Mathematical Physics*, vol. 57, no. 8, p. 082202, 2016.

[9] R. Renner, “Security of quantum key distribution.” PhD Thesis, ETH Zurich, Diss. ETH No. 16242, arXiv:quant-ph/0512258, 2005.

[10] M. Tomamichel, R. Colbeck, and R. Renner, “Duality between smooth min- and max-entropies,” *IEEE Transactions on Information Theory*, vol. 56, pp. 4674 – 4681, 2010.

[11] M. Tomamichel, “A framework for non-asymptotic quantum information theory,” 2012. PhD Thesis, ETH Zurich.

[12] N. Datta, “Min- and max- relative entropies and a new entanglement monotone,” *IEEE Transactions on Information Theory*, vol. 55, pp. 2816–2826, 2009.

[13] W. F. Stinespring, “Positive functions on c*-algebras,” *Proceedings of the American Mathematical Society*, p. 211216, 1955.

[14] H. Barnum, C. M. Cave, C. A. Fuch, R. Jozsa, and B. Schmacher, “Noncommuting mixed states cannot be broadcast,” *Phys. Rev. Lett.*, vol. 76, no. 15, pp. 2818–2821, 1996.

[15] G. Lindblad, “Completely positive maps and entropy inequalities,” *Commun. Math. Phys.*, vol. 40, pp. 147–151, 1975.

[16] A. Uhlmann, “The “transition probability” in the state space of a *-algebra,” *Rep. Math. Phys.*, vol. 9, pp. 273–279, 1976.
[17] A. Winter, “Coding theorem and strong converse for quantum channels.” *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.

[18] T. Ogawa and H. Nagaoka, “A new proof of the channel coding theorem via hypothesis testing in quantum information theory,” in *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, pp. 73–, 2002.

[19] M. Hayashi and H. Nagaoka, “A general formula for the classical capacity of a general quantum channel,” in *Proceedings IEEE International Symposium on Information Theory*, pp. 71–, 2002.

[20] M. Berta, M. Christandl, and R. Renner, “The Quantum Reverse Shannon Theorem based on one-shot information theory,” *Commun. Math. Phys.*, vol. 306, pp. 579–615, 2011.

[21] A. Anshu, R. Jain, and N. A. Warsi, “One shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach.” https://arxiv.org/abs/1702.01940, 2017.

[22] A. Anshu, V. K. Devabathini, and R. Jain, “Quantum message compression with applications.” arXiv:1410.3031, 2014.