Random coding exponents galore via decoupling

Naresh Sharma
Tata Institute of Fundamental Research
Mumbai 400005, India
Email: nsharma@tifr.res.in
April 28, 2015

Abstract

To the best of our knowledge, a missing piece in quantum information theory, with very few exceptions, is providing the random coding exponents for quantum information-processing protocols. We remedy the situation by providing these exponents for a variety of protocols including those at the top of the family tree of protocols. Our line of attack is to provide an exponential bound on the decoupling error for a restricted class of completely positive maps where a key term in the exponent is in terms of a Rényi $\alpha$-information-theoretic quantity for any $\alpha \in (1,2]$. Among the protocols covered are fully quantum Slepian-Wolf, quantum state merging, quantum state redistribution, quantum communication across channels with or without entanglement assistance, and communication across broadcast channels.

1 Introduction

Analysis of optimal resources needed/generated in an information-processing protocol is one of the holy grails of information theory [1, 2, 3, 4, 5]. Nice answers in terms of information-theoretic quantities are obtained, in general, for large copies such as of inputs and channel uses. One part in establishing these answers is the achievability that says that for resources arbitrarily close to the optimal, there exists a protocol accomplishing the task with arbitrarily small error.

Achievability proofs come in various flavors and we list some of them (not in a chronological order). One way is via the law of large numbers (or typicality) that involves making statements for large copies. Another way is via the smooth information-theoretic quantities that are defined in terms of a semi-definite program (see Refs. [6, 7] and references therein). This method has the advantage that one can make statements for any number of copies and it matches the optimal answer for large number of copies using the law of large numbers. A third way has been via the random coding exponents, i.e.,
one makes statements for any number of copies by obtaining an exponential bound on
the error of the protocol. In many comparisons with the second method, this method
provides stronger bounds and was pioneered by Gallager who obtained such bounds for
the classical capacity [8, 9]. Yet another method has been via the optimal terms in the
asymptotic expansions of the rate at which the resources are generated or used and this
was pioneered by Strassen [10].

It is the Gallager’s approach that would be further investigated in this paper. If one
scours the literature on the quantum random coding exponents, one finds that not much
work has been done on this topic. Indeed, apart from Burnashev and Holevo [11], Holevo
[12], and Hayashi [13], no other work, to the best of the author’s knowledge, provides
random coding exponents for the quantum protocols. (Exponential bounds on the error
for the Schumacher compression can be obtained without much difficulty leveraging the
analysis for the classical source compression [3].) Burnashev and Holevo [11] provide the
reliability function (loosely defined as the best exponent one could get for large number
of copies [9]) for sending classical information across the quantum channel for the case
of pure states, and Holevo [12] extends it for the case of commuting density matrices.
Hayashi provides a random coding exponent for the same protocol for general density
matrices but his exponent when specialized to classical does not match with Gallager’s
[12, 8].

Quantum information theory is much richer than the classical and with a plethora of
protocols (one can just glance at the family tree of quantum protocols [14, 15] to appreciate
this), it is not just important to provide the random coding exponents but, if possible, also
a unified approach to get these exponents for a variety of protocols.

Where would such a unified approach come from? An answer lies in decoupling, a
phenomenon where random evolution of a part of the quantum system would, on the
average, make it decouple from the other part. That decoupling would be useful for
quantum error correction was first observed by Schumacher and Nielsen [16]. It has sub-
sequently been recognized as a building block in quantum information theory (see Refs.
[17, 18] and references therein).

The decoupling theorem quantifies the average error between the state, part of which
is randomly evolved, and the completely decoupled state, and is now known in various
versions. We go through some of them not necessarily in the chronological order. The
one provided by Hayden et al [19] gives a bound in terms of dimensions of the quantum
systems involved and this, with an appeal to typicality for large copies, yields the optimal
answers – similar approach is followed by Abeyesinghe et al [20]. Dupuis et al provide
another version that gives a bound in terms of smooth entropies [21].

Another version by Dupuis gives an exponential bound for any number of copies and
the exponent has two Rényi 2-conditional entropies: first one is computed using the den-
sity matrix that is evolved and the second one is computed using the Choi-Jamiołkowski
representation of a map [17].

Since this version gives an exponential bound, it seems close to the stated purpose of
this paper but it is not quite there simply because for the random coding exponents, we
shall need the first term to be in terms of Rényi $\alpha$-conditional entropies for $\alpha$ arbitrarily close to $1$. It is not necessary to strengthen the second term that determines the rate.

Could there be a way of modifying Dupuis’ bound? This paper stems from asking this question, answering it in the affirmative, and then applying the new version to obtain the random coding exponents for a variety of protocols. In particular, we are able to replace the first term by a Rényi $\alpha$-conditional entropy for all $\alpha \in (1, 2]$ (although adding some inconsequential terms in the process). We do this by leveraging ideas from the independent works of Dupuis and Hayashi [17, 3].

Some of the protocols we analyze are at the top of the family tree of protocols and the author didn’t encounter any protocol that could be analyzed by other versions of the decoupling theorem but not from the version provided in this paper. The application of our version of the decoupling theorem for these protocols is, in some cases, but not always, inspired by the application of other versions of the decoupling theorem for these protocols.

We don’t address how close the exponent in the proposed bounds might be to the reliability function. There is, however, one resemblance between the exponents we obtain and the reliability function for the classical case (in certain regimes), which is that in both the cases, it is in terms of Rényi $\alpha$-information-theoretic quantities.

The structure of the paper is as follows. Section 2 provides the notation and definitions used throughout this paper. Section 3 provides a new version of the decoupling theorem. (There is a more general version provided as well in Appendix C although we don’t use it!) The subsequent sections apply this version to various protocols. Following protocols are analyzed: Schumacher compression, fully quantum Slepian-Wolf, fully quantum reverse Shannon, quantum state merging, quantum communication with side information at the transmitter with or without entanglement assistance, entanglement-assisted classical communication, quantum state distribution, quantum communication across broadcast channels, and destroying correlations by adding classical randomness. The lemmas are provided in the appendix so as to not interrupt the flow.

## 2 Notation and Preliminaries

Let $\mathcal{H}_A$ be the Hilbert space associated with the quantum system $A$. We shall confine ourselves to the finite dimensional Hilbert spaces in this paper and $|A|$ denotes the dimension of $\mathcal{H}_A$. $A \cong B$ implies that $|A| = |B|$. For a system $A$, we denote $A^n$ to be a quantum system described by $\bigotimes_{i=1}^{n} \mathcal{H}_{A_i}$, where $A_i \cong A$, $i = 1, \ldots, n$. Let $L(\mathcal{H}_A, \mathcal{H}_B)$ be the set of all matrices from $\mathcal{H}_A$ to $\mathcal{H}_B$ and $L(\mathcal{H}_A)$ denotes $L(\mathcal{H}_A, \mathcal{H}_A)$. Let $\text{Herm}(\mathcal{H}_A)$, $\text{Pos}(\mathcal{H}_A) \subseteq L(\mathcal{H}_A)$ be the set of Hermitian and positive semidefinite matrices respectively. Let $\text{D}(\mathcal{H}_A) \subseteq \text{Pos}(\mathcal{H}_A)$ be the set of unit trace matrices and $\text{D}_\leq(\mathcal{H}_A) \subseteq \text{Pos}(\mathcal{H}_A)$ be the set of matrices with trace not greater than $1$. Let $\nu_{\sigma^A}$ be the number of distinct eigenvalues of $\sigma^A \in \text{Herm}(\mathcal{H}_A)$. For $\rho^A, \sigma^A \in \text{Herm}(\mathcal{H}_A)$, let $\{\rho^A \geq \sigma^A\}$ denote the projector onto the subspace spanned by the eigenvectors corresponding to the non-negative eigenvalues of $\rho^A - \sigma^A$. Let $X \cdot \rho \equiv X \rho X^\dagger$. For $X \in L(\mathcal{H}_A, \mathcal{H}_B)$ (also denoted as $X^{A\rightarrow B}$), the trace
norm, \( \|X\|_1 \) is the sum of its singular values. The Fidelity between \( \rho, \sigma \in \text{Pos}(\mathcal{H}_A) \) is \( F(\rho, \sigma) \equiv \|\sqrt{\rho\sigma}\|_1. \)

Let \( \mathbb{U}(A) \) be a Unitary 2-design on a quantum system \( A \) (see Ref. [17] and references therein). For a function \( f : \mathbb{U}(A) \to \mathcal{L}(\mathcal{H}_E) \), \( E_U f(U) \) denotes the expectation taken over a random Unitary \( U \) distributed uniformly on \( \mathbb{U}(A) \).

Let \( |\Phi\rangle^{AA'} \) be the maximally entangled state (MES) on \( AA' \), i.e., for \( A \cong A' \), orthonormal bases \( \{ |i\rangle^A \} \) and \( \{ |i\rangle^{A'} \} \), \( |\Phi\rangle^{AA'} \equiv |A\rangle^{1/2} \sum_i |i\rangle^A |i\rangle^{A'} \). Let the maximally mixed state in \( \mathcal{H}_A \) be denoted by \( \pi^A \equiv \mathbb{1}^A/|A| \), where \( \mathbb{1}^A \) is the Identity matrix. The zero matrix (with all entries as zero) is denoted by \( 0 \).

A matrix \( V^{A\rightarrow B} \) is an isometry if either \( V^\dagger V = 1 \) or \( VV^\dagger = 1 \), and is a partial isometry if its singular values are either 0 or 1. A full-rank partial isometry \( V^{A\rightarrow B} \) has rank \( \min\{|A|, |B|\} \).

The Kronecker delta function is \( \delta_{j,k} = 1 \) if \( j = k \), and 0 otherwise. The indicator function \( \text{ind}_{\text{condition}} = 1 \) if condition is true, and 0 otherwise. The partial trace over \( B \) of \( \rho^{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \) is denoted by \( \text{Tr}_B \rho^{AB} \) or \( \rho^A \). For a pure state \( |\Psi\rangle^{AB} \), \( \Psi^{AB} = |\Psi\rangle \langle \Psi|^{AB} \), and it does not necessarily imply that \( \Psi^A \) is also a pure state. The logarithm is defined as \( \ln(\varepsilon) \equiv \sqrt{\varepsilon}(4 + 3\varepsilon) \).

### 2.1 Super-operators

A super-operator \( \mathcal{T}^{A\rightarrow B} \) is a map from \( \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B) \). Important classes include completely positive maps \( \mathcal{T}^{A\rightarrow B} \), which map \( \text{Pos}(\mathcal{H}_A \otimes \mathcal{H}_R) \) to \( \text{Pos}(\mathcal{H}_B \otimes \mathcal{H}_R) \) for any ancilla \( R \), and completely positive and trace preserving (cptp) maps which are completely positive and have an additional property that the trace is preserved.

The Choi-Jamiołkowski representation of a map \( \mathcal{T}^{A\rightarrow E} \) is given by \( \omega^{E_{A'}} = \mathcal{T}^{A\rightarrow E}(\Phi^{AA'}) \).

To a completely positive map, we associate a quantity \( \Theta(\mathcal{T}) \) defined as the negative of the Rényi old 2-conditional entropy (defined in Section 2.2) and is given by

\[
\Theta(\mathcal{T}) \equiv -H^\text{old}_2(A'|E)_{\omega^{E_{A'}}}.
\]

Concatenation of two maps, i.e., \( \mathcal{E} \) followed by \( \mathcal{D} \) is denoted by \( \mathcal{D} \circ \mathcal{E} \), and with a slight abuse of notation, for an isometry \( V \) and a map \( \mathcal{E} \), \( \mathcal{E} \circ V(\rho) \) denotes \( \mathcal{E}(V \cdot \rho) \), and \( V \circ \mathcal{E}(\rho) \) denotes \( V \cdot \mathcal{E}(\rho) \).

We now define three maps. For \( \sigma^{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \), \( Q_A(\sigma^{AB}) \equiv |A|\text{Tr}_A\sigma^{AB}(\sigma^{AB})^\dagger - \sigma^{B}(\sigma^{B})^\dagger \). For \( \rho, \sigma \in \text{Pos}(\mathcal{H}_A) \), the spectral decomposition \( \sigma = \sum_{i=1}^{\nu_\sigma} \lambda_i \Pi_i \) where \( \lambda_i \)'s are all distinct and \( \Pi_i \)'s are projectors, a pinching map in the eigenbasis of \( \sigma \) is defined as \( M_\sigma(\rho) = \sum_{i=1}^{\nu_\sigma} \Pi_i \rho \Pi_i \). Let \( W^{A\rightarrow B} \), \( |B| \leq |A| \), be a full-rank partial isometry. Then a compressive map \( C_W^{A\rightarrow B} \) is defined as \( C_W^{A\rightarrow B}(\rho^A) \equiv W\rho^AW^\dagger + \left[\text{Tr}(\mathbb{1}^A - W^\dagger W)\rho^A\right] \pi^B \).

**Definition 1** (Class-1 maps). A map \( \mathcal{T}^{A\rightarrow E} \) is said to be in class-1 if it is completely positive and for any \( \sigma \in \mathcal{L}(\mathcal{H}_A) \), \( E_U \|T(U \cdot \sigma)\|_1 < \|\sigma\|_1 \).

Note that all cptp maps fall under class-1. Another set of completely positive maps under class-1 are those with \( \text{Tr} \mathcal{T}(\mathbb{1}^A) = |A| \) (see Lemma 25 for proof). An example of
such a map (taken from Ref. [17]) that we shall use later in the paper is given by

$$\mathcal{T}_{W}^{A\rightarrow B}(\sigma^A) \equiv \frac{|A|}{|B|}(W^{A\rightarrow B} \cdot \sigma^A),$$

(2)

where $W^{A\rightarrow B}$, $|A| \geq |B|$, is a full-rank partial isometry.

### 2.2 Information-theoretic quantities

The quantum relative entropy from $\rho$ to $\sigma$ is given by $D(\rho||\sigma) \equiv \text{Tr}\rho(\log \rho - \log \sigma)$, the von Neumann entropy of $\rho^A \in D(\mathcal{H}_A)$ is given by $H(\rho) \equiv -\text{Tr}\rho^A \log \rho^A$. For a tripartite state $\rho^{ABC}$, the conditional entropy of $A$ given $B$ is given by $H(A|B)_{\rho} \equiv H(AB)_{\rho} - H(B)_{\rho}$, the conditional mutual information between $A$ and $B$ given $C$ is $I(A:B|C)_{\rho} \equiv H(A|C)_{\rho} - H(A|BC)_{\rho}$, and the coherent information is given by $I(AB|\rho) \equiv -H(A|B)_{\rho}$. The Rényi generalizations of the quantum relative entropy can be done in various ways and we mention two prominent candidates.

**Definition 2** (Rényi entropies). For $\alpha \in (0, 2]\backslash\{1\}$, from $\rho$ to $\sigma$, the quasi old $\alpha$-relative entropy is given by $Q^{\alpha}_{\text{old}}(\rho||\sigma) \equiv \text{Tr}\rho^\alpha \sigma^{1-\alpha}$, and the quasi sandwiched $\alpha$-relative entropy (proposed independently in Refs. [22, 23]) is given by $Q^{\alpha}_{\text{sand}}(\rho||\sigma) \equiv \text{Tr}\left(\sigma^{\frac{1-\alpha}{\alpha}} \rho^{\frac{1-\alpha}{\alpha}}\right)^{\alpha}$. The Rényi old (sandwiched) $\alpha$-relative entropy from $\rho$ to $\sigma$ is given by

$$D^{\alpha}_{\text{old(sand)}}(\rho||\sigma) \equiv \frac{1}{\alpha - 1} \log Q^{\alpha}_{\text{old(sand)}}(\rho||\sigma), \quad \alpha \in (0, 2]\backslash\{1\}.$$  

(3)

We can extend these definitions to include $\alpha = 1$ by taking limits and we drop the subscript and the superscript. The Rényi $\alpha$-conditional entropies of $A$ given $B$ are defined as

$$H^{\text{type}}_{\alpha}(A|B)_{\rho} \equiv -\inf_{\sigma_B \in D(\mathcal{H}_B)} D^{\text{type}}_{\alpha}(\rho^{AB}\|1^A \otimes \sigma^B)$$

(4)

$$\uparrow H^{\text{type}}_{\alpha}(A|B)_{\rho} \equiv -D^{\text{type}}_{\alpha}(\rho^{AB}\|1^A \otimes \rho^B),$$

(5)

where ‘type’ is ‘old’ or ‘sand’.

It follows from Refs. [24, 25, 22, 23] that for $\alpha \in (0, 2]\backslash\{1\}$ and a cptp map $\mathcal{E}$, $D^{\text{type}}_{\alpha}(\rho||\sigma) \geq D^{\text{type}}_{{\tilde{\alpha}}} [\mathcal{E}(\rho)||\mathcal{E}(\sigma)]$.

There are duality relations known for a tripartite pure state $\Psi^{ABC}$. One such example is $H^{\text{sand}}_{\alpha}(A|B)_{\Psi} + H^{\text{sand}}_{\alpha}(A|C)_{\Psi} = 0$, $\tilde{\alpha} = 1/\alpha$, $\alpha \in [0.5, 1) \cup (1, 2]$. Ref. [26] gives a complete list of duality relations. In the remainder of the paper, the ‘type’ superscript is dropped, and it implies that the expression holds for either one and one could pick one’s favorite. For example, $D_{\alpha}(\rho||\sigma)$ denotes either $D^{\text{old}}_{\alpha}(\rho||\sigma)$ or $D^{\text{sand}}_{\alpha}(\rho||\sigma)$. Furthermore, while invoking the above duality relations, since there are many options, we we also drop the downnarrow superscript from the conditional entropies and assume that appropriate superscript is implicitly assumed and $\tilde{\alpha}$ is assumed to be an appropriate function of $\alpha$ depending on the type of conditional entropies involved.
3 Yet another version of the decoupling theorem with a useful Rényification

In this section, we provide a version of the decoupling theorem where the crucial term in the exponent is in terms of a Rényi α-information-theoretic quantity for α ∈ (1, 2] instead of just α = 2 as provided in Ref. [17].

We leverage ideas from the independent works of Dupuis and Hayashi and in particular Theorem 3.7 in Ref. [17] and Lemma 9.2 in Ref. [3].

**Theorem 1.** Let \( \rho^{AR} \in \mathcal{D}(\mathcal{H}_{AR}) \) and \( \mathcal{T}^{A \to E} \) be a class-1 map. Then for \( \alpha \in (1, 2] \), a random Unitary \( U \) acting on \( A \), we have for any \( \sigma^R \in \mathcal{D}(\mathcal{H}_{R}) \),

\[
E_U \| \mathcal{T}(U \cdot \rho^{AR}) - \omega_T^E \otimes \rho^R \|_1 \leq 4 \exp \left\{ \frac{\alpha - 1}{2 \alpha} \left[ \log \nu_{\sigma^R} + D_\alpha(\rho^{AR} \| \mathbb{1}^A \otimes \sigma^R) + \Theta(\mathcal{T}) \right] \right\}.
\]

(6)

In particular, for \( n \) copies, a random Unitary over \( A^n \), and a class-1 map \( \mathcal{T}^{A^n \to E} \), we have

\[
E_U \| \mathcal{T} \left[ U \cdot (\rho^{AR})^{\otimes n} \right] - \omega_T^E \otimes (\rho^R)^{\otimes n} \|_1 \leq 4 \exp \left\{ \frac{\alpha - 1}{2 \alpha} \left[ |R| \log(n+1) - nH_\alpha(A|R)_\rho + \Theta(\mathcal{T}) \right] \right\}.
\]

(7)

**Proof.** For a \( \zeta > 0 \), let \( \Pi^{AR} \equiv \{ \mathcal{M}_{1^A \otimes \sigma^R}(\rho^{AR}) \geq \zeta \mathbb{1}^A \otimes \sigma^R \}, \hat{\Pi}^{AR} \equiv 1^{AR} - \Pi^{AR}, \mu_1 \equiv \omega_T^E \otimes \text{Tr}_A \{ \Pi^{AR} \rho^{AR} \}, \) and \( \mu_2 \equiv \omega_T^E \otimes \text{Tr}_A \{ \hat{\Pi}^{AR} \rho^{AR} \}. \) Note that \( \mu_1 + \mu_2 = \omega_T^E \otimes \rho^R \). We now have

\[
E_U \| \mathcal{T}(U \cdot \rho^{AR}) - \omega_T^E \otimes \rho^R \|_1 = E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] - \mu_1 + \mathcal{T} \left[ U \cdot (\hat{\Pi}^{AR} \rho^{AR}) \right] - \mu_2 \|_1 \\
\leq E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] - \mu_1 \|_1 + E_U \| \mathcal{T} \left[ U \cdot (\hat{\Pi}^{AR} \rho^{AR}) \right] - \mu_2 \|_1,
\]

(8)

where we have used the triangle inequality.

We attack the first term.

\[
E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] - \mu_1 \|_1 \leq E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] \|_1 + \| \mu_1 \|_1 \leq 2 E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] \|_1 \leq 2 \| \Pi^{AR} \rho^{AR} \|_1 \\
\leq 2 \| \Pi^{AR} \rho^{AR} \|_1 \leq 2 \zeta \frac{1-\alpha}{\alpha} \exp \left\{ \frac{\alpha - 1}{2} D_\alpha(\rho^{AR} \| \mathbb{1}^A \otimes \sigma^R) \right\}.
\]

(9)

(10)

(11)

(12)

where the first inequality follows from the triangle inequality, the second inequality follows from the convexity of the trace norm to have

\[
\| \mu_1 \|_1 = \| E_U \{ \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] \} \|_1 \leq E_U \| \mathcal{T} \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] \|_1.
\]

(13)
the third inequality follows from the definition of class-1 maps, the fourth inequality follows from Lemma 28 (proved by Hayashi [3]).

We now attack the second term. Let \( \Delta_U \equiv T \left[ U \cdot (\Pi^{AR} \rho^{AR}) \right] - \mu_2 \), and \( \theta^E \in D(H_E) \) be such that \( \Theta(T) = -D_{\text{old}}(\omega_T E^A / \theta \otimes 1^A) \). We now have

\[
E_U \| \Delta_{U}^{ER} \|_1 \leq E_U \sqrt{\text{Tr} \left[ (\theta^E)^{-1} \otimes (\sigma^R)^{-1} ] \Delta_U \Delta_U^1 \right]} 
\leq \sqrt{\text{Tr} \left[ (\theta^E)^{-1} \otimes (\sigma^R)^{-1} \right] E_U \left\{ \Delta_U \Delta_U^1 \right\} }
\leq \sqrt{\frac{|A|^2 \text{Tr} \left\{ (\theta^E)^{-1} \text{Tr}_{A'} (\omega_T E^{A'})^2 \right\} \text{Tr} \left\{ (\sigma^R)^{-1} \text{Tr}_{A} \Pi^{AR} (\rho^{AR})^2 \Pi^{AR} \right\} }{|A|^2 - 1}}
\leq \sqrt{\frac{\nu_{\alpha \kappa} \zeta |A|^2 \exp \left\{ \Theta(T) \right\} }{|A|^2 - 1}}
\]

where the first inequality follows since for any matrix \( \Upsilon \) and a density matrix \( \kappa \) (with appropriate dimensions), \( \| \Upsilon \|_1 \leq \sqrt{\text{Tr} \kappa^{-1} \Upsilon \Upsilon^\dagger} \), the second inequality follows from the concavity of \( x \rightarrow \sqrt{x} \), the third inequality follows from Lemma 27, and the last inequality follows from Lemma 29 (proved by Hayashi [3]). We now have

\[
E_U \| T(U \cdot \rho^{AR}) - \omega_T^E \otimes \rho^R \|_1 
\leq 2 \zeta^{\frac{\alpha}{1+\alpha}} \exp \left\{ \frac{\alpha - 1}{2} D_\alpha(\rho^{AR} \| 1^A \otimes \sigma^R) \right\} + \sqrt{\frac{\nu_{\alpha \kappa} \zeta |A|^2 \exp \left\{ \Theta(T) \right\} }{|A|^2 - 1}}. \quad (18)
\]

Note that \( \zeta \) is a free parameter and a convenient upper bound for

\[
\min \left( x \zeta^{\frac{\alpha}{1+\alpha}} + y \zeta^{1/2} \right)
\]

is obtained by choosing \( \zeta = (xy^{-1})^{\frac{\alpha}{1+\alpha}} \). Making that choice by feeding in appropriate values of \( x, y \), taking \( |A|^2/(|A|^2 - 1) \leq 4/3 \), noting that for \( \alpha \in (1, 2), 2^{1/\alpha}(4/3)^{(\alpha-1)/(2\alpha)} \leq 2 \), we get

\[
E_U \| T(U \cdot \rho^{AR}) - \omega_T^E \otimes \rho^R \|_1 
\leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ \log \nu_{\alpha \kappa} + D_\alpha(\rho^{AR} \| 1^A \otimes \sigma^R) + \Theta(T) \right] \right\}. \quad (20)
\]

Note that this is a convenient upper bound and while one could further optimize the choice of \( \zeta \), for \( \alpha \) near 1, the above bound is near the optimal.
For $n$ copies, a random Unitary over $A^n$, and a class-1 map $T^{A^n\rightarrow E}$, using (20), we have
\[
E_U \| T \left[ U \cdot (\rho^{AR})^{\otimes n} \right] - \omega_T^{E} \otimes (\rho^{R})^{\otimes n} \|_1 \\
\leq 4 \min_{\sigma^R} \exp \left\{ \frac{\alpha - 1}{2\alpha} [\nu(\sigma^R)\otimes n + D_\alpha \left( (\rho^{AR})^{\otimes n} \| (1^{A^n} \otimes (\sigma^R)^{\otimes n}) + \Theta(T) \right) \right\} \\
\leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} [nH_\alpha(A|R)_\rho + \Theta(T)] \right\}, \quad (21)
\]
where the first inequality follows from (20) and making a (possibly suboptimal) choice of a product state, and the second inequality follows since we have used a convenient upper bound that for any $\sigma^R \in D(H_R)$, $\log \nu(\sigma^R)^{\otimes n} \leq |R| \log(n + 1)$ (see Theorem 11.1.1 in Ref. [1] or Lemma 3.7 in Ref. [3]) and we choose $\sigma^R$ to be the one that minimizes $D_\alpha(\rho^{AR}\|1^{A} \otimes \sigma^R)$.

QED.

We now have the following corollary of Theorem 1.

**Corollary 2.** For $i = 1, ..., K$, let $T_i^{A^n\rightarrow E_i}$ be class-1 maps, and $\rho_i^{AR_i} \in D(H_{AR_i})$. Then there exists a Unitary $U$ over $A^n$ such that for all $i = 1, ..., K$, and $n \in \mathbb{N},$
\[
\| T_i \left[ U \cdot (\rho_i^{AR_i})^{\otimes n} \right] - \omega_{T_i}^{E_i} \otimes (\rho_i^{R_i})^{\otimes n} \|_1 \\
\leq 4K \exp \left\{ \frac{\alpha - 1}{2\alpha} [R_i \log(n + 1) - nH_\alpha(A|R_i)_{\rho_i} + \Theta(T_i)] \right\}. \quad (22)
\]

**Proof.** It follows from Theorem 1 that for all $i = 1, ..., K,$
\[
E_U \| T_i \left[ U \cdot (\rho_i^{AR_i})^{\otimes n} \right] - \omega_{T_i}^{E_i} \otimes (\rho_i^{R_i})^{\otimes n} \|_1 \\
\leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} [R_i \log(n + 1) - nH_\alpha(A|R_i)_{\rho_i} + \Theta(T_i)] \right\}. \quad (23)
\]
We now invoke Lemma I.7 in Ref. [17] to arrive at the claim. (Note that Lemma I.7 in Ref. [17] stipulates a multiplying factor of $K + 1$ instead of $K$ but it can be easily strengthened.)

It is possible to provide a unified theorem that yields both Theorem 1 and Lemma 9.2 in Ref. [3] as special cases. We do that in Theorem 33 (see Appendix C) and we note that although we provide this unified theorem, we don’t use it for the protocols treated later in the paper!

## 4 Schumacher compression

**Definition 3.** A $(\rho, \text{error}, n)$ Schumacher compression protocol consists of $n$ copies of $\rho^A$ (with a purification $\Psi^{AR}$), Alice applying an encoding ctp map $E : A^n \rightarrow B$, and Bob applying a decoding ctp map $D : B \rightarrow A^n$ such that for $\rho^{\tilde{A}^nR^n} \equiv D^{B \rightarrow \tilde{A}^n} \circ E^{A^n \rightarrow B} \left[ (\Psi^{AR})^{\otimes n} \right],$ 
\[
\| \rho^{\tilde{A}^nR^n} - (\Psi^{AR})^{\otimes n} \|_1 \leq \text{error}. \quad (24)
\]
(log |B|)/n is called the compression rate of the protocol. A real number \( R_C \) is called an achievable rate if there exist, for \( n \to \infty \), Schumacher compression protocols with compression rate approaching \( R_C \) and the error approaching 0.

**Theorem 3** (Schumacher, 1995 [27]). The smallest achievable rate for Schumacher compression is given by \( H(\rho) \).

We prove the following theorem.

**Theorem 4.** For any \( n \in \mathbb{N} \), there exists a \((\rho, \text{error}, n)\) Schumacher compression protocol such that for any \( \delta > 0 \),

\[
    \frac{\log |B|}{n} = |R| \frac{\log(n+1)}{n} + H_\delta(\rho) + \delta. \tag{25}
\]

and the error approaches 0 exponentially in \( n \).

**Proof.** Consider a full-rank partial isometry \( W^{A^n} \to B, |B| \leq |A|^n \). Then, using Theorem 1, there exists a Unitary \( U \) over \( A^n \),

\[
    \left\| \text{Tr}_B \circ \mathcal{T}^{A^n} _{W^{A^n} \to B} [U \cdot (\Psi^{AR})^{\otimes n}] - (\Psi^R)^{\otimes n} \right\|_1 \\
    \leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R| \log(n+1) - nH_\alpha(\rho) \right] + \Theta(\text{Tr}_B \circ \mathcal{T}_W) \right\} \\
    = 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R| \log(n+1) + nH_\alpha(\rho) - \log |B| \right] \right\} \equiv \epsilon_n, \tag{26}
\]

where we have used \( \Theta(\text{Tr}_B \circ \mathcal{T}_W) = - \log |B| \) from Lemma 21. We claim using Lemma 31 that there exists some Unitary \( V^{A^n} \to A^n \) such that

\[
    \left\| W^\dagger \cdot \mathcal{T}^{A^n} _{W} [U \cdot (\Psi^{AR})^{\otimes n}] - V \cdot (\Psi^R)^{\otimes n} \right\|_1 \leq h(\epsilon_n), \tag{27}
\]

and hence, using monotonicity of the trace norm under ctp maps (\( C_W \) in this case),

\[
    \left\| \mathcal{T}^{A^n} _{W} (U \cdot (\Psi^{AR})^{\otimes n}) - C_W [V \cdot (\Psi^R)^{\otimes n}] \right\|_1 \leq h(\epsilon_n), \tag{28}
\]

or

\[
    \left\| W^\dagger \cdot C_W [V \cdot (\Psi^{AR})^{\otimes n}] - W^\dagger \cdot \mathcal{T}^{A^n} _{W} (U \cdot (\Psi^{AR})^{\otimes n}) \right\|_1 \leq h(\epsilon_n). \tag{29}
\]

Define a partial isometry \( W_2^{A^n} \to B \) as \( W_2 \equiv WV \) and note that \( C_{W_2}(\sigma^{AR}) = C_{W}(V \cdot \sigma^{AR}) \). We now have

\[
    \left\| W_2^\dagger \cdot C_{W_2} [(\Psi^{AR})^{\otimes n}] - (\Psi^R)^{\otimes n} \right\|_1 \\
    = \left\| W^\dagger W^\dagger \cdot C_W [V \cdot (\Psi^{AR})^{\otimes n}] - W^\dagger \cdot (\Psi^R)^{\otimes n} \right\|_1 \\
    \leq \left\| W^\dagger \cdot C_W [V \cdot (\Psi^{AR})^{\otimes n}] - W^\dagger \cdot \mathcal{T}^{A^n} _{W} (U \cdot (\Psi^{AR})^{\otimes n}) \right\|_1 \\
    + \left\| W^\dagger \cdot \mathcal{T}^{A^n} _{W} (U \cdot (\Psi^{AR})^{\otimes n}) - V \cdot (\Psi^R)^{\otimes n} \right\|_1 \\
    \leq 2h(\epsilon_n), \tag{30}
\]

where we have used the triangle inequality, (27), and (29). It is now clear that Alice applies \( C_{W_2} \) and Bob applies the isometry \( W_2^\dagger \). The claim now follows readily. \( \Box \)
Remark: This is not the best exponent for this protocol and one can get the exponent that matches with the classical case (see Prob. 2.15 in Ref. [28]) when specialized and this can be construed from the treatment in Ref. [3]. Our purpose of stating the above proof is that the ideas would prove useful for other protocols later in this paper since it is based on decoupling.

5 Fully Quantum Slepian-Wolf (FQSW)

Definition 4. A \((\Psi, \text{error}, n)\) FQSW protocol consists of \(n\) copies of a pure state \(\ket{\Psi}^{ABR}\) shared between with Alice (A) and Bob (B), and reference system (R), Alice applying an encoding cptp map \(\mathcal{E} : A^n \rightarrow A_1 A_2\), quantum communication across a noiseless quantum channel from Alice to Bob \(\mathcal{T}^{A_2 \rightarrow B_2}\), and Bob applying a decoding cptp map \(\mathcal{D} : B_2 B^n \rightarrow B_1 \tilde{B}_3 B^n\) such that for

\[
\rho^{A_1 B_1 \tilde{B}_3 B^n R^n} \equiv \mathcal{D}^{B_2 B^n} \mathcal{T}^{A_2 \rightarrow B_2} \mathcal{E}^{A^n \rightarrow A_1 A_2} [\ket{\Psi^{ABR}}^{\otimes n}],
\]

\[
\left\| \rho^{A_1 B_1 \tilde{B}_3 B^n R^n} - \Phi^{A_1 B_1} \otimes [\Psi^{B_3 R^n}]^{\otimes n} \right\|_1 \leq \text{error}.
\]

The number \((\log |A_2|)/n\) is called the quantum communication rate and \((\log |A_1|)/n\) is called the entanglement gain rate of the protocol.

A pair of real numbers \((R_Q, R_E)\) is called an achievable rate pair if there exist, for \(n \rightarrow \infty\), FQSW protocols with quantum communication rate approaching \(R_Q\), entanglement gain rate approaching \(R_E\), and error approaching 0.

The achievable rates are described by the following theorem.

Theorem 5 (Abeyesinghe et al, 2009 [20]). The following rates are achievable for the FQSW:

\[
R_Q > \frac{1}{2} I(A : R)_\Psi \quad \text{and} \quad R_E < R_Q + H(A|R)_\Psi.
\]

Our goal in the remainder of this section is to provide the achievability of the above rate region with error decaying to 0 exponentially in \(n\).

Theorem 6. For any \(n \in \mathbb{N}\), there exists a FQSW protocol for any \(\alpha \in (1, 2]\) and \(\delta_1, \delta_2 > 0\), such that

\[
\frac{\log |A_2|}{n} = \frac{1}{2} \left[ H_\alpha(A) - H_\alpha(A|R)_\Psi \right] + (|B| + 1)|R| \frac{\log(n+1)}{2n} + \frac{\delta_1 + \delta_2}{2},
\]

\[
\frac{\log |A_1|}{n} = \frac{\log |A_2|}{n} + H_\alpha(A|R)_\Psi - |R| \frac{\log(n+1)}{n} - \delta_2,
\]

and the error approaches 0 exponentially in \(n\).
Proof. Let $W : A^n \to A_1A_2$ be a full-rank partial isometry with $|A_1||A_2| \leq |A|$. Then, using Corollary 2, we claim that there exists a Unitary $U$ over $A^n$ such that for $\alpha \in (1, 2]$,

$$
\| \text{Tr}_{A_1A_2} \circ T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] - (\Psi^{BR})^\otimes n \|_1
\leq 8 \exp \left\{ \alpha - 1 \frac{\beta}{2\alpha} \left[ |B| |R| \log(n + 1) - n H_\alpha(A|BR) + \Theta(\text{Tr}_{A_1A_2} \circ T_W) \right] \right\}
= 8 \exp \left\{ \alpha - 1 \frac{\beta}{2\alpha} \left[ |B| |R| \log(n + 1) - n H_\alpha(A) + \log |A_1||A_2| \right] \right\} \equiv \varepsilon_n, \quad (36)
$$

and

$$
\| \text{Tr}_{A_1A_2} \circ T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] - \pi^{A_1} \otimes (\Psi^{R})^\otimes n \|_1
\leq 8 \exp \left\{ \alpha - 1 \frac{\beta}{2\alpha} \left[ |R| \log(n + 1) - n H_\alpha(A|R) + \log |A_1| |A_2| \right] \right\} \equiv \vartheta_n, \quad (37)
$$

It follows from (37) and Lemma 31 that there exists an isometry $\tilde{U}_{A_2B^n \to B_1B_3B_5^n}$ such that

$$
\| \tilde{U} \cdot \{ T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] \} - \Phi^{A_1B_1} \otimes (\Psi^{B_3B_5^n R})^\otimes n \|_1 \leq h(\vartheta_n). \quad (38)
$$

It follows from (36) and Lemma 31 that there exists a Unitary $V^{A^n \to A^n}$ such that

$$
h(\varepsilon_n) \geq \| W^\dagger \cdot T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] - V \cdot (\Psi^{ABR})^\otimes n \|_1
\geq \| T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] - C_W [V \cdot (\Psi^{ABR})^\otimes n] \|_1
= \| \tilde{U} \cdot \{ T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] \} - \tilde{U} \cdot \{ C_W [V \cdot (\Psi^{ABR})^\otimes n] \} \|_1, \quad (39)
$$

where the second inequality follows from the monotonicity and noting that

$$
C_W \{ W^\dagger \cdot T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n] \} = T_W^{A^n \to A_1A_2} [U \cdot (\Psi^{ABR})^\otimes n], \quad (40)
$$

and the last equality is true since $(\tilde{U})^\dagger \tilde{U} = 1_{A_2B^n}$. Lastly, we use the triangle inequality, (38), and (39) to claim that

$$
\| \tilde{U}_{B_2B^n \to B_1B_3B_5^n} \cdot \{ T_{A_2 \to B_2} \circ C_W [V \cdot (\Psi^{ABR})^\otimes n] \} - \Phi^{A_1B_1} \otimes (\Psi^{B_3B_5^n R})^\otimes n \|_1
\leq h(\varepsilon_n) + h(\vartheta_n). \quad (41)
$$

It follows that the protocol consists of Alice applying $C_W^{A \to A_1A_2} \circ V^{A^n}$, and Bob applies $\tilde{U}$, albeit on $B_2B^n$ instead of $A_2B^n$.

It is now clear that if for $\alpha \in (1, 2], \delta_1, \delta_2 > 0$,

$$
\frac{\log |A_1|}{n} + \frac{\log |A_2|}{n} = H_\alpha(A) + |B| |R| \frac{\log(n + 1)}{n} + \delta_1, \quad (42)
$$

$$
\frac{\log |A_1|}{n} - \frac{\log |A_2|}{n} = H_\alpha(A|R) - |R| \frac{\log(n + 1)}{n} - \delta_2, \quad (43)
$$

11
then the error decays exponentially in $n$ to zero.

Note that in view of the trivial protocol where one qubit transmitted across a noiseless qubit channel from Alice and Bob generates one EPR pair shared by Alice and Bob (the reverse implication is not true), it makes sense to keep the quantum communication as small as possible, which is accomplished by making $\alpha$ close to 1, and $\delta_1, \delta_2$ close to 0.

The claim of the theorem now follows and we exhaust the entire achievable rate region as stipulated by Theorem 5.

6 Fully Quantum Reverse Shannon (FQRS)

The following definition is from Ref. [20].

**Definition 5.** A $(\Psi, \text{error}, n)$ FQRS protocol consists of $n$ copies of a pure state $|\Psi\rangle^{AA'}$ (both $A$ and $A'$ held by Alice), a MES $\Phi^{A_1B_1}$ shared between Alice ($A_1$) and Bob ($B_1$), a ctp map $\mathcal{N}^{A'\rightarrow B}$ with Stinespring representation $V^{A'\rightarrow BE}_N$ and $|\Psi\rangle^{ABE} = V^{A'\rightarrow BE}_N |\Psi\rangle^{AA'}$, Alice applying an encoding ctp map $\mathcal{E}^{A_1B_1\rightarrow A_2E^n}$, quantum communication across a noiseless quantum channel from Alice to Bob $I^{A_2\rightarrow B_2}$, and Bob applying a decoding ctp map $\mathcal{D}^{B_1B_2\rightarrow B^n}$ such that

$$|\rho^{A^nB^nE^n} - (\Psi^{ABE})^{\otimes n} \rangle_{A_1B_1} \ \text{and} \ |\rho^{A^nB^nE^n} - (\Psi^{ABE})^{\otimes n} \rangle_{A_1B_1} \leq \text{error.}$$

(44) (45)

The number $(\log |B_2|)/n$ is called the **quantum communication rate** and $(\log |B_1|)/n$ is called the **entanglement consumption rate** of the protocol.

A pair of real numbers $(R_Q, R_E)$ is called an **achievable rate pair** if there exist, for $n \rightarrow \infty$, FQRS protocols with quantum communication rate approaching $R_Q$, entanglement consumption rate approaching $R_E$, and error approaching 0.

The achievable rates are described by the following theorem.

**Theorem 7** (Abeyesinghe et al, 2009 [20]). The following rates are achievable for the FQRS:

$$R_Q > \frac{1}{2} I(A : B)_\Psi \quad \text{and} \quad R_E < R_Q + H(B|A)_\Psi.$$  

(46)

We now provide the random coding exponents for the achievability of this protocol.

**Theorem 8.** For any $n \in \mathbb{N}$, there exists a $(\Psi, \text{error}, n)$ FQRS protocol for any $\alpha \in (1, 2]$, $\delta_1, \delta_2 > 0$, such that

$$\frac{\log |B_2|}{n} = \frac{1}{2} [H_\alpha(B)_\Psi - H_\alpha(B|A)_\Psi] + (|E| + 1)|A| \frac{\log(n + 1)}{n} + \frac{\delta_1 + \delta_2}{2},$$

(47)

$$\frac{\log |B_1|}{n} = \frac{\log |B_2|}{n} + H_\alpha(B|A)_\Psi - |A| \frac{\log(n + 1)}{n} - \delta_2,$$

(48)

and the error approaches 0 exponentially in $n$.  

12
Proof. We note the insightful observation in Refs. [29, 20] that FQRS can be implemented using ideas from FQSW. Let \( W^{B^n} \rightarrow B_1B_2, |B_1||B_2| \leq |B|^n \), be a full-rank partial isometry. Then, using Corollary 2, we claim that there exists a Unitary \( U \) over \( B^n \) such that for \( \alpha \in (1, 2) \),

\[
\| \text{Tr}_{B_1B_2} \circ T_W^{B^n} [U \cdot (\Psi^{ABE})^\otimes n] - (\Psi^{AE})^\otimes n \|_1 \\
\leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A||E| \log(n + 1) - nH_\alpha(B|AE) + \Theta(\text{Tr}_{B_1B_2} \circ T_W) \right] \right\}
= 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A||E| \log(n + 1) + nH_\alpha(B) \log |B_1||B_2| \right] \right\} \equiv \varepsilon_n, \tag{49}
\]

and

\[
\| \text{Tr}_{B_2} \circ T_W^{B^n} [U \cdot (\Psi^{AB})^\otimes n] - \pi_{B_1} \otimes (\Psi^A)^\otimes n \|_1 \\
\leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A| \log(n + 1) - nH_\alpha(B|A) + \log |B_1||B_2| \right] \right\} \equiv \vartheta_n. \tag{50}
\]

Using (50) and Lemma 31, we claim that there exists an isometry \( \tilde{U}^{B_2E^n} \rightarrow A_1\tilde{B}^n\tilde{E}^n \) such that

\[
\| \tilde{U} \cdot T_W^{B^n} [U \cdot (\Psi^{ABE})^\otimes n] - \Phi^{A_1B_1} \otimes (\Psi^{\tilde{A}\tilde{B}\tilde{E}})^\otimes n \|_1 \leq h(\vartheta_n). \tag{51}
\]

Using the compressive map \( C_{\tilde{U}_1} : A_1\tilde{B}^n\tilde{E}^n \rightarrow A_2E^n \), (51), and monotonicity, we get

\[
\| W^\dagger \cdot T_W^{B^n} [U \cdot (\Psi^{AB})^\otimes n] - W^\dagger \cdot C_{\tilde{U}_1} [\Phi^{A_1B_1} \otimes (\Psi^{\tilde{A}\tilde{B}\tilde{E}})^\otimes n] \|_1 \leq h(\vartheta_n). \tag{52}
\]

Using (49) and Lemma 31, we claim that there exists a Unitary \( V \) over \( B^n \) such that

\[
\| W^\dagger \cdot T_W^{B^n} [U \cdot (\Psi^{ABE})^\otimes n] - V \cdot (\Psi^{ABE})^\otimes n \|_1 \leq h(\varepsilon_n). \tag{53}
\]

Using the triangle inequality, (52), and (53), we now have

\[
\| (V^\dagger W^\dagger) \circ T^{A_2 \rightarrow B_2} \circ C_{\tilde{U}_1} [\Phi^{A_1B_1} \otimes (\Psi^{\tilde{A}\tilde{B}\tilde{E}})^\otimes n] - (\Psi^{ABE})^\otimes n \|_1 \leq h(\varepsilon_n) + h(\vartheta_n). \tag{54}
\]

Hence, the FQRS protocol consists of Alice applying

\[
\mathcal{E}^{A^nA_1 \rightarrow A_2E^n} = C_{\tilde{U}_1} \circ (V^\dagger W^\dagger)^\otimes n
\]

and Bob applying \( \mathcal{D}^{B_1B_2 \rightarrow B^n} = V^\dagger W^\dagger \). The claim now follows readily. □
7 Quantum state merging

Definition 6. A (Ψ, error, n) state-merging protocol consists of n copies of a pure state |Ψ\(^{ABR}\)\rangle shared between Alice (A), Bob (B), and reference (R) inaccessible to both Alice and Bob, a MES Φ\(^{A_0B_0}\) shared between Alice (A₀) and Bob (B₀), and a LOCC quantum operation \(\mathcal{M}: A^n A₀ \otimes B^n B₀ \rightarrow A₁ \otimes B₁ B₂ B₂^n\) such that for

\[
\rho_{A₁B₁B₂^nB₂^nR^n} = \mathcal{M}\left[(|Ψ^{ABR}\rangle^{\otimes n} \otimes Φ^{A₀B₀})\right],
\]

where \(\mathcal{M}\) is a MES shared between Alice (A₁) and Bob (B₁).

Theorem 9 (Horodecki et al, 2005 [30]). The merging cost is the quantum conditional entropy \(H(A|B)_Ψ\). Furthermore, there exists a state-merging protocol that achieves this merging cost using one-way LOCC with a classical communication cost of at most \(\frac{(\log |A₀| - \log |A₁|)}{n}\) copies of a pure state \(|Ψ\rangle\) per input copy.

Proof. Our line of attack is similar to that in Ref. [30], Corollary 3.11 in Ref. [17], and Theorem 5.2 in Ref. [21].

The merging cost is given in the next theorem.

Theorem 10. For any \(n \in \mathbb{N}\), there exists a (Ψ, error, n) state merging protocol using one-way LOCC for arbitrary \(δ₁, δ₂ > 0\), such that

\[
\frac{\log |A₀| - \log |A₁|}{n} = H_A(A|B)_Ψ + |R|\frac{\log(n + 1)}{n} + δ₁,
\]

and a classical communication cost of at most

\[
H_A(A)_Ψ - H_A(A|R)_Ψ + \frac{(|B| + 1)|R|\log(n + 1) + 2}{n} + δ₁ + δ₂,
\]

with the error approaching 0 exponentially in \(n\).

Proof. Our line of attack is similar to that in Ref. [30], Corollary 3.11 in Ref. [17], and Theorem 5.2 in Ref. [21].
and we have

\[ \omega^{X_{A_1}} \equiv \mathcal{E}_{E_{A_0} \rightarrow X_{A_1}} \circ \mathcal{T}_W^{A^n \rightarrow E} (\pi^{A^n \cdot A_0}) \]

\[ = \mathcal{E}_{E_{A_0} \rightarrow X_{A_1}} \left( \pi^{E_{A_0}} \right) \]

\[ = \frac{1}{\zeta} \sum_{x=1}^{J} |x \rangle \langle x|^X \otimes \pi^{A_1} - |J \rangle \langle J|^X \otimes \frac{P_{A_1}}{|E| |A_0|} \]

where \( P_{A_1} \) is a projector with rank \( < A_1 \). Note that

\[ \left\| \omega^{X_{A_1}} - \pi^{X_{A_1}} \right\| _1 \leq \left\| \left( \frac{J}{\zeta} - 1 \right) \pi^{X_{A_1}} \right\| _1 + \left\| \frac{P_{A_1}}{|E| |A_0|} \right\| _1 < \left( \frac{J}{\zeta} - 1 \right) + \frac{1}{\zeta} < \frac{2}{\zeta} , \]

where the first inequality follows from the triangle inequality, the second one from \( \text{Tr} P_{A_1} < |A_1| \), and the third one from \( J - \zeta < 1 \).

Invoking Corollary 2, we first claim that there exists a Unitary \( U^{A^n \cdot A_0} \) such that for any \( \alpha \in (1, 2] \),

\[ \left\| \mathcal{E}_{E_{A_0} \rightarrow X_{A_1}} \circ \mathcal{T}_W^{A^n \rightarrow E} \left( U^{A^n \cdot A_0} \cdot \left( (\Psi^{ABR}) \otimes \pi^{A_0} \right) \right) - \omega^{A_1} \otimes (\Psi^{R}) \otimes \pi^{A_0} \right\| _1 \]

\[ \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R| \log(n + 1) - H_\alpha(A^n \cdot A_0 | R^n)_{\psi \otimes \pi^{A_0}} + \Theta(\mathcal{E} \circ \mathcal{T}_W) \right] \right\} \]

\[ \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R| \log(n + 1) + nH_\alpha(A \cdot B | \psi) - (\log |A_0| - \log |A_1|) \right] \right\} \equiv \psi_n, \]

(66)

(66) implies using Lemma 31 that there exists a Unitary \( V^{A^n \cdot A_0 \rightarrow A^n \cdot A_0} \) such that

\[ \left\| W^\dagger \circ \mathcal{T}_W^{A^n \rightarrow E} \left( U^{A^n \cdot A_0} \cdot \left( (\Psi^{ABR}) \otimes \pi^{A_0} \right) \right) - V^{A^n \cdot A_0 \rightarrow A^n \cdot A_0} \cdot (\Psi^{ABR}) \otimes \pi^{A_0} \right\| _1 \]

\[ \leq h(\varepsilon_n), \]
and, using monotonicity, this implies that
\[
\lVert T_{W}^{A_{n} \to E} \{ U^{A_{n} A_{0}} \cdot (\Psi^{ABR} \otimes n \otimes \Phi^{A_{0} B_{0}}) \} - \mathcal{C}_{W} [ V \cdot (\Psi^{ABR}) \otimes n \otimes \Phi^{A_{0} B_{0}} ] \rVert_{1} \leq h(\varepsilon_{n}). \tag{70}
\]

We now have
\[
\lVert \mathcal{E}_{E_{0} \to A_{1} X} \circ T_{W}^{A_{n} \to E} \{ U \cdot (\Psi^{AR}) \otimes n \otimes \pi^{A_{0}} \} - \pi^{A_{1} X} \otimes (\Psi^{R}) \otimes n \rVert_{1}
\leq \lVert \mathcal{E}_{E_{0} \to A_{1} X} \circ T_{W}^{A_{n} \to E} \{ U \cdot (\Psi^{AR}) \otimes n \otimes \pi^{A_{0}} \} - \omega^{A_{1} X} \otimes (\Psi^{R}) \otimes n \rVert_{1}
\]
\[
\leq \vartheta_{n} + 2 \frac{\zeta}{\xi} \equiv \beta_{n}, \tag{71}
\]

where the first inequality follows from the triangle inequality, and in the second inequality the first term is upper bounded using (66), and the last term by using (65). Let
\[
\xi_{x}^{A_{1} B_{n} B_{0}^{R_{n}}} \equiv \frac{J |A_{n}|}{|E|} (M_{x} W U) \cdot (\Psi^{ABR} \otimes n \otimes \Phi^{A_{0} B_{0}}) \tag{72}
\]
\[
\sigma^{X A_{1} B_{n} B_{0}^{R_{n}}} \equiv \mathcal{E}_{E_{0} \to A_{1} X} \circ T_{W}^{A_{n} \to E} \{ U \cdot (\Psi^{ABR}) \otimes n \otimes \Phi^{A_{0} B_{0}} \}
\]
\[
= \sum_{x=1}^{J} |x \rangle \langle x| \otimes \xi_{x}^{A_{1} B_{n} B_{0}^{R_{n}}}. \tag{73}
\]

Note that \(\xi_{x}^{A_{1} B_{n} B_{0}^{R_{n}}} \) is a pure state for all \(x\). Let \(\varepsilon'_{x} \equiv \lVert \xi_{x}^{A_{1} R_{n}} - \pi^{A_{1}} \otimes (\Psi^{R}) \otimes n \rVert_{1}\). We now have
\[
\beta_{n} \geq \lVert \sigma^{X A_{1} R_{n}} - \pi^{A_{1} X} \otimes (\Psi^{R}) \otimes n \rVert_{1} = \sum_{x=1}^{J} \frac{\varepsilon'_{x}}{J}. \tag{74}
\]

From Lemma 31, let \(V_{x}^{A_{n} B_{0} \to B_{1} \tilde{B}_{2}^{n} B_{n}^{2}} \) be an isometry such that
\[
\lVert V_{x}^{A_{n} B_{0} \to B_{1} \tilde{B}_{2}^{n} B_{n}^{2}} \cdot \xi_{x}^{A_{1} B_{n} B_{0}^{R_{n}}} - \Phi^{A_{1} B_{1}} \otimes (\Psi^{\tilde{B}_{2} B_{2}^{R_{n}}} \otimes n \rVert_{1} \leq h(\varepsilon'_{x}). \tag{75}
\]

Define a cptp map
\[
\mathcal{D}_{X B_{n} B_{0} \to B_{1} \tilde{B}_{2}^{n} B_{n}^{2}} \left( \sum_{x=1}^{J} |x \rangle \langle x| \otimes \gamma_{x}^{B_{n} B_{0}} \right) = \sum_{x=1}^{J} (V_{x} \cdot \gamma_{x}^{B_{n} B_{0}}). \tag{76}
\]
We now have
\[
\left\| \mathcal{D} \circ \mathcal{E} \circ \mathcal{T}_W \left[ U \cdot (\Psi^{ABR})^\otimes n \otimes \Phi^{A_0B_0} \right] - \Phi^{A_1B_1} \otimes (\tilde{\Psi}^{B_2B_2R})^\otimes n \right\|_1 \\
= \left\| \sum_{x=1}^J \frac{1}{J} V_{x}^{B^n A_0 \rightarrow B_1 \tilde{B}_2 B_2^*} \cdot \xi_x^{A_1B_1B_0R} - \Phi^{A_1B_1} \otimes (\tilde{\Psi}^{B_2B_2R})^\otimes n \right\|_1 \\
\leq \sum_{x=1}^J \frac{1}{J} \left\| V_{x}^{B^n A_0 \rightarrow B_1 \tilde{B}_2 B_2^*} \cdot \xi_x^{A_1B_1B_0R} - \Phi^{A_1B_1} \otimes (\tilde{\Psi}^{B_2B_2R})^\otimes n \right\|_1 \\
\leq \frac{1}{J} \sum_{x=1}^J \left( 2 \sqrt{\varepsilon'_x} + \sqrt{3} \varepsilon'_x \right) \\
\leq 2 \sqrt{\sum_{x=1}^J \varepsilon'_x / J} + \sqrt{3} \sum_{x=1}^J \varepsilon'_x / J \leq 2 \sqrt{\beta_n} + \sqrt{3} \beta_n, \quad (77)
\]
where the first inequality follows from the convexity of the trace norm, the second inequality follows from (75), the third and the fourth inequalities are straightforward, and the last inequality follows from (74). Using (70) and the triangle inequality, we have
\[
\left\| \mathcal{D} \circ \mathcal{E} \circ \mathcal{C}_W \left[ V \cdot (\Psi^{ABR})^\otimes n \otimes \Phi^{A_0B_0} \right] - \Phi^{A_1B_1} \otimes (\tilde{\Psi}^{B_2B_2R})^\otimes n \right\|_1 \\
\leq h(\varepsilon_n) + 2 \sqrt{\beta_n} + \sqrt{3} \beta_n. \quad (78)
\]

Alice performs \( \mathcal{E}^{A^n A_0 \rightarrow A_1 X} \circ \mathcal{C}_W \circ V \) and Bob performs \( \mathcal{D}^{X B^n B_0 \rightarrow B_1 \tilde{B}_2 B_2^*} \). Note that \( J = \frac{|E| |A_0|}{|A_1|} \leq \frac{2 |E| |A_0|}{|A_1|} \), since \( |E| |A_0| \geq |A_1| \) as per the assumption, determines the classical communication cost. We have now shown the existence of a state merging protocol using one-way LOCC for arbitrary \( \delta_1, \delta_2 > 0, \alpha \in (1, 2) \), with
\[
\frac{1}{n} \log \frac{|A_0|}{|A_1|} = H_{\alpha}(A|B)_{\Psi} + |R| \frac{\log(n+1)}{n} + \delta_1 \quad (79) \\
\frac{\log |E|}{n} = H_{\alpha}(A)_{\Psi} + |B| |R| \frac{\log(n+1)}{n} + \delta_2 \quad (80) \\
\frac{\log J}{n} \leq H_{\alpha}(A)_{\Psi} - H_{\alpha}(A|R)_{\Psi} + \frac{(|B|+1)|R| \log(n+1) + 1}{n} + \delta_1 + \delta_2 \quad (81)
\]
that has the error converging to 0 exponentially in \( n \). \( \square \)

8 Entanglement-assisted quantum communication with side information at the transmitter (Father with side information at the transmitter)

The definitions are directly from Ref. [17].
Definition 7. Let $N^{A'S\rightarrow B}$ be a ctp map with Stinespring dilation $V_{N}^{A'S\rightarrow BE}$ and $|\Upsilon\rangle^{SS'}$ be a pure state. Then the transmitter encodes its information contained in $\rho_{A'R} \in D(\mathcal{H}_{A'R})$ using a ctp map $\mathcal{E}_{A'S'} \rightarrow A'$, and the output of the channel is $\rho_{BR}^{S} = N^{A'S\rightarrow B} \circ \mathcal{E}_{A'S'} \rightarrow A'$ ($\rho_{A'R} \otimes \Upsilon^{SS'}$). We denote this channel by $(N^{A'S\rightarrow B}, |\Upsilon\rangle^{SS'})$.

Definition 8. A $(\mathcal{N}, \text{error}, n)$ father protocol with side information at the transmitter consists of $n$ copies of two MES $\Phi_{A0R}$ and $\Phi_{A1B1}$ where Alice has $A_0, A_1$, Bob has $B_1$, and the reference $R$ is inaccessible to both Alice and Bob, Alice applying an encoding map $\Phi_{A0R} \otimes \Phi_{A1B1} \otimes \Upsilon^{SS'}$ of the channel by $(\mathcal{N}^{A'S\rightarrow B}, |\Upsilon\rangle^{SS'})$, and Bob applying a decoding map $D_{B_1} \rightarrow B_2^n$ such that for

$$\rho_{B_2^n}^{\text{R}} \equiv D_{B_1}^{\text{R}} \circ (N^{A'S\rightarrow B})^{\otimes n} \circ \mathcal{E}_{A_0^n A_1^n S^n \rightarrow A^n} (\Phi_{A0R} \otimes \Phi_{A1B1} \otimes \Upsilon^{SS'})^{\otimes n},$$

The number $\log |B_1|$ is called the entanglement rate of the protocol and $\log |R|$ is called the quantum communication rate of the protocol.

A pair of real numbers $(R_Q, R_E)$ is called an achievable rate pair if there exist, for $n \rightarrow \infty$, protocols with quantum communication rate approaching $R_Q$, entanglement gain rate approaching $R_E$, and error approaching 0.

The achievable rates are described by the following theorem.

Theorem 11 (Dupuis, 2009 [17]). Let $|\Psi\rangle^{CA_A'S}$ be a pure state with $\mathcal{H}_A = \mathcal{H}_R \otimes \mathcal{H}_{B_1}$ such that $\Psi^S = \Upsilon^S$, and $|\Psi\rangle^{CABE} = V_{N}^{A'S\rightarrow BE} |\Psi\rangle^{CA_A'S}$. The following rates are achievable:

$$R_Q + R_E < H(A|S)_\Psi$$

(84)

$$R_Q - R_E < -H(A|B)_\Psi.$$  

(85)

We now have the following theorem.

Theorem 12. For any $n \in \mathbb{N}$, and $\Psi$ as defined in Theorem 11, there exist $(\mathcal{N}, \text{error}, n)$ Father protocols with side information at the transmitter such that for any $\alpha \in (1, 2]$ and $\delta_1, \delta_2 > 0$,

$$\log |R| + \log |B_1| = H_\alpha (A|S)_\Psi - |S| \frac{\log (n+1)}{n} - \delta_1$$

(86)

$$\log |R| - \log |B_1| = -H_\alpha (A|B)_\Psi - |C||E| \frac{\log (n+1)}{n} - \delta_2,$$

(87)

and the error approaches 0 exponentially in $n$.

Proof. We first claim using Corollary 2 that there exists a Unitary $U$ on $R^n B_1^n$ such that

$$\left\| \text{Tr}_{B_1^n} [U \cdot (\Psi^{CRB_1 E}^{\otimes n})] - (\pi^R \otimes \Psi^{CE})^{\otimes n} \right\|_1$$

$$\leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left| |C||E| \log (n+1) - n H_\alpha (A|CE)_\Psi + n \log \frac{|R|}{|B_1|} \right| \right\}$$

$$= 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |C||E| \log (n+1) + n H_\alpha (A|B)_\Psi + n \log \frac{|R|}{|B_1|} \right] \right\} \equiv \varepsilon_n,$$

(88)
and

\[ \left\| U \cdot (\Psi^{RB_1}_S)^n \right\|_1 = \left\| U \cdot (\Psi^{RB_1}_S)^n \otimes (\Psi^S)^n \right\|_1 \]

\[ \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |S| \log(n+1) - nH_{\alpha}(A|S)_{\Psi} + n \log(|R||B_1|) \right] \right\} \equiv \vartheta_n. \tag{89} \]

where in (89), we have used \( \Psi^S = \Upsilon^S \), and it follows from (89) and Lemma 31 that there exists an isometry \( V_1^{A_0^A A_1^A S^n \rightarrow A^n C^n} \) such that

\[ \left\| U \cdot (\Psi^{CRB_1 A'} S)^n - V_1^{A_0^A A_1^A S^n \rightarrow A^n C^n} \cdot (\Phi^{A_0 R} \otimes \Phi^{A_1 B_1} \otimes \Upsilon^{S'} S)^n \right\|_1 \leq 2\sqrt{\vartheta_n}. \tag{90} \]

Using the triangle inequality, (88) and monotonicity, we have

\[ \left\| \text{Tr}_{B_1^n B^n} \left\{ (V_{A'})^n V_1^{A_0^A A_1^A S^n \rightarrow A^n C^n} \cdot (\Phi^{A_0 R} \otimes \Phi^{A_1 B_1} \otimes \Upsilon^{S'} S)^n \right\} - (\pi R \otimes \Psi^{CE})^n \right\|_1 \leq \varepsilon_n + 2\sqrt{\vartheta_n}. \tag{91} \]

Hence there exists an isometry \( V_2^{B_1^n B^n \rightarrow B_2^n \tilde{A}_n \tilde{B}_n} \) such that for some purifications \( \Phi^{RB_2} \) and \( \tilde{\Phi}^{ABCE} \) of \( \pi R \) and \( \Psi^{CE} \) respectively, we have

\[ \left\| V_2^{B_1^n B^n \rightarrow B_2^n \tilde{A}_n \tilde{B}_n} (V_{A'})^n V_1^{A_0^A A_1^A S^n \rightarrow A^n C^n} \cdot (\Phi^{A_0 R} \otimes \Phi^{A_1 B_1} \otimes \Upsilon^{S'} S)^n \right\|_1 \leq 2\sqrt{\varepsilon_n} + 2\sqrt{\vartheta_n}. \tag{92} \]

and hence,

\[ \left\| \text{Tr}_{\tilde{A}_n \tilde{B}_n C^n} \left\{ V_2 \cdot (\tilde{N})^n V_1 \cdot (\Phi^{A_0 R} \otimes \Phi^{A_1 B_1} \otimes \Upsilon^{S'} S)^n \right\} - (\Phi^{RB_2})^n \right\|_1 \leq 2\sqrt{\varepsilon_n} + 2\sqrt{\vartheta_n}. \tag{93} \]

It is now clear that Alice just applies \( \text{Tr}_{C^n} \circ V_1^{A_0^A A_1^A S^n \rightarrow A^n C^n} \) and Bob applies \( \text{Tr}_{\tilde{A}_n \tilde{B}_n} \circ V_2^{B_1^n B^n \rightarrow B_2^n \tilde{A}_n \tilde{B}_n} \). The claim now follows readily. \( \square \)

We now have the following corollary to obtain the regularized expressions by additional blocking.

**Corollary 13.** For any \( m,n \in \mathbb{N} \), a pure state \( \Psi^{CAA^m S^m} \) with \( \mathcal{H}_A = \mathcal{H}_R \otimes \mathcal{H}_{B_1} \) such that \( \Psi^S = (\Upsilon^S)^m \) and \( \Psi^{CAB^m E^m} = (V_{A'}^{S \rightarrow BE})^m \otimes \Psi_{CAB^m}^{AA^m S^m} \), there exist \( (\tilde{N}, \text{error}, mn) \) Father protocols with side information at the transmitter such that for any \( \alpha \in (1,2) \) and \( \delta_1, \delta_2 > 0 \),

\[ \frac{\log |R|}{m} + \frac{\log |B_1|}{m} = \frac{H_{\alpha}(A|S^m)_{\Psi}}{m} - |S| \frac{\log(mn+1)}{mn} - \delta_1 \tag{94} \]

\[ \frac{\log |R|}{m} - \frac{\log |B_1|}{m} = - \frac{H_{\tilde{\alpha}}(A|B^m)_{\Psi}}{m} - C||E|^m \frac{\log(n+1)}{mn} - \delta_2, \tag{95} \]

and the error approaches 0 exponentially in \( mn \).
We omit the proof. Rather than blindly applying Theorem 12, we need to use $\nu(\Omega_{S})^{\otimes mn} \leq (mn + 1)^{|S|}$. The number $m$ serves two purposes. Firstly, it enables a better approximation to the optimal rates, and, secondly, it allows for finer approximation to the Rényi quantities through the choices of $|R|$ and $|B_{1}|$.

Note that by choosing $|B_{1}| = 1$, we get entanglement-unassisted quantum communication as a special case of the above and for any $\alpha \in (1, 2)$ and $\delta_{1}, \delta_{2} > 0$, the rate is given by

$$\frac{\log |R|}{m} = \min \left\{ \frac{H_{\alpha}(A|S)^{m}_{\Psi}}{m} - |S|^\frac{\log(mn + 1)}{mn} - \delta_{1}, \right.$$

$$\left. - \frac{H_{\alpha}(A|B)^{m}_{\Psi}}{m} - |C||E|m^\frac{\log(n + 1)}{mn} - \delta_{2} \right\}. \quad (96)$$

The rate for entanglement-assisted quantum communication for any $\alpha \in (1, 2)$ and $\delta > 0$ is given by

$$\frac{\log |R|}{m} = \frac{H_{\alpha}(A|S)^{m}_{\Psi} - H_{\alpha}(A|B)^{m}_{\Psi}}{2m} - \frac{|S|^\frac{\log(mn + 1)}{mn} + |C||E|m^\frac{\log(n + 1)}{mn}}{2mn} - \delta. \quad (97)$$

**Definition 9.** A $(N, \text{error}, n)$ entanglement-assisted classical communication protocol with side information at the transmitter consists of $n$ copies of an MES $\Phi^{A_{2}B_{2}}$ where Alice has $A_{2}$ and Bob has $B_{2}$, Alice having a random variable $X$ uniformly distributed over a set $\mathcal{X}$ that models the information, Alice applying an encoding map $E_{x}^{A_{2}S^{n} \rightarrow A_{n}}$, $x \in \mathcal{X}$, if $X = x$, $n$ uses of the channel with side information at the transmitter $(N^{A_{n} \rightarrow B}, |\Upsilon\rangle^{SS'})$, and Bob applying a POVM (positive operator-valued measure) $\Lambda_{x'}^{B_{n}B_{2}}$, $x' \in \mathcal{X}$, such that for

$$Pr\{x'|x\} \equiv \text{Tr} \Lambda_{x'}^{B_{n}B_{2}} \left[ (N^{A_{n} \rightarrow B} \otimes n) \circ E_{x}^{A_{2} \rightarrow A_{n}} (\Phi^{A_{2}B_{2} \otimes S^{S'}}) \otimes n \right], \quad (98)$$

$$\frac{1}{|\mathcal{X}|} \sum_{x} (1 - Pr\{x|x\}) \leq \text{error}. \quad (99)$$

The number $(\log |\mathcal{X}|)/n$ is called the classical communication rate of the protocol.

A real number $R_{C}$ is called an achievable rate if there exist, for $n \rightarrow \infty$, protocols with classical communication rate approaching $R_{C}$ and error approaching 0.

We now provide the random coding exponents for the entanglement-assisted classical communication.

**Corollary 14.** For any $m, n \in \mathbb{N}$, a pure state $\Psi^{CA_{2}A_{n}}$ with $H_{A} = H_{R} \otimes H_{B_{1}}$, such that $\Psi^{S_{2}} = (\Upsilon^{S})^{\otimes m}$ and $|\Psi\rangle^{CA_{2}B_{2} \rightarrow E_{m}} = (V_{N}^{A_{n} \rightarrow BE})^{\otimes m} |\Psi\rangle^{CA_{2}A_{n}S_{2}}$, there exist $(N, \text{error}, mn)$ entanglement-assisted classical communication protocols with side information at the transmitter such that for any $\alpha \in (1, 2)$ and $\delta > 0$, the rate per channel use is given by

$$\frac{\log |\mathcal{X}|}{mn} = \frac{H_{\alpha}(A|S)^{m}_{\Psi}}{m} - \frac{H_{\alpha}(A|B)^{m}_{\Psi}}{m} - |S|^\frac{\log(mn + 1)}{mn} - |C||E|m^\frac{\log(n + 1)}{mn} - \delta, \quad (100)$$

and the error approaches 0 exponentially in $mn$. 

20
Definition 10. A $(Ψ, error, n)$ QSR protocol consists of $n$ copies of a pure state $|Ψ⟩^{ACBR}$ shared between with Alice ($A$ and $C$), Bob ($B$), and the reference ($R$) unavailable to both Alice and Bob, a MES $Φ_{A_1B_1}$ shared between Alice ($A_1$) and Bob ($B_1$), Alice applying $E : A_1C^nA^n → C_2C_3A^n$, a quantum communication across a noiseless quantum channel from Alice to Bob $I^C_{A_1}→ B$, and Bob applying $D : B_1B_3B_3^→ B_2B_3B_3^$ such that for

$$\rho^{C_2B_2A^nB_3^nB_3^nR^n} \equiv D^{B_1B_3^n→ B_2B_3^nB_3^n} \circ I^C_{A_1}→ B \circ E^{A_1C^nA^n→ C_2C_3A^n} [(Ψ^{ACBR})^n ⊗ Φ_{A_1B_1}],$$

(105)

and

$$\left\| ρ^{C_2B_2A^nB_3^nB_3^nR^n} - Φ_{C_2B_2} ⊗ (Ψ^{B_3B_3R})^n \right\|_1 ≤ error.$$  

(106)

The number $(log |C_3|)/n$ is called the quantum communication rate and $(log |C_2| - log |B_1|)/n$ is called the entanglement gain rate of the protocol.

9 Quantum state redistribution (QSR)

Proof. We follow the well-understood strategy to encapsulate the entanglement-assisted quantum communication protocol in the qudit superdense coding protocol. We follow the notation in Definition 8. Let $H_{A_3} = H_{A_0} ⊗ H_{A_1}$. Alice has access to $A_0, A_1$ and Bob has access to $R, B_1$. Let $V_j ∈ U(R^n)$ such that $Tr V_j V^†_j = |R|^n δ_{i,j}$. Alice chooses $|X| = |R|^{2n}$, and, for $X = x$, Alice applies $V_x$ over $R^n$ on $(Φ_{A_0R})^⊗n$ (Alice does this by exploiting the Schmidt symmetry) and passes that MES as input to the father protocol that uses the channel $m × n$ times. At the end of the father protocol, we have a state $ρ^{B_2^nR^n}$ such that

$$\left\| ρ^{B_2^nR^n} - V_x (Φ^{B_2R})^⊗mn \right\|_1 ≤ β_{mn},$$

(101)

where $β_{mn} = 2\sqrt{ε_{m,n} + 2v_{m,n}}$, and

$$ε_{m,n} = 8 exp \left\{ \frac{α - 1}{2α} \left[ |C| |E|^m \log(n + 1) + nH_α(A|B^n) + n \log |R| |B_1| \right] \right\},$$

(102)

$$v_{m,n} = 8 exp \left\{ \frac{α - 1}{2α} \left[ |S| \log(mn + 1) − nH_α(A|S^n) + n \log(|R| |B_1|) \right] \right\},$$

(103)

and for appropriately chosen $|R|$ and $|B_1|$ as per (94) and (95), $β_{mn}$ decays exponentially in $mn$. Bob now applies the POVM given by $\{V_x (Φ^{B_2R})^⊗mn, x' ∈ X, \}$ and

$$Pr\{x|x\} = Tr ρ^{B_2^nR^n} [V_x (Φ^{B_2R})^⊗mn] = F [ρ^{B_2^nR^n} V_x (Φ^{B_2R})^⊗mn]^2 ≥ 1 − β_{mn},$$

(104)

where the inequality follows from the Fuchs-van de Graaf inequalities between trace distance and Fidelity [31] and in particular Corollary 9.3.2 in Ref. [5], and hence, the error of the protocol is upper bounded by $β_{mn}$. Lastly, it is easy to show that a cptp map followed by a POVM can be implement just by a suitably chosen POVM, and hence, the decoder of the father protocol and the POVM of the superdense coding protocol can be implemented by a POVM. The claim now follows readily. □
A pair of real numbers \((R_Q, R_E)\) is called an **achievable rate pair** if there exist, for \(n \to \infty\), QSR protocols with quantum communication rate approaching \(R_Q\), entanglement gain rate approaching \(R_E\), and error approaching 0.

The achievable rates are described by the following theorem.

**Theorem 15** (Devetak and Yard, 2008 [32]). The following rates are achievable for the QSR protocol:

\[
R_Q > \frac{1}{2} I(C : R|B) \Psi \quad \text{and} \quad R_Q + R_E > H(C|B) \Psi.
\]  

(107)

Our goal in the remainder of this section is to provide the random coding exponents for the achievability of this protocol.

**Theorem 16.** For any \(n \in \mathbb{N}\), there exists a \((\Psi, \text{error}, n)\) QSR protocol for any \(\alpha \in (1,2], \delta_1, \delta_2 > 0\), such that

\[
\frac{1}{n} \log \frac{|C_3|}{|B_1|} = H_\alpha(C|B) \Psi + |A||R| \frac{1}{n} \log \left(\frac{n + 1}{n}\right) + \delta_2,
\]  

(109)

and the error approaches 0 exponentially in \(n\).

**Proof.** Our line of attack is similar to that in Ref. [33]. Let \(W^{C^\alpha_{1}} \rightarrow B_1 C_2 C_3, |B_1||C_2||C_3| \leq |C|^n\), be a full-rank partial isometry. Then we can claim using Corollary 2 that for any \(\alpha \in (1,2]\), there exists a Unitary \(U^{C^n}\) such that

\[
\left\| \operatorname{Tr}_{C_2 C_3} \circ \mathcal{T}_W^{C^n} - \pi_{B_1} \otimes (\psi^{BR})^{\otimes n} \right\|_1 \\
\leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A||R| \log(n + 1) - nH_\alpha(C|BR) \Psi + \log \frac{|B_1|}{|C_2||C_3|} \right] \right\} \equiv \varepsilon_n,
\]  

(110)

and

\[
\left\| \operatorname{Tr}_{B_1 C_3} \circ \mathcal{T}_W^{C^n} - \pi_{B_1} \otimes (\psi^{ACR})^{\otimes n} \right\|_1 \\
\leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A||R| \log(n + 1) - nH_\alpha(C|AR) \Psi + \log \frac{|C_2|}{|B_1||C_3|} \right] \right\} \\
= 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |A||R| \log(n + 1) + nH_\alpha(C|B) \Psi + \log \frac{|C_2|}{|B_1||C_3|} \right] \right\} \equiv \vartheta_n.
\]  

(111)

Using (110), we claim that there exist an isometry \(V_1^{C_2 C_3 A^n_{1}} \rightarrow A_1 A^n_{1} C^n\) such that

\[
\left\| V_1 \cdot \mathcal{T}_W - \phi_{A_1 B_1} \otimes (\psi^{ACR})^{\otimes n} \right\|_1 \leq h(\varepsilon_n),
\]  

(112)

22
and hence, using the compressive map $C_{V_1} : A_1 A^n C^n \rightarrow C_2 C_3 A^n$, we have
\[
\left\| C_{V_1} \left[ \Phi^{A_1 B_1} \otimes (\Psi^{ACBR})^\otimes n \right] - T_W \left[ U^{C^n} \cdot (\Psi^{\tilde{A}CBR})^\otimes n \right] \right\|_1 \leq h(\varepsilon_n). \tag{113}
\]
Using (111), we claim that there exist an isometry $V_2^{B_1 B^n B_2 B_3 B_4} \otimes n$ such that
\[
\left\| V_2 \cdot I \circ T_W \left[ U^{C^n} \cdot (\Psi^{\tilde{A}CBR})^\otimes n \right] - \Phi^{C_2 B_2} \otimes (\Psi^{\tilde{A}B_4 B_3 R})^\otimes n \right\|_1 \leq h(\varepsilon_n) + h(\vartheta_n). \tag{114}
\]
Using monotonicity and triangle inequality, we now have
\[
\left\| V_2 \cdot I \circ C_{V_1} \left[ \Phi^{A_1 B_1} \otimes (\Psi^{ACBR})^\otimes n \right] - \Phi^{C_2 B_2} \otimes (\Psi^{\tilde{A}B_4 B_3 R})^\otimes n \right\|_1 \leq h(\varepsilon_n) + h(\vartheta_n). \tag{115}
\]
Hence, Alice’s operation is $C_{V_1}^{A_1 A^n C^n \rightarrow C_2 C_3 A^n}$ and Bob’s operation is $V_2^{B_1 B^n B_2 B_3 B_4} \otimes n$. The claim now follows readily. \hfill \Box

10 Quantum communication across Broadcast Channels (QCBC)

**Definition 11.** A $(N, \text{error}, n)$ QCBC protocol consists of $n$ copies of four MES $|\Phi\rangle^{S_1 R_1}, |\Phi\rangle^{A_1 B_1}, |\Phi\rangle^{S_2 R_2}$, and $|\Phi\rangle^{A_2 B_2}$, where Alice has $S_1, S_2, A_1, A_2$, Bob 1 has $B_1, B_2$, and the references (R1 and R2) are inaccessible to both Alice and Bob, Alice applying the encoding map $E^{A_1 S_1 A_2 S_2 \rightarrow A^n}$, $n$ uses of a quantum broadcast channel from Alice to Bob 1 and 2, $N^{A' \rightarrow C_1 C_2}$ (with Stinespring dilation $V_N^{A' \rightarrow C_1 C_2 E}$), and local quantum operations by Bobs $D_i^{B_i C_i n \rightarrow \tilde{S}_i n}$, $i = 1, 2$, such that for
\[
\rho_{\tilde{S}_i n R_i n \tilde{S}_2 n R_2 n} = \left( D_1^{B_1 C_1 n \rightarrow \tilde{S}_1 n} \circ D_2^{B_2 C_2 n \rightarrow \tilde{S}_2 n} \right) \circ (N^{A' \rightarrow C_1 C_2})^\otimes n \circ E^{A_1 S_1 A_2 S_2 \rightarrow A^n} \left[ (\Phi^{S_1 R_1} \otimes \Phi^{A_1 B_1} \otimes \Phi^{S_2 R_2} \otimes \Phi^{A_2 B_2})^\otimes n \right], \tag{116}
\]
\[
\left\| \rho_{\tilde{S}_i n R_i n \tilde{S}_2 n R_2 n} - (\Phi^{S_1 R_1} \otimes \Phi^{S_2 R_2})^\otimes n \right\|_1 \leq \text{error}. \tag{117}
\]
For $i = 1, 2$, the numbers $\log |R_i|$ are the **quantum communication rates** and $\log |B_i|$ are the **entanglement consumption rates** of the protocol.

A vector of real numbers $(R_{Q,1}, R_{Q,2}, R_{E,1}, R_{E,2})$ is called an **achievable rate vector** if there exist, for $n \rightarrow \infty$, QCBC protocols with quantum communication rates approaching $R_{Q,i}$, entanglement consumption rates approaching $R_{E,i}$, $i = 1, 2$, and error approaching 0.
Theorem 17 (Dupuis, 2009 [17]). Let $|\Psi^{A\rightarrow D}_{\psi}\rangle$ be any pure state with $\mathcal{H}_A = \mathcal{H}_{R_1} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{R_2} \otimes \mathcal{H}_{B_2}$ and $|\Psi^{AC_1C_2ED}_{\psi}\rangle = V_{\mathcal{N}}^{A\rightarrow C_1C_2E} |\Psi^{A\rightarrow D}_{\psi}\rangle$. The following rates are achievable

$$\log |R_1| + \log |B_1| < H(R_1|B_1)_{\psi}$$  \hspace{1cm} (118)
$$\log |R_2| + \log |B_2| < H(R_2|B_2)_{\psi}$$  \hspace{1cm} (119)
$$\log |R_1| + \log |B_1| + \log |R_2| + \log |B_2| < H(A)_{\psi}$$  \hspace{1cm} (120)
$$\log |R_1| - \log |B_1| < I(R_1|B_1)_{C_1}$$  \hspace{1cm} (121)
$$\log |R_2| - \log |B_2| < I(R_2|B_2)_{C_2}$$  \hspace{1cm} (122)

We follow the line of attack from Ref. [17] that we need to show the following theorem, which would yield Theorem 17. The regularized expressions can be obtained by additional blocking.

Theorem 18. For any $n \in \mathbb{N}$, $|\Psi^{A\rightarrow D}_{\psi}\rangle$ and $|\Psi^{AC_1C_2ED}_{\psi}\rangle$ the states defined in Theorem 17, there exists a $(N, error, n)$ QCBC protocol such that for any $\alpha \in (1, 2], \delta_1, \delta_2, \delta_3, \delta_4 > 0$,

$$\log |R_1| + \log |B_1| = H_a(R_1|B_1|B_2)_{\psi} - \frac{|R_2|B_2|\log(n+1)}{n} - \delta_1$$  \hspace{1cm} (123)
$$\log |R_1| - \log |B_1| = -H_{\tilde{a}}(R_1|B_1|C_1)_{\psi} - \frac{|R_2|B_2|C_2ED|\log(n+1)}{n} - \delta_2$$  \hspace{1cm} (124)
$$\log |R_2| + \log |B_2| = H_a(R_2|B_2)_{\psi} - \delta_3$$  \hspace{1cm} (125)
$$\log |R_2| - \log |B_2| = -H_{\tilde{a}}(R_2|B_2|C_2)_{\psi} - \frac{|R_1|B_1|C_1ED|\log(n+1)}{n} - \delta_4$$  \hspace{1cm} (126)

and the error approaches 0 exponentially in $n$.

Proof. For $i = 1, 2$, we claim using Corollary 2 (twice for each $i$) that there exist Unitaries $U_i$ on $R_i^n B_i^n$ such that

$$\|U_1 \cdot (\Psi^{R_1B_1R_2B_2}_{\psi})^{\otimes n} - (\pi^{R_1B_1} \otimes \Psi^{R_2B_2}_{\psi})^{\otimes n}\|_1 \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R_2|B_2|\log(n+1) - nH_a(R_1|B_1|B_2)_{\psi} + n \log |R_1| |B_1| \right] \right\} \equiv \epsilon_{n,1},$$  \hspace{1cm} (127)

$$\|\text{Tr}_{B_1} \circ U_1 \cdot (\Psi^{R_1B_1R_2B_2C_2ED}_{\psi})^{\otimes n} - (\pi^{R_1} \otimes \Psi^{R_2B_2C_2ED}_{\psi})^{\otimes n}\|_1 \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R_2|B_2|C_2ED|\log(n+1) - nH_a(R_1|B_1|B_2|C_2ED)_{\psi} + n \log \frac{|R_1|}{|B_1|} \right] \right\}$$
$$= 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ |R_2|B_2|C_2ED|\log(n+1) + nH_{\tilde{a}}(R_1|B_1|C_1)_{\psi} + n \log \frac{|R_1|}{|B_1|} \right] \right\} \equiv \epsilon_{n,2},$$  \hspace{1cm} (128)

$$\|U_2 \cdot (\Psi^{R_2B_2}_{\psi})^{\otimes n} - (\pi^{R_2B_2}_{\psi})^{\otimes n}\|_1 \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ - nH_{\tilde{a}}(R_2B_2)_{\psi} + n \log(|R_2|B_2) \right] \right\} \equiv \epsilon_{n,3},$$  \hspace{1cm} (129)
\[ \| \text{Tr}_{B_2} \left\{ U_2 \cdot (\Psi^{R_1B_1B_2B_3C_1ED}) \otimes n \right\} - (\pi^{R_2} \otimes \Psi^{R_1B_1C_1ED}) \otimes n \|_1 \leq 8 \exp \left( \frac{\alpha - 1}{2\alpha} \left[ |R_1B_1C_1ED| \log(n + 1) - nH_\alpha(R_2B_2|R_1B_1C_1ED)_\Psi + n \log \frac{R_2}{|B_2|} \right] \right) \]
\[ = 8 \exp \left( \frac{\alpha - 1}{2\alpha} \left[ |R_1B_1C_1ED| \log(n + 1) + nH_\alpha(R_2B_2|C_2)_\Psi + n \log \frac{R_2}{|B_2|} \right] \right) \equiv \varepsilon_{n,4}. \quad (130) \]

We now have
\[ \| (U_1 \otimes U_2) \cdot (\Psi^{R_1B_1B_2B_2A'D}) \otimes n - V_1 \cdot (\Phi^{S_1R_1} \otimes \Phi^{A_1B_1} \otimes \Phi^{S_2R_2} \otimes \Phi^{A_2B_2}) \otimes n \|_1 \leq 2\sqrt{\varepsilon_{n,1} + \varepsilon_{n,3}}. \quad (132) \]

It follows from (128) and (130) that there exist isometries \( V_1^{B_1^nC_1^n} \rightarrow \tilde{R}_1^{\tilde{S}_1} \tilde{B}_1^{\tilde{C}_1} \) and \( V_2^{B_2^nC_2^n} \rightarrow \tilde{R}_2^{\tilde{S}_2} \tilde{B}_2^{\tilde{C}_2} \) such that
\[ \| (V_2U_1) \cdot (\Psi^{R_1B_1B_2B_2C_1C_2ED}) \otimes n - (\Phi^{R_1\tilde{S}_1}) \otimes (\Psi^{\tilde{R}_1\tilde{B}_1B_2B_2\tilde{C}_1C_2ED}) \otimes n \|_1 \leq 2\sqrt{\varepsilon_{n,2}}, \quad (133) \]
\[ \| (V_2U_2) \cdot (\Psi^{R_1B_1B_2B_2C_1C_2ED}) \otimes n - (\Phi^{R_2\tilde{S}_2}) \otimes (\Psi^{\tilde{R}_2\tilde{B}_2B_2B_2\tilde{C}_1C_2ED}) \otimes n \|_1 \leq 2\sqrt{\varepsilon_{n,4}}, \quad (134) \]

We now have for
\[ \mathcal{E}^{A_1S_1A_2S_2 \rightarrow A''} = \text{Tr}_{D^n} \circ V_1^{S_1^nA_1^nS_2^nA_2^n} \rightarrow A''D^n, \quad (135) \]
\[ D_1^{B_1^nC_1^n} \rightarrow \tilde{S}_1 = \text{Tr}_{\tilde{R}_1^{\tilde{B}_1^n\tilde{C}_1^n}} \circ V_2^{B_1^nC_1^n} \rightarrow \tilde{R}_1^{\tilde{S}_1^n\tilde{B}_1^n\tilde{C}_1^n}, \quad (136) \]
\[ D_2^{B_2^nC_2^n} \rightarrow \tilde{S}_2 = \text{Tr}_{\tilde{R}_2^{\tilde{B}_2^n\tilde{C}_2^n}} \circ V_3^{B_2^nC_2^n} \rightarrow \tilde{R}_2^{\tilde{S}_2^n\tilde{B}_2^n\tilde{C}_2^n}, \quad (137) \]
\[ \| D_1 \circ D_2 \circ (\mathcal{N}) \otimes n \circ \mathcal{E} \left[ (\Phi^{S_1R_1} \otimes \Phi^{A_1B_1} \otimes \Phi^{S_2R_2} \otimes \Phi^{A_2B_2}) \otimes n \right] - (\Phi^{R_1\tilde{S}_1} \otimes \Phi^{R_2\tilde{S}_2}) \otimes n \|_1 \leq 2\sqrt{\varepsilon_{n,2}} + \sqrt{\varepsilon_{n,4}} + 2\sqrt{\varepsilon_{n,1} + \varepsilon_{n,3}}, \quad (138) \]
where the first inequality follows from (132), the triangle inequality and the monotonicity, the second inequality follows from the triangle inequality, the third inequality follows as:

\[
\left\| D_1 \circ D_2 \left[ (U_1 \otimes U_2) \cdot (\Psi R_1 B_1 R_2 B_2 C_1 C_2)^{\otimes n} \right] - (\Phi R_1 S_1)^{\otimes n} \otimes D_2 \left[ U_2 \cdot (\Psi R_2 B_2 C_2)^{\otimes n} \right] \right\|_1 \\
\leq \left\| D_1 \left[ U_1 \cdot (\Psi R_1 B_1 R_2 B_2 C_1 C_2)^{\otimes n} \right] - (\Phi R_1 S_1)^{\otimes n} \otimes (\Psi R_2 B_2 C_2)^{\otimes n} \right\|_1 \\
\leq \left\| (V_2 U_1) \cdot (\Psi R_1 B_1 R_2 B_2 C_1 C_2)^{\otimes n} - (\Phi R_1 S_1)^{\otimes n} \otimes (\Phi R_1 \tilde{B}_1 R_2 B_2 C_1 C_2)^{\otimes n} \right\|_1 \\
\leq 2\sqrt{\varepsilon_{n,2}},
\] (139)

where both the first two inequalities follow from the monotonicity and the last inequality from (133), and

\[
\left\| (\Phi R_1 S_1)^{\otimes n} \otimes D_2 \left[ U_2 \cdot (\Psi R_2 B_2 C_2)^{\otimes n} \right] - (\Phi R_1 \tilde{S}_1) \otimes (\Phi R_2 \tilde{S}_2)^{\otimes n} \right\|_1 \leq 2\sqrt{\varepsilon_{n,4}},
\] (140)

where we have used (134) and monotonicity. The claim of the Theorem now follows from (138).

\[\square\]

**Remark:** It is clear from the above theorem that any rate in the following rate region is achievable with error decaying exponentially in \( n \) to zero:

\[
\log |R_1| + \log |B_1| < H(R_1 B_1 | R_2 B_2)_\Psi
\] (141)
\[
\log |R_2| + \log |B_2| < H(R_2 B_2)_\Psi
\] (142)
\[
\log |R_1| - \log |B_1| < I(R_1 B_1 | C_1)_\Psi
\] (143)
\[
\log |R_2| - \log |B_2| < I(R_2 B_2 | C_2)_\Psi
\] (144)

We now repeat the argument given in Theorem 5.3 in Ref. [17] that by switching the roles of Bob 1 and Bob 2 and doing time sharing, we can achieve any point in the rate region as stipulated in the claim of the Theorem 17.

## 11 Destroying correlations by adding classical randomness

**Definition 12.** A \((\rho, \text{error}, n)\) protocol for destroying correlations by adding classical randomness consists of \( n \) copies of a bipartite state \( \rho^{AR} \), and applying \( M \) Unitaries \( U_i, i = 1, \ldots, M \), over \( A^n \) such that

\[
\left\| \frac{1}{M} \sum_{i=1}^{M} \left[ U_i \cdot (\rho^{AR})^{\otimes n} \right] - \sigma^{A^n} \otimes (\rho^R)^{\otimes n} \right\|_1 \leq \text{error},
\] (145)

where \( \sigma^{A^n} \in \mathcal{D}(\mathcal{H}_{A^n}) \) and we make no apriori restrictions on the choice of \( \sigma^{A^n} \).

The number \((\log M)/n\) is called the rate of the protocol. A real numbers \( \mathcal{R}_C \) is called an achievable rate if there exist, for \( n \to \infty \), protocols with rate approaching \( \mathcal{R}_C \) and the error approaching 0.

**Theorem 19** (Groisman et al, 2005 [34]). The smallest achievable rate is \( I(A:R)_\rho \).
We prove the following theorem.

**Theorem 20.** For any $n \in \mathbb{N}$, there exists a $(\rho, \text{error}, n)$ protocol such that for any $\delta > 0$, $\alpha \in (1, 2]$ and $|\Psi^{ARE}\rangle$ a purification of $\rho^{AR}$,

$$\frac{\log M}{n} = H_{\tilde{A}}(A)_{\rho} - H_{\alpha}(A|R)_{\rho} + (|E| + 1)|R|\frac{\log(n + 1)}{n} + \delta,$$

(146)

and the error approaches 0 exponentially in $n$.

**Proof.** Consider a partial isometry $W: A^n \to B$, $|B| \leq |A^n|$. For $M \leq |B|^2$, we can choose $M$ Unitaries $V^B_i \in \mathbb{U}(B)$ such that $\text{Tr}(V^B_i) V^B_j = |B| \delta_{i,j}$, and let $V_M: B \to B$ be a cptp map given by

$$V_M(\sigma^B) \equiv \frac{1}{M} \sum_{i=1}^{M} V^B_i \cdot \sigma^B.$$  

(147)

Then, from Corollary 2, for any $\alpha \in (1, 2]$, there exists a Unitary $U$ such that

$$\|\text{Tr}_B \circ T_W [U \cdot (\Psi^{ARE}) \otimes^n] - (\Psi^{RE}) \otimes^n\|_1 \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} [ |R| |E| \log(n + 1) + n H_{\tilde{A}}(A)_{\rho} - \log |B| ] \right\} \equiv \epsilon_n,$$

(148)

and

$$\|V_M \circ T_W [U \cdot (\rho^{AR}) \otimes^n] - \pi^B \otimes (\rho^R) \otimes^n\|_1 \leq 8 \exp \left\{ \frac{\alpha - 1}{2\alpha} [ |R| \log(n + 1) - n H_{\alpha}(A|R)_{\rho} - \log M + \log |B| ] \right\} \equiv \vartheta_n,$$

(149)

where we have used $\Theta(V_M \circ T_W) \leq \log |B| - \log M$ from Lemma 23. From (148) and Lemma 31, we claim that there exists a Unitary $U_2$ over $A^n$ such that

$$\|W^+ \cdot T_W [U \cdot (\Psi^{ARE}) \otimes^n] - U_2 \cdot (\Psi^{ARE}) \otimes^n\|_1 \leq h(\epsilon_n).$$

(150)

Consider now the following Unitaries over $A^n$ constructed from $V^B_i$ as $V^{A^n}_i = W^+ \cdot V^B_i + (1^A - W^+W)$. Note that $V^{A^n}_i W^+ = W^+ V^B_i$. We now claim that $V^{A^n}_i U_2$ are the $M$ Unitaries
we need. We have

\[
\left\| \frac{1}{M} \sum_{i=1}^{M} (V_i^{A^m} U_2) \cdot (\rho^{AR})^{\otimes n} - (W^\dagger \cdot \pi^B) \otimes (\rho^R)^{\otimes n} \right\|_1 \\
\leq \left\| \frac{1}{M} \sum_{i=1}^{M} (V_i^{A^m} U_2) \cdot (\rho^{AR})^{\otimes n} - \frac{1}{M} \sum_{i=1}^{M} (V_i^{A^m} W^\dagger) \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] \right\|_1 + \\
\left\| \frac{1}{M} \sum_{i=1}^{M} (V_i^{A^m} W^\dagger) \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] - (W^\dagger \cdot \pi^B) \otimes (\rho^R)^{\otimes n} \right\|_1 \\
\leq \frac{1}{M} \sum_{i=1}^{M} \left\| (V_i^{A^m} U_2) \cdot (\rho^{AR})^{\otimes n} - (V_i^{A^m} W^\dagger) \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] \right\|_1 + \\
\left\| \frac{1}{M} \sum_{i=1}^{M} (W^\dagger V_i^B) \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] - (W^\dagger \cdot \pi^B) \otimes (\rho^R)^{\otimes n} \right\|_1 \\
\leq \frac{1}{M} \sum_{i=1}^{M} \left\| U_2 \cdot (\rho^{AR})^{\otimes n} - W^\dagger \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] \right\|_1 + \\
\left\| \frac{1}{M} \sum_{i=1}^{M} V_i^B \cdot \mathcal{T}_W [U \cdot (\rho^{AR})^{\otimes n}] - \pi^B \otimes (\rho^R)^{\otimes n} \right\|_1 \\
\leq h(\varepsilon_n) + \vartheta_n,
\]

(151)

where the first inequality follows from the triangle inequality, in the second inequality, the first term follows again using the triangle inequality \((M - 1)\) times and the second term follows by invoking \(V_i^{A^m} W^\dagger = W^\dagger V_i^B\), in the third inequality, the first term follows by invoking the Unitary invariance of the trace norm and the second term from monotonicity, in the fourth inequality, the first term is upper bounded using (150) and the second term is upper bounded using (149). The claim now follows readily. \(\square\)

12 Conclusions

In conclusion, we have provided a new version of the decoupling theorem that gives an exponential bound on the average decoupling error with a Rényi \(\alpha\)-conditional entropy in the exponent for a restricted class of completely positive maps for any \(\alpha \in (1, 2]\) as opposed to only \(\alpha = 2\) in Ref. [17]. This key step allows us to make a connection with the random coding exponents, which we provide for several important protocols at the top of the family tree of protocols. The importance of random coding exponents for the achievability of information-processing tasks has been well known since the seminal work by Gallager [8]. Such an analysis, with very few exceptions thus far, has been missing and we now fill that void with this paper. The decoupling theorem and other ideas developed in this paper may well find wider applications with or without further extensions.
A Computation of $\Theta$ for some cases

**Lemma 21.** For a full-rank partial isometry $W^{A\rightarrow A_1A_2}$, $|A_1||A_2| \leq |A|$,\]

$$\Theta(\text{Tr}_{A_2} \circ T_W^{A\rightarrow A_1A_2}) \leq \log \frac{|A_1|}{|A_2|}$$ \hspace{1cm} (152)

$$\Theta(\text{Tr}_{A_2} \circ C_W^{A\rightarrow A_1A_2}) \leq \log \frac{|A_1|}{|A_2|}.$$ \hspace{1cm} (153)

**Proof.** Since we have the freedom in choosing the local orthonormal bases in describing the MES, hence, let them be such that $W |i\rangle^A = |i\rangle^{A_1A_2}$ for $i \leq |A_1||A_2|$, and $W |i\rangle^A = 0$ for $i > |A_1||A_2|$, where $\{|i\rangle^A\}$ and $\{|i\rangle^{A_1A_2}\}$ are orthonormal states in their respective systems. It now follows that

$$T_W(|i\rangle \langle j|^A) = \frac{|A_1|}{|A_1||A_2|} |i\rangle \langle j|^{A_1A_2} \text{ind}_{\{i,j\leq |A_1||A_2|\}}$$ \hspace{1cm} (154)

$$C_W(|i\rangle \langle j|^A) = |i\rangle \langle j|^{A_1A_2} \text{ind}_{\{i,j\leq |A_1||A_2|\}} + \delta_{i,j} \pi^{A_1A_2} \text{ind}_{\{i,j>|A_1||A_2|\}}.$$ \hspace{1cm} (155)

We now have

$$\exp\{\Theta(\text{Tr}_{A_2} \circ C_W)\} \leq \frac{|A_1|}{|A|^2} \sum_{i,j} \text{Tr} \left[ \text{Tr}_{A_2} \circ C_W(|i\rangle \langle j|^A) \right] \left[ \text{Tr}_{A_2} \circ C_W(|j\rangle \langle i|^A) \right]$$ \hspace{1cm} (156)

$$= \frac{|A_1|}{|A|^2} \text{Tr} \left[ \sum_{i,j\leq |A_1||A_2|} \text{Tr}_{A_2}(|i\rangle \langle j|^{A_1A_2}) \text{Tr}_{A_2}(|j\rangle \langle i|^{A_1A_2}) + \sum_{i,j>|A_1||A_2|} \delta_{i,j} \left( \text{Tr}_{A_2} \pi^{A_1A_2} \right)^2 \right]$$ \hspace{1cm} (157)

$$= \frac{|A_1|}{|A|^2} \left( |A_1|^2|A_2| + \frac{|A_1|}{|A_2|} \right) \leq \frac{|A_1|}{|A_2|},$$ \hspace{1cm} (158)

where the first inequality follows using (1). Following the above, we arrive at

$$\exp\{\Theta(\text{Tr}_{A_2} \circ T_W)\} \leq \frac{|A_1|}{|A|^2} \left( \left( \frac{|A_1|}{|A_1||A_2|} \right)^2 |A_1|^2|A_2| \right) = \frac{|A_1|}{|A_2|},$$ \hspace{1cm} (159)

QED.

**Lemma 22.** Let $\{M_i \in L(BC, D), i = 1, \ldots, J\}$, $J = \left[ \frac{BC}{D} \right]$, be a complete set of measurement operators ($\sum_i M_i^\dagger M_i = 1^{BC}$). Let $\zeta \equiv \frac{B|C|}{D}$ and let the first $\vartheta \equiv \frac{BC}{D}$ $M_i$’s be rank-$|D|$ partial isometries. Define for any orthonormal basis $\{|i\rangle^X\}$, $i = 1, \ldots, J$,

$$\mathcal{E}^{BC\rightarrow XD}(\sigma^{BC}) = \sum_{i=1}^J |i\rangle \langle i|^X \otimes (M_i \cdot \sigma^{BC})$$ \hspace{1cm} (160)
and let $W : A \rightarrow B$, $|B| \leq |A|$, be a full-rank partial isometry. Then

$$\Theta(\mathcal{E} \circ \mathcal{T}_W) \leq \log |D|. \quad (161)$$

**Proof.** Let $W^{A \rightarrow B} = \sum_{i=1}^{|B|} |i\rangle_B^B \langle i^A|$. Once again, we exploit the freedom in choosing the local bases in defining MES and have

$$|\Phi\rangle^{A'CC'} = \frac{1}{\sqrt{|A||C|}} \sum_{i_1, i_2} |i_1\rangle^A |i_1\rangle^{A'} |i_2\rangle^C |i_2\rangle^{C'}. \quad (162)$$

Hence,

$$X_{i_1, i_2} \equiv \mathcal{T}_W(|i_1\rangle \langle j_1|A) = \frac{|A|}{|B|} |i_1\rangle \langle j_1|B \text{ ind}_{\{i_1, i_2\leq|B|\}}. \quad (163)$$

We now have for $\theta^{XD} = \sum_x p_x |x\rangle \langle x|^X \otimes \pi^D$, $\{p_x\}$ a probability vector (whose choice is specified below),

$$\exp\{\Theta(\mathcal{E} \circ \mathcal{T}_W)\} \leq \frac{1}{|A|^2|C|^2} \sum_{i_1, i_2, x} \text{Tr}[\mathcal{E}(X_{i_1, i_1} \otimes |i_2\rangle \langle j_2|^C)\mathcal{E}(X_{j_1, i_1} \otimes |j_2|^C)](\theta^{XD})^{-1} \quad (164)$$

$$= \frac{1}{|B|^2|C|^2} \sum_{i_1, i_2, x} \text{Tr}[|x\rangle \langle x|^X \otimes M_x(|i_1\rangle \langle j_1|^B \otimes |i_2\rangle \langle j_2|^C)M_x^\dagger]M_x \quad (165)$$

$$= \frac{1}{|B|^2|C|^2} \sum_{i_1, i_2, x} (\text{Tr}M_x^\dagger M_x) \text{Tr}[|x\rangle \langle x|^X \otimes M_x(|i_1\rangle \langle j_1|^B \otimes |i_2\rangle \langle j_2|^C)M_x^\dagger]M_x \quad (166)$$

$$= \frac{1}{|B|^2|C|^2} \sum_x (\text{Tr}M_x^\dagger M_x) \frac{|D|}{p_x}. \quad (167)$$

Let $p = 1 - \frac{\vartheta}{\zeta}$, $p_x = (1 - p)/\vartheta$ for $x = 1, \ldots, \vartheta$, and if $|D|$ doesn’t divide $|B||C|$, then there is an additional entry $p_x = p$ if $x = \vartheta + 1$. Continuing from above, we now have

$$\exp\{\Theta(\mathcal{E} \circ \mathcal{T}_W)\} \leq \frac{1}{|B|^2|C|^2} \left[\vartheta |D|^{2} \frac{|D|}{|D| - \vartheta} + (|B||C| - |D|\vartheta) \frac{|D|}{p} \right] \quad (168)$$

$$= |D| \left[ \frac{\vartheta}{\vartheta(1 - p)} + \left(1 - \frac{\vartheta}{\zeta}\right) \frac{1}{p} \right] \quad (169)$$

$$= |D| \left[ \frac{\vartheta}{\zeta} + 1 - \frac{\vartheta}{\zeta} \right] = |D|. \quad (170)$$

QED. □
Lemma 23. For $M \in \mathbb{N}$, $M \leq |B|^2$, $M$ unitaries $V^B_i \in \mathbb{U}(B)$ such that $\text{Tr}(V^B_i V^B_j) = |B| \delta_{i,j}$, let $\mathcal{V}_M : B \to B$ be a ctp map given by

$$\mathcal{V}_M(\sigma^B) \equiv \frac{1}{M} \sum_{i=1}^{M} V^B_i \cdot \sigma^B.$$  \hfill (171)

Then

$$\Theta(\mathcal{V}_M \circ T_W) \leq \log |B| - \log M.$$  \hfill (172)

Proof. Let $W |i\rangle^A = |i\rangle^B$ for $i \leq |B|$, and $W |i\rangle^A = 0$ for $i > |B|$, where $\{|i\rangle^A\}$ and $\{|i\rangle^B\}$ are orthonormal states in their respective systems. Using $T_W(|i\rangle \langle j|) = \frac{|A|}{|B|} |i\rangle^B \langle j|^{B \text{ ind}_{[i,j \leq |B|]}}$, we have

$$\exp\{\Theta(\mathcal{V}_M \circ T_W)\} \leq \frac{|B|^2}{|A|^2} \sum_{i,j} \text{Tr} \left[ \mathcal{V} \circ T_W(|i\rangle \langle j|) \mathcal{V} \circ T_W(|j\rangle \langle i|) \right]$$  \hfill (173)

$$= \frac{1}{|B|^2} \text{Tr} \left[ \sum_{i,j \leq |B|} \mathcal{V}(|i\rangle \langle j|) \mathcal{V}(|j\rangle \langle i|) \right]$$  \hfill (174)

$$= \frac{1}{|B|^2} \text{Tr} \left[ \sum_{i,j \leq |B|} \sum_{k,l=1}^{M} V_k |i\rangle \langle j| V_l \mathcal{V}(|i\rangle \langle j|) V_l^{\dagger} V_k^{\dagger} \right]$$  \hfill (175)

$$= \frac{1}{|B|^2} \sum_{k,l=1}^{M} \text{Tr} V_l^{\dagger} V_k^2 = \frac{1}{|B|^2} \sum_{k,l=1}^{M} |B|^2 \delta_{k,l} = \frac{|B|}{M},$$  \hfill (176)

where the first inequality follows using (1) and the fourth equality follows since $\text{Tr} V_l^{\dagger} V_k = |B| \delta_{k,l}$. QED.

B Lemmata

Lemma 24. Let $T$ be a completely positive map. Then for any inputs $\sigma$, $\theta$ (not necessarily Hermitian), there exists a contraction $K$ such that

$$T(\sigma^{\dagger}) T(\theta^{\dagger}) = \sqrt{T(\sigma^{\dagger})} K T(\theta^{\dagger}) K^{\dagger} \sqrt{T(\sigma^{\dagger})}.$$  \hfill (177)

In particular, if $\theta = 1$ and $T(1)$ is a scaled identity, i.e., commutes with all matrices, then

$$T(\sigma) T(\sigma^{\dagger}) \leq T(\sigma^{\dagger}) T(1).$$  \hfill (178)

An example of such a $T$ is the partial trace.
Proof. Since $\mathcal{T}$ is completely positive, it is also 2-positive. Hence, if $\mathcal{I}_2$ is the identity super-operator for $2 \times 2$ matrices, then for orthonormal $|0\rangle, |1\rangle$, we have

$$0 \leq (\mathcal{I}_2 \otimes \mathcal{T}) \left[ (|0\rangle \otimes \theta + |1\rangle \otimes \sigma)(|0\rangle \otimes \theta + |1\rangle \otimes \sigma)^\dagger \right]$$

$$= |0\rangle \langle 0| \otimes \mathcal{T}(\theta \theta^\dagger) + |1\rangle \langle 1| \otimes \mathcal{T}(\theta \theta^\dagger) + |0\rangle \langle 1| \otimes \mathcal{T}(\theta \sigma^\dagger) + |1\rangle \langle 0| \otimes \mathcal{T}(\sigma \theta^\dagger). \quad (179)$$

We now invoke Theorem IX.5.9 in Ref. [35] to claim that there exists a contraction $K$ such that

$$\mathcal{T}(\sigma \theta^\dagger) = \sqrt{\mathcal{T}(\sigma \sigma^\dagger)} K \sqrt{\mathcal{T}(\theta \theta^\dagger)}. \quad (181)$$

The claim and the particular case now follow easily.

Lemma 25. Let $\mathcal{T}^{A \to E}$ be any completely positive map such that $\text{Tr} \mathcal{T}(1^A) = |A|$. Then $\mathcal{T}^{A \to E}$ is a class-1 map. For any ctp map $\mathcal{E}^{E \to C}$, $\mathcal{E}^{E \to C} \circ \mathcal{T}^{A \to E}$ is also a class-1 map.

Proof. Let the Kraus operators of $\mathcal{T}$ be given by $\{E_i\}$. We have for a random Unitary $U$ over $A$ and any $\sigma \in L(H_A)$,

$$E_U \|\mathcal{T}(U \cdot \sigma)\|_1 = \frac{1}{|A|^2} \sum_j \|\mathcal{T}(U_j \cdot \sigma)\|_1 = \frac{1}{|A|^2} \sum_{i,j} \|\langle j | B \otimes E_i U_j \rangle \cdot \sigma\|_1 = \|\mathcal{F}(\sigma)\|_1 \leq \|\sigma\|_1, \quad (182)$$

where in the second equality, $\{|j\rangle_B\}$ is an orthonormal basis in $B$, $\mathcal{F}^{A \to BE}$ is a ctp map with Kraus operators $\{\frac{1}{|A|}[\langle j | B \otimes E_i U_j \rangle]\}$, and the last inequality is well known. The second statement of the claim follows simply by noting that $\text{Tr} \mathcal{E} \circ \mathcal{T}(1^A) = \text{Tr} \mathcal{T}(1^A) = |A|$. QED.

Lemma 26. For any matrices $\sigma^{AR}, X^A, W^R$ (not necessarily Hermitian) and for $U$ acting on $A$, we have

$$E_U \left\{ U \sigma^{AR} U^\dagger (X^A \otimes W^R) U (\sigma^{AR})^\dagger U^\dagger \right\} = X^A \otimes \left( |A| \Lambda^R - \Upsilon^R \right) + (\text{Tr} X^A) \mathbb{1}^A \otimes \left( |A| \Upsilon^R - \Lambda^R \right), \quad (186)$$

where $\Lambda^R = \sigma^RW^R(\sigma^R)^\dagger$ and $\Upsilon^R = \text{Tr}_A [\sigma^{AR}(1^A \otimes W^R)(\sigma^{AR})^\dagger]$. 

32
Proof. Consider first vectors \{ |\varphi_i\rangle \}, i \in 1, \ldots, 6, in \mathcal{H}_A and we have
\[
\mathbb{E}_U \left\{ U |\varphi_1\rangle \langle \varphi_2| U^\dagger |\varphi_3\rangle \langle \varphi_4| U |\varphi_5\rangle \langle \varphi_6| U^\dagger \right\} 
= (1 \otimes \langle \varphi_4|) \mathbb{E}_U \left\{ (U \otimes U)(|\varphi_1\rangle \langle \varphi_2|) (U^\dagger \otimes U^\dagger) \right\} (1 \otimes |\varphi_3\rangle) 
= (1 \otimes \langle \varphi_4|) \left( \frac{q_1|A| - q_2}{|A|(|A| - 1)} I_{AA'} + \frac{q_2|A| - q_1}{|A|(|A| - 1)} F_{AA'} \right) (1 \otimes |\varphi_3\rangle)
\]
where the integral in the second equality is well known (see Lemma 3.4 in Ref. [17]), 
\( q_1 = \langle \varphi_6 | \varphi_1 \rangle \langle \varphi_2| \varphi_5 \rangle, \quad q_2 = \langle \varphi_2| \varphi_1 \rangle \langle \varphi_6| \varphi_5 \rangle, \) and \( F_{AA'} \) is the swap operator. We have by singular value decomposition:
\[
X^A = \sum_i \eta_i |y_i\rangle \langle z_i|^A.
\]
We also have by the singular value and Schmidt decompositions:
\[
\sigma^{AR} = \sum_{i,j,k} \sqrt{\beta_i^2 \lambda_{i,j} \mu_{i,k}} |v_{ij}\rangle \langle w_{ik}|^A \otimes |v_{ij}\rangle \langle w_{ik}|^R.
\]
Let \( i_1^2 = (i_1, j_1), i_2^3 = (i_1, \ldots, i_3), j_1^2 = (j_1, j_2) \) and \( k_1^2 = (k_1, k_2) \). We now have
\[
\mathbb{E}_U \left\{ U \sigma^{AR} U^\dagger (X^A \otimes W^R) U (\sigma^{AR})^\dagger U^\dagger \right\} 
= \sum_{i_1^2, j_1^2, k_1^2} f_1(i_1^2, j_1^2, k_1^2) \mathbb{E}_U \left\{ U(|v_{i_1 j_1}\rangle \langle w_{i_1 k_1}|^A \otimes |v_{i_1 j_1}\rangle \langle w_{i_1 k_1}|^R) U^\dagger(|y_{i_3}\rangle \langle z_{i_3}|^A \otimes W^R) \right\} 
= \sum_{i_1^2, j_1^2, k_1^2} f_1(i_1^2, j_1^2, k_1^2) \langle w_{i_1 k_1}| W |w_{i_2 j_2}|^R \times 
\mathbb{E}_U \left\{ U(|v_{i_3 j_3}|^A \langle w_{i_1 k_1}| U^\dagger |y_{i_3}\rangle \langle z_{i_3}| U |w_{i_2 j_2}|^A \langle v_{i_2 k_2}| U^\dagger \right\} \otimes |v_{i_1 j_1}\rangle \langle v_{i_2 k_2}|^R \right\}
= \sum_{i_1^2, j_1^2, k_1^2} f_1(i_1^2, j_1^2, k_1^2) \langle w_{i_1 k_1}| W |w_{i_2 j_2}|^R \left[ \frac{q_1(i_1^2, j_1^2, k_1^2)|A| - q_2(i_1^2, j_1^2, k_1^2)}{|A|(|A| - 1)} \right] \langle z_{i_3}| y_{i_3}\rangle \langle z_{i_3}|^A I^A + 
\frac{q_2(i_1^2, j_1^2, k_1^2)|A| - q_1(i_1^2, j_1^2, k_1^2)}{|A|(|A| - 1)} \langle y_{i_3}\rangle \langle z_{i_3}|^A \right\} \otimes |v_{i_1 j_1}\rangle \langle v_{i_2 k_2}|^R \right\}
= X^A \otimes (|A^R - \Upsilon^R| + (\text{Tr}X^A)I^A \otimes (|A^R - \Lambda^R|)
\]
where in the first equality
\[
f_1(i_1^2, j_1^2, k_1^2) = \sqrt{\beta_i^2 \lambda_{i_1, j_1} \mu_{i_1, k_1} \eta_{i_2} \beta_{i_2}^2 \lambda_{i_2, j_2} \mu_{i_2, k_2}}.
\]
in the third equality,
\[
q_1(i_1^2, j_1^2, k_1^2) = \langle w_{i_1k_1} | w_{i_2j_2} \rangle^A \langle v_{i_2k_2} | v_{i_1j_1} \rangle^A
\]
(198)
\[
q_2(i_1^2, j_1^2, k_1^2) = \langle w_{i_1k_1} | v_{i_1j_1} \rangle^A \langle v_{i_2k_2} | w_{i_2j_2} \rangle^A,
\]
(199)
and the fourth equality follows after simplifications. QED.

**Lemma 27.** Let \( T^{A\rightarrow E} \) be a completely positive map with the Choi-Jamiołkowski representation \( \omega_T^{E_A} \). Then for random Unitary \( U \) acting on \( A \), any matrix \( \sigma^{AR} \), we have
\[
E_U \left\{ \left[ T \left( U \cdot \sigma^{AR} \right) - \omega_T^E \otimes \sigma^R \right] \left[ T \left( U \cdot \sigma^{AR} \right) - \omega_T^E \otimes \sigma^R \right]^\dagger \right\} = \frac{Q_A' \left( \omega_T^{E_A} \right) \otimes Q_A(\sigma^{AR})}{|A|^2 - 1}
\]
\[
\leq \frac{|A|^2}{|A|^2 - 1} \text{Tr}_{A'} \left( \omega_T^{E_A} \right)^2 \otimes \text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right].
\]
(200)

**Proof.** Let \( T \) be described by the Kraus operators \( \{ T_k \} \). We now have
\[
E_U \left\{ \left[ T \left( U \cdot \sigma^{AR} \right) - \omega_T^E \otimes \sigma^R \right] \left[ T \left( U \cdot \sigma^{AR} \right) - \omega_T^E \otimes \sigma^R \right]^\dagger \right\}
= \sum_{k,l} T_k E_U \left\{ U \sigma^{AR} U^\dagger T_k^\dagger T_l U (\sigma^{AR})^\dagger U^\dagger \right\} T_l^\dagger - (\omega_T^E)^2 \otimes \sigma^R(\sigma^R)^\dagger
\]
(201)
\[
= \sum_{k,l} T_k \left\{ T_k^\dagger T_l \otimes \frac{|A|\sigma^R(\sigma^R)^\dagger - \text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right]}{|A|(|A|^2 - 1)} \right\} T_l^\dagger + (\text{Tr}_{k} T_l^\dagger) 1_A \otimes \frac{|A|\text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] - \sigma^R(\sigma^R)^\dagger}{|A|(|A|^2 - 1)}
\]
(202)
\[
= \frac{|A|^2}{|A|^2 - 1} \left( \omega_T^E \right)^2 \otimes |A|\sigma^R(\sigma^R)^\dagger - \text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] + |A|^2 \text{Tr}_{A'} \left( \omega_T^{E_A} \right)^2 \otimes \frac{|A|\text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] - \sigma^R(\sigma^R)^\dagger}{|A|(|A|^2 - 1)} - (\omega_T^E)^2 \otimes \sigma^R(\sigma^R)^\dagger
\]
(203)
\[
= \frac{|A|^2}{|A|^2 - 1} \left( \omega_T^E \right)^2 \otimes |A|^2 \sigma^R(\sigma^R)^\dagger - |A|\text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] + |A|^2 \text{Tr}_{A'} \left( \omega_T^{E_A} \right)^2 \otimes \frac{|A|\text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] - \sigma^R(\sigma^R)^\dagger}{|A|(|A|^2 - 1)} - (\omega_T^E)^2 \otimes \sigma^R(\sigma^R)^\dagger
\]
(204)
\[
= \frac{Q_A' \left( \omega_T^{E_A} \right) \otimes Q_A(\sigma^{AR})}{|A|^2 - 1}
\]
(205)
\[
\leq \frac{|A|^2}{|A|^2 - 1} \text{Tr}_{A'} \left( \omega_T^{E_A} \right)^2 \otimes \text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right],
\]
(206)
where in the second equality, we have used Lemma 26, and the inequality follows by noting from Lemma 24 that \(|A|\text{Tr}_{A} \left[ \sigma^{AR}(\sigma^{AR})^\dagger \right] - \sigma^R(\sigma^R)^\dagger \in \text{Pos}(\mathcal{H}_R)\). QED. □
Lemma 28 (Exercise 9.9 in Ref. [3]). Let $\rho \in \mathcal{D}(\mathcal{H}_A)$, $\sigma \in \text{Pos}(\mathcal{H}_A)$, and $\Pi = \{ \mathcal{M}_\sigma(\rho) \geq \zeta \sigma \}$. Then for any $\alpha \in (1, 2]$, we have

$$\| \Pi \rho \|_1 \leq \zeta^{1/\alpha} \sqrt{Q_\alpha(\rho\|\sigma)} = \zeta^{1/2} \exp \left\{ \frac{\alpha - 1}{2} D_\alpha(\rho\|\sigma) \right\}.$$  

(207)

Lemma 29 (Hayashi [3]). Let $\rho \in \mathcal{D}(\mathcal{H}_A)$, $\sigma \in \text{Pos}(\mathcal{H}_A)$, $\Pi = \{ \mathcal{M}_\sigma(\rho) \geq \zeta \sigma \}$ and $\hat{\Pi} = \mathbb{1} - \Pi$. Then

$$\text{Tr} \sigma^{-1} \hat{\Pi} \rho \| \hat{\Pi} \leq \nu_\sigma \zeta.$$  

(208)

The proof of this lemma is contained in Lemma 9.2 in Ref. [3].

Lemma 30. Let $\sigma, \rho \in \text{Pos}(\mathcal{H}_A)$. Then

$$\text{Tr} \rho + \text{Tr} \sigma - 2 F(\rho, \sigma) \leq \| \rho - \sigma \|_1 \leq \sqrt{(\text{Tr} \rho + \text{Tr} \sigma)^2 - 4F(\rho, \sigma)^2}. $$  

(209)

Proof. The proof is essentially along the lines of the Fuchs-van de Graaf inequalities. We know that

$$F(\rho, \sigma) = \min_{\text{POVM}\{\Lambda_m\}} \sum_m \sqrt{p_m q_m},$$

where $p_m \equiv \text{Tr} \Lambda_m \rho$ and $q_m \equiv \text{Tr} \Lambda_m \sigma$. Note that $\sum_m p_m = \text{Tr} \rho$ and $\sum_m q_m = \text{Tr} \sigma$. Let $\{\Lambda_m\}$ be the minimizing POVM in the above equation. We now have

$$\| \rho - \sigma \|_1 \geq \left\| \sum_m |m\rangle \langle m| X \otimes \sqrt{\Lambda_m} \rho \sqrt{\Lambda_m} - \sum_m |m\rangle \langle m| X \otimes \sqrt{\Lambda_m} \sigma \sqrt{\Lambda_m} \right\|_1$$

$$\geq \left\| \sum_m p_m |m\rangle \langle m| X - \sum_m q_m |m\rangle \langle m| X \right\|_1 = \sum_m |p_m - q_m|$$

$$= \sum_m |\sqrt{p_m} - \sqrt{q_m}| |\sqrt{p_m} + \sqrt{q_m}| \geq \sum_m (\sqrt{p_m} - \sqrt{q_m})^2 = \text{Tr} \rho + \text{Tr} \sigma - 2 F(\rho, \sigma),$$

(211)

where the first inequality follows from the monotonicity under the application of a cptp map with Kraus operators $\{|m\rangle X \otimes \sqrt{\Lambda_m}\}$, where $\{|m\rangle X\}$ is an orthonormal basis, and the second inequality follows again from monotonicity under partial trace.

To prove the other inequality, let $|u_\rho\rangle$ and $|v_\sigma\rangle$ be purifications of $\rho$ and $\sigma$ respectively such that $F(\rho, \sigma) = \langle u_\rho | v_\sigma \rangle$. We now have

$$\| \rho - \sigma \|_1 \leq \| u_\rho - v_\sigma \|_1 = \sqrt{(\text{Tr} \rho + \text{Tr} \sigma)^2 - 4F(\rho, \sigma)^2}. $$

(212)

QED.
Lemma 31. Let $\Psi^A \in \mathcal{D}(\mathcal{H}_A)$, $\xi^A \in \text{Pos}(\mathcal{H}_A)$ such that $\|\xi^A - \Psi^A\|_1 \leq \varepsilon$. Let $\xi^{AB}$, $\Psi^{AC}$, $|B| \leq |C|$, be purifications of $\xi^A$ and $\Psi^A$ respectively. Then there exists a partial isometry $V^{B\rightarrow C}$ such that
\[
\|V^{B\rightarrow C} \cdot \xi^{AB} - \Psi^{AC}\|_1 \leq \sqrt{4 + 3\varepsilon}.
\] (213)

Note that if it is known that $\xi^A \in \mathcal{D}(\mathcal{H}_A)$, then from Corollary 2.2 in Ref. [36], the bound in the RHS can be refined to $2\sqrt{\varepsilon}$.

Proof. We use the first inequality in the claim of Lemma 30 to have
\[
\text{Tr}\xi^A + \text{Tr}\Psi^A - 2F(\xi^A, \Psi^A) \leq \varepsilon.
\] (214)

Using the Uhlmann’s theorem [37], we claim that there exists a partial isometry $V^{B\rightarrow C}$ such that $F(\xi^A, \Psi^A) = F(V^{B\rightarrow C} \cdot \xi^{AB}, \Psi^{AC})$, and hence,
\[
\text{Tr}\xi^{AC} + \text{Tr}\Psi^{AC} - 2F(V^{B\rightarrow C} \cdot \xi^{AB}, \Psi^{AC}) \leq \varepsilon.
\] (215)

Since, using monotonicity, $F(V^{B\rightarrow C} \cdot \xi^{AB}, \Psi^{AC}) \leq (\text{Tr}\xi^A)(\text{Tr}\Psi^A)$, and $|\text{Tr}\xi^A - \text{Tr}\Psi^A| \leq \varepsilon$, or, $\text{Tr}\xi^A \leq 1 + \varepsilon$, hence, $\text{Tr}\xi^{AC} + \text{Tr}\Psi^{AC} + 2F(V^{B\rightarrow C} \cdot \xi^{AB}, \Psi^{AC}) \leq 4 + 3\varepsilon$. Using the second inequality in the claim of Lemma 30 again, we arrive at
\[
\|V^{B\rightarrow C} \cdot \xi^{AB} - \Psi^{AC}\|_1 \leq \sqrt{\text{Tr}\xi^{AC} + \text{Tr}\Psi^{AC} - 2F(V^{B\rightarrow C} \cdot \xi^{AB}, \Psi^{AC})} \leq \sqrt{4 + 3\varepsilon}. 
\] (216)

QED.

\[\square\]

Corollary 32 (A straightforward corollary of Lemma 9.2 in Ref. [3]). Consider a cq state
\[
\rho^{XR} \equiv \sum_{x \in \mathcal{X}} p_x \langle x| x \rangle^X \otimes \rho_x^R,
\] (217)
where $\rho_x^R \in \mathcal{D}(\mathcal{H}_R)$, $x \in \mathcal{X}$, and \{ $p_x, x \in \mathcal{X}$ \} is a probability vector. Let $\rho^R = \text{Tr}_X \rho^{XR}$, $\zeta > 0$, $M \in \mathbb{N}$, any $\kappa^R \in \mathcal{D}(\mathcal{H}_R)$, and $X^M \equiv (X_1, ..., X_M)$ be $M$ i.i.d. random variables with probability distribution \{ $p_x, x \in \mathcal{X}$ \}. Then we have for any $\alpha \in (1, 2]$,
\[
E_X M \left\| \frac{1}{M} \sum_{i=1}^{M} \rho_{X_i}^R - \rho^R \right\|_1 \leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ \log \nu_{\kappa_R} + D_{\alpha}(\rho^{XR}\|\rho^X \otimes \kappa^R) - \log M \right] \right\}. 
\] (218)

Proof. It follows from the claims of Lemma 9.2 in Ref. [3] that for any $\zeta > 0$,
\[
E_X M \left\| \frac{1}{M} \sum_{i=1}^{M} \rho_{X_i}^R - \rho^R \right\|_1 \leq 2 \sum_{x} p_x \zeta^{\frac{1-\alpha}{2}} \sqrt{Q_{\alpha}(\rho_x^R\|\kappa^R)} + \sqrt{\frac{\nu_{\kappa_R} \zeta}{M}} \leq 2 \zeta^{\frac{1-\alpha}{2}} \exp \left( \frac{\alpha - 1}{2} D_{\alpha}(\rho^{XR}\|\rho^X \otimes \kappa^R) \right) + \sqrt{\frac{\nu_{\kappa_R} \zeta}{M}}. 
\] (219)
If we make a choice of
\[
\zeta = \left( \frac{2 \exp \left\{ \frac{\alpha - 1}{2 \alpha} D_\alpha (\rho^{XR} \| \rho^X \otimes \kappa^R) \right\}}{\nu_{\kappa,R}} \right)^{\frac{2}{\alpha}}, \tag{221}
\]
we get
\[
\mathbb{E}_M \left\| \frac{1}{M} \sum_{i=1}^{M} \rho^R_{X_i} - \rho^R \right\|_1 \leq 4 \exp \left\{ \frac{\alpha - 1}{2 \alpha} \left[ \log \nu_{\kappa,R} + D_\alpha (\rho^{XR} \| \rho^X \otimes \kappa^R) - \log M \right] \right\}. \tag{222}
\]
QED.

C  A more general decoupling theorem that we never use!

**Theorem 33.** Let \( \mathcal{X} \) be a finite set, \( \{p_x, x \in \mathcal{X}\} \) a probability distribution on \( \mathcal{X} \), \( \rho^{AR}_x \in \mathcal{D}(\mathcal{H}_{AR}) \) \( \forall x \in \mathcal{X} \), and \( \{|x\rangle \langle x|\}_{\mathcal{X}} \) a set of orthonormal states in \( X \). Consider a cq state
\[
\rho^{XAR} \equiv \sum_{x \in \mathcal{X}} p_x |x\rangle \langle x| \otimes \rho^{AR}_x. \tag{223}
\]
For \( M \in \mathbb{N} \), let \( X_1, \ldots, X_M \) be \( M \) independent and identically distributed (i.i.d.) random variables having probability distribution \( \{p_x, x \in \mathcal{X}\} \), and \( \mathcal{T}_{\mathcal{A} \rightarrow \mathcal{E}} \) a class-1 map. Then for \( \alpha \in (1,2] \), \( X_i^M \equiv (X_1, \ldots, X_M) \), random Unitaries \( U_i^M \equiv (U_1, \ldots, U_M) \) acting independently on \( \mathcal{A} \), we have for any \( \sigma^R, \kappa^R \in \mathcal{D}(\mathcal{H}_R) \),
\[
\mathbb{E}_{X_i^M} \mathbb{E}_{U_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} \mathcal{T}(U_i \cdot \rho^{AR}_{X_i}) - \omega^E_T \otimes \rho^R \right\|_1
\]
\[
\leq 4 \exp \left\{ \frac{\alpha - 1}{2 \alpha} \left[ \log \nu_{\kappa,R} + D_\alpha (\rho^{XAR} \| \rho^X \otimes \mathbb{1}_A \otimes \sigma^R) - \log M + \Theta(\mathcal{T}) \right] \right\} \text{ind}_{|\mathcal{X}| \neq 1}
\]
\[
+ 4 \exp \left\{ \frac{\alpha - 1}{2 \alpha} \left[ \log \nu_{\kappa,R} + D_\alpha (\rho^{XR} \| \rho^X \otimes \kappa^R) - \log M \right] \right\} \text{ind}_{|\mathcal{X}| \neq 1}. \tag{224}
\]

**Proof.** We have
\[
\mathbb{E}_{X_i^M} \mathbb{E}_{U_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} \mathcal{T}(U_i \cdot \rho^{AR}_{X_i}) - \omega^E_T \otimes \rho^R \right\|_1
\]
\[
\leq \mathbb{E}_{X_i^M} \mathbb{E}_{U_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} [\mathcal{T}(U_i \cdot \rho^{AR}_{X_i}) - \omega^E_T \otimes \rho^R_{X_i}] \right\|_1 + \mathbb{E}_{X_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} \omega^E_T \otimes \rho^R_{X_i} - \omega^E_T \otimes \rho^R \right\|_1
\]
\[
= \mathbb{E}_{X_i^M} \mathbb{E}_{U_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} [\mathcal{T}(U_i \cdot \rho^{AR}_{X_i}) - \omega^E_T \otimes \rho^R_{X_i}] \right\|_1 \text{ind}_{|\mathcal{A}| \neq 1} + \mathbb{E}_{X_i^M} \left\| \frac{1}{M} \sum_{i=1}^{M} \rho^R_{X_i} - \rho^R \right\|_1 \text{ind}_{|\mathcal{X}| \neq 1}, \tag{225}
\]
where the inequality follows from the triangle inequality and the last equality follows since \( \|X \otimes Y\|_1 = \|X\|_1\|Y\|_1 \), and the first and the second terms are identically zero if \(|A| = 1\) and \(|X| = 1\) respectively. The upper bound for the second term can be deduced from Lemma 9.2 in Ref. [3] for any \( \alpha \in (1, 2) \) and any \( \kappa^R \in \mathfrak{D}(\mathcal{H}_R) \) as

\[
E_{X_i^M} \left\| \frac{1}{M} \sum_{i=1}^M \rho_{X_i}^R - \rho^R \right\|_1 \leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ \log \nu_R + D_\alpha(\rho_X^R \| \rho^X \otimes \kappa^R) - \log M \right] \right\}. \tag{226}
\]

Note that Lemma 9.2 in Ref. [3] doesn’t provide an upper bound in the above form but it is easy to deduce it from the claim, and, for the sake of completeness, it is provided in Corollary 32 in the appendix.

The rest of the proof is to upper bound the first term in (225). For \( \zeta > 0 \) and \( \forall x \in \mathcal{X} \), let \( \Pi^R_x \equiv \{ \mathcal{M}_{1^A \otimes \sigma^R}(\rho^A_x) \geq \zeta \mathbb{1}^A \otimes \sigma^R \} \), \( \tilde{\Pi}_x^R \equiv \mathcal{I}^A - \Pi_x^R \), \( \mu_1 \equiv \omega^E \otimes \text{Tr}_A \{ \Pi_x^R \rho^A_x \} \), and \( \mu_2 \equiv \omega^E \otimes \text{Tr}_A \{ \tilde{\Pi}_x^R \rho^A_x \} \). Note that \( \mu_1 + \mu_2 = \omega^E \otimes \rho^R \). We now have from the triangle inequality

\[
E_{X_i^M}^U \left\| \frac{1}{M} \sum_{i=1}^M \left\{ T(U_i \cdot (\Pi^R_x \rho_{X_i}^R)) - \mu_{1,X_i} \right\} \right\|_1 \leq 2 \sum_{i=1}^M p_x \left\| \Pi^R_x \rho_{X_i}^R \right\|_1 \leq \zeta \frac{1}{\alpha} \sum_{x} p_x \sqrt{Q_\alpha(\rho^A_x \| \mathbb{1}^A \otimes \sigma^R)} \leq 2\zeta \frac{1}{\alpha} \exp \left\{ \frac{\alpha - 1}{2} \left[ D_\alpha(\rho^X \| \rho^X \otimes \mathbb{1}^A \otimes \sigma^R) \right] \right\}, \tag{232}
\]

We now attack the first term.

\[
E_{X_i^M}^U \left\| \frac{1}{M} \sum_{i=1}^M \left\{ T(U_i \cdot (\Pi^R_x \rho_{X_i}^R)) - \mu_{1,X_i} \right\} \right\|_1 \leq 2 \sum_{i=1}^M p_x \left\| \Pi^R_x \rho_{X_i}^R \right\|_1 \leq \zeta \frac{1}{\alpha} \sum_{x} p_x \sqrt{Q_\alpha(\rho^A_x \| \mathbb{1}^A \otimes \sigma^R)} \leq 2\zeta \frac{1}{\alpha} \exp \left\{ \frac{\alpha - 1}{2} \left[ D_\alpha(\rho^X \| \rho^X \otimes \mathbb{1}^A \otimes \sigma^R) \right] \right\}, \tag{232}
\]

38
where the first inequality follows from the triangle inequality, the second inequality follows from the convexity of the trace norm to have

$$E_{X_i} \| \mu_{1,X_i} \|_1 = E_{X_i} \left\| \frac{1}{M} \sum_{i=1}^M E_{U_i} \left\{ T \left[ U_i \cdot (\Pi_{X_i}^{AR} \rho_{X_i}^{AR}) \right] \right\} \right\|_1$$

$$\leq \frac{1}{M} \sum_{i=1}^M E_{X_i} \left\| E_{U_i} \left\{ T \left[ U_i \cdot (\Pi_{X_i}^{AR} \rho_{X_i}^{AR}) \right] \right\} \right\|_1 \leq \frac{1}{M} \sum_{i=1}^M E_{X_i} E_{U_i} \left\{ T \left[ U_i \cdot (\Pi_{X_i}^{AR} \rho_{X_i}^{AR}) \right] \right\} \right\|_1,$$  \hspace{1cm} (233)

and similarly for the first term, the first equality follows since $X_i$'s and $U_i$'s are i.i.d., the third inequality follows from the definition of class-1 maps, the fourth inequality follows from Lemma 28 (proved by Hayashi [3]), and the last inequality follows from the concavity of $x \mapsto \sqrt{x}$.

We now attack the second term. Let $\Delta_{X,U_i} \equiv T \left[ U_i \cdot (\hat{\Pi}_{X_i}^{AR} \rho_{X_i}^{AR}) \right] - \mu_{2,X_i}$ and $\Delta_{X,U_i}^{M_U} \equiv \frac{1}{M} \sum_{i=1}^M \Delta_{X,U_i}$. Note that $E_{X_i} \left\{ \Delta_{X,i} \Delta_{X,i}^\dagger \right\} = 0, \forall i \neq j$, and hence,

$$E_{X_i} \left\{ \Delta_{X,U_i}^{M_U} \Delta_{X,U_i}^{\dagger M_U} \right\} = \frac{1}{M^2} \sum_{i=1}^M E_{X_i} \left\{ \Delta_{X,U_i} \Delta_{X,U_i}^\dagger \right\} = \frac{1}{M} E_{X_i} \left\{ \Delta_{X,U_i} \Delta_{X,U_i}^\dagger \right\} \right\}$$

$$\leq \frac{|A|^2 \text{Tr}_{A'} \left( \omega_{E'}^2 \right)^2}{M(|A|^2 - 1)} \otimes \text{Tr}_A E_{X_i} \left\{ \hat{\Pi}_{X_i}^{AR}(\rho_{X_i}^{AR})^2 \hat{\Pi}_{X_i}^{AR} \right\}$$

(234)

where the inequality follows from Lemma 27. Following the arguments in Theorem 1 in dealing with the second term, we get

$$E_{X_i} \left\{ \frac{1}{M} \sum_{i=1}^M \left\{ T \left[ U_i \cdot (\hat{\Pi}_{X_i}^{AR} \rho_{X_i}^{AR}) \right] - \mu_{2,X_i} \right\} \right\} \right\} \leq \sqrt{\frac{\nu_{\sigma R} \zeta |A|^2 \exp \{ \Theta(T) \}}{M(|A|^2 - 1)}}.$$  \hspace{1cm} (236)

We now have

$$E_{X_i} E_{U_i}^M \left\{ \frac{1}{M} \sum_{i=1}^M \left\{ T \left( U_i \cdot \rho_{X_i}^{AR} \right) - \omega_{T} \otimes \rho_{X_i} \right\} \right\}$$

$$\leq 2^{\zeta \frac{1-\alpha}{2}} \exp \left\{ \frac{\alpha - 1}{2} \left[ D_{\alpha}(\rho_{X}^{AR} \| \rho_{X} \otimes 1^A \otimes \sigma^R) \right] \right\} + \sqrt{\frac{\nu_{\sigma R} \zeta |A|^2 \exp \{ \Theta(T) \}}{M(|A|^2 - 1)}},$$  \hspace{1cm} (237)

and by appropriately choosing $\zeta$, we get

$$E_{X_i} E_{U_i}^M \left\{ \frac{1}{M} \sum_{i=1}^M \left\{ T \left( U_i \cdot \rho_{X_i}^{AR} \right) - \omega_{T} \otimes \rho_{X_i} \right\} \right\}$$

$$\leq 4 \exp \left\{ \frac{\alpha - 1}{2\alpha} \left[ \log \nu_{\sigma R} + D_{\alpha}(\rho_{X}^{AR} \| \rho_{X} \otimes 1^A \otimes \sigma^R) - \log M + \Theta(T) \right] \right\}.$$  \hspace{1cm} (238)

The claim now follows from (225), (226), and (238).
References

[1] T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley, Hoboken, NJ, USA, 2nd edn., 2006.

[2] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[3] M. Hayashi. *Quantum information: An introduction*. Springer, Berlin, 2006.

[4] M. Ohya and D. Petz. *Quantum Entropy and its use*. Springer-Verlag, Berlin, 1st edn., 1993.

[5] M. M. Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[6] R. Renner. *Security of quantum key distribution*. Ph.D. thesis, Swiss Federal Institute of Technology, ETH, Zurich, Switzerland, 2005.

[7] M. Tomamichel. *A framework for non-asymptotic quantum information theory*. Ph.D. thesis, Swiss Federal Institute of Technology, ETH, Zurich, Switzerland, 2012.

[8] R. G. Gallager. *A simple derivation of the coding theorem and some applications*. IEEE Trans. Inf. Theory, vol. 11: pp. 3–18, Jan. 1965.

[9] R. G. Gallager. *Information theory and reliable communication*. John Wiley & Sons, Inc., New York, 1968.

[10] V. Strassen. *Asymptotische Abschätzungen in Shannon’s informationtheorie*. In Trans. third Prague Conf. Inf. Theory, pp. 689–723. 1962.

[11] M. V. Burnashev and A. S. Holevo. *On reliability function of quantum communication channel*. Prob. Inf. Trans., vol. 34: pp. 97–107, 1998.

[12] A. S. Holevo. *Reliability function of general classical-quantum channel*. IEEE Trans. Inf. Theory, vol. 46: pp. 2256–2261, 2000.

[13] M. Hayashi. *Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding*. Phys. Rev. A, vol. 76: p. 062301, 2006.

[14] I. Devetak, A. W. Harrow, and A. Winter. *A family of quantum protocols*. Phys. Rev. Lett., vol. 93: p. 230504, Dec 2004.

[15] I. Devetak, A. W. Harrow, and A. Winter. *A resource framework for quantum Shannon theory*. IEEE Trans. Inf. Theory, vol. 54: pp. 4587–4618, 2008.

[16] B. Schumacher and M. A. Nielsen. *Quantum data processing and error correction*. Phys. Rev. A, vol. 54: pp. 2629–2635, Oct. 1996.
[17] F. Dupuis. *The decoupling approach to quantum information theory*. Ph.D. thesis, University of Montreal, Montreal, Canada, 2009.

[18] P. Hayden. *Decoupling: A building block for quantum information theory*. Tutorial at Quantum Information Processing (QIP) workshop, Jan. 2011.

[19] P. Hayden, M. Horodecki, A. Winter, and J. Yard. *A decoupling approach to the quantum capacity*. Open Syst. Inf. Dyn., vol. 15: pp. 7–19, 2008.

[20] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. *The mother of all protocols: restructuring quantum information’s family tree*. Proc. R. Soc. A, vol. 465: pp. 2537–63, 2009.

[21] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. *One-shot decoupling*. arXiv: 1012.6044.

[22] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. *On quantum Rényi entropies: a new generalization and some properties*. J. Math. Phys., vol. 54: p. 122203, 2013.

[23] M. M. Wilde, A. Winter, and D. Yang. *Strong converse for the classical capacity of entanglement-breaking and Hadamard channels*. arXiv: 1306.1586.

[24] D. Petz. *Quasi-entropies for finite quantum systems*. Rep. Math. Phys., vol. 23: pp. 57–65, Feb. 1986.

[25] D. Petz. *From f-divergence to quantum quasi-entropies and their use*. Entropy, vol. 12: pp. 304–325, Mar. 2010.

[26] M. Tomamichel, M. Berta, and M. Hayashi. *A duality relation connecting different quantum generalizations of the conditional Rényi entropy*. arXiv: 1311.3887.

[27] B. Schumacher. *Quantum coding*. Phys. Rev. A, vol. 51: pp. 2738–2747, 1995.

[28] I. Csiszár and J. Körner. *Information Theory: Coding theorems for discrete memoryless systems*. Cambridge University Press, New York, USA, 2nd edn., 2011.

[29] I. Devetak. *A triangle of dualities: reversibly decomposable quantum channels, source-channel duality, and time reversal*. Phys. Rev. Lett., vol. 97: p. 140503, 2006.

[30] M. Horodecki, J. Oppenheim, and A. Winter. *Quantum state merging and negative information*. Commun. Math. Phys., vol. 269: pp. 107–136, 2007.

[31] C. A. Fuchs and J. van de Graaf. *Cryptographic distinguishability measures for quantum mechanical states*. IEEE Trans. Inf. Theory, vol. 45: pp. 1216—1227, May 1998.
[32] I. Devetak and J. Yard. *Exact cost of redistributing multipartite quantum states.* Phys. Rev. Lett., vol. 100: p. 230501, Jun 2008.

[33] M.-Y. Ye, Y.-K. Bai, and Z. D. Wang. *Quantum state redistribution based on a generalized decoupling.* Phys. Rev. A, vol. 78: p. 030302, 2008.

[34] B. Groisman, S. Popescu, and A. Winter. *Quantum, classical, and total amount of correlations in a quantum state.* Phys. Rev. A, vol. 72: p. 032317, 2005.

[35] R. Bhatia. *Matrix Analysis.* Springer-Verlag, New York, 1997.

[36] F. Dupuis, O. Szehr, and M. Tomamichel. *A decoupling approach to classical data transmission over quantum channels.* IEEE Trans. Inf. Theory, vol. 60: pp. 1562–1572, Mar. 2014.

[37] A. Uhlmann. *The ‘transition probability’ in the state space of a *-algebra.** Rep. Math. Phys., vol. 9: pp. 273–279, 1976.