Smooth Entropy Bounds on One-Shot Quantum State Redistribution
Mario Berta, Matthias Christandl, Dave Touchette

Abstract

We give upper and lower bounds on the amount of quantum communication required to perform the task of quantum state redistribution in a one-shot setting. In quantum state redistribution as considered in [Luo and Devetak (2009)] and [Devetak and Yard (2008)], there are 4 systems of interest: the $A$ system held by Alice, the $B$ system held by Bob, the $C$ system that is to be transmitted from Alice to Bob, and the $R$ system that holds a purification of the state in the $ABC$ registers. Our bounds are in terms of smooth conditional min- and max- entropies, and the smooth max-information. The protocol for the upper bound has a clear structure, building on the work [Oppenheim (2008)]: it decomposes the quantum state redistribution task into two simpler quantum state merging tasks by introducing a coherent relay.

There remains a gap between our upper and lower bounds. This gap vanishes in the independent and identical (iid) asymptotic limit and the remaining terms can then be rewritten as a quantum conditional mutual information, thus yielding an alternative proof of optimality of this communication rate for iid asymptotic quantum state redistribution.

1 Introduction

In the task of quantum state redistribution, we are interested in the amounts of quantum communication and entanglement that are required to transmit part of the system of one party to another party who possess some side information about this system. It is required that all correlations, including those with any external system, are maintained. More formally, consider two parties Alice and Bob, with Alice initially holding the $A$ and $C$ registers, and Bob holding the $B$ register. The goal is then for Alice to transmit the $C$ register to Bob. If we consider a reference register $R$ holding a purification of the $ABC$ systems, then the global state on $ABCR$ is uncorrelated with any other external system, and it is sufficient to insure that correlations are maintained across these systems.

In the independent and identical (iid) asymptotic version, Alice and Bob want to perform this task on blocks of $n$ identical states, for $n$ large, and we are interested in the best asymptotic rates achievable. Luo and Devetak [20] proved a converse theorem in the iid asymptotic regime, stating that the quantum communication rate $q$ and the sum of the entanglement consumption rate $e$ and the quantum communication rate $q$, must be at least

\[ q \geq \frac{1}{2} I(C;R|B) \quad \text{and} \quad e + q \geq H(C|B). \]  

(1.1)
Subsequently, Devetak and Yard \cite{13, 30} proved that these rates are also achievable and hence fully characterized the achievable rate region for iid asymptotic quantum state redistribution. In \cite{11}, $H(C) = -\text{Tr}[\rho_C \log \rho_C]$ denotes the von Neumann entropy, $H(C|B) = H(CB) - H(B)$ the conditional von Neumann entropy, and

\begin{align}
I(C; R|B)_\rho &= H(BC)_\rho + H(BR)_\rho - H(B)_\rho - H(BCR)_\rho \\
&= H(C|B)_\rho - H(C|BR)_\rho
\end{align}

is the conditional quantum mutual information. Note that since the overall state $\rho_{ABCR}$ for quantum state redistribution is pure, we have the symmetry in $A-B$,

\begin{equation}
I(C; R|B)_\rho = I(C; R|A)_\rho.
\end{equation}

Later the achievability proofs for quantum state redistribution were significantly simplified by Oppenheim \cite{21} and independently by Ye et al. \cite{31}. State redistribution can be seen as the most general bipartite noiseless coding problem, and indeed, other noiseless quantum coding primitives such as Schumacher source coding \cite{23}, quantum state merging \cite{18, 19} (including fully quantum Slepian-Wolf \cite{1}), and state splitting \cite{1} can be obtained by considering the case of trivial $AB$, $A$ or $B$ system, respectively. Quantum state redistribution can also be understood as the fully quantum analogue of the tensor power input reverse Shannon theorem \cite{2, 6} with feedback to the sender and side information at the receiver.

In recent years, there has been some effort on finding good bounds for the one-shot version of these results (see, e.g., \cite{3, 15, 8, 6, 11, 16} and references therein). In the one-shot setting, instead of being interested in iid asymptotic rates, we are interested in the cost of achieving these tasks when only a single copy of the input state is available. Useful bounds are often stated in terms of so-called smooth conditional entropies (see the theses of Renner \cite{22} and Tomamichel \cite{24}, as well as references therein).

We are interested in finding good bounds for the quantum communication cost of one-shot quantum state redistribution in terms of smooth conditional entropies. Our main result states that it is possible to implement quantum state redistribution for a pure quantum state $\rho_{ABCR}$ up to error $\varepsilon$ with quantum communication cost at most

\begin{equation}
\frac{1}{2} \left( H_{\max}^{\varepsilon}(C|B)_\rho - H_{\min}^{\varepsilon}(C|BR)_\rho \right) + O(\log(1/\varepsilon)),
\end{equation}

when free entanglement assistance is available. Note that both the conditional min- and max-entropy terms appearing in \cite{15} are smoothed notwithstanding the fact that it is in general unknown how to simultaneously smooth marginals of overlapping quantum systems (see, e.g., \cite{14} and references therein). For the special case of iid asymptotic resources this then allows us to recover the optimal quantum communication rate \cite{11} by means of the fully quantum asymptotic equipartition property for smooth conditional entropies \cite{25}.

We also state lower bounds in terms of smooth conditional min- and max-entropies, and smooth max-information. However, our achievability bound \cite{15} does only match these lower bounds in an iid asymptotic scenario. We then also speculate on how to improve the bound \cite{15} with the help of embezzling entangled quantum states \cite{10} along with some of the ideas in \cite{6}. 

2
Our work originates from the author’s manuscripts [5, 28], where [5] is partly based on the preliminary results from [4]. Independently, the achievability bound (1.5) has also been derived by Datta et al. [12] (stated as in preparation in [11]). We mention that our main result (1.5) has already proven useful for applications in quantum complexity theory. In particular, based on the idea of quantum information complexity, one of the authors [27] was able to derive the first multi-round direct sum theorem in quantum communication complexity.

This document is structured as follows. In Section 2, we introduce our notation and give the definitions of the relevant smooth entropy measures. We then discuss in Section 3 the work of Oppenheim [21] arguing that quantum state redistribution can be optimally decomposed into two applications of quantum state merging. Our achievability bound for one-shot quantum state redistribution is then derived in Section 4, and the converse bounds can be found in Section 5. We end with some conclusions (Section 6).

2 Preliminaries

We assume that all Hilbert spaces are finite-dimensional. The dimension of the Hilbert space associated to a quantum system $A$ is denoted by $|A|$. The set of linear operators on a quantum system $A$ is denoted by $\mathcal{L}(A)$, and the set of linear, nonnegative operators by $\mathcal{P}(A)$. We denote by $\mathcal{D}_\leq(A)$ the set of sub-normalized states on $A$, i.e., the set of operators $\rho^A \in \mathcal{P}(A)$ that are positive semi-definite, denoted $\rho \geq 0$, and have trace at most one. The set of normalized states is denoted by $\mathcal{D}(A)$, and $\rho^A \in \mathcal{D}(A)$ is a pure state if it has rank one with $\rho^A = |\rho\rangle \langle \rho|_A$. Multipartite systems are described by the tensor product of the Hilbert spaces, and denoted by $A \otimes B$. Given a multipartite state $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$, we write $\rho^A = \text{Tr}_B[\rho^{AB}]$ for the reduced state on the system $A$. For $M^A \in \mathcal{L}(A)$, we write $M^A = M^A \otimes I^B$ for the enlargement on any $A \otimes B$, where $I^B$ denotes the identity in $\mathcal{P}(B)$. Quantum channels are described by completely positive trace preserving maps from some input $\mathcal{L}(A)$ to some output $\mathcal{L}(B)$.

The max-relative entropy of $\rho \in \mathcal{D}_\leq(A)$ with respect to $\sigma \in \mathcal{P}(A)$ is defined as

$$D_{\text{max}}(\rho \| \sigma) = \inf \{ \lambda \in \mathbb{R} : 2^\lambda \sigma \geq \rho \} .$$

(2.1)

The conditional min-entropy of $A$ given $B$ for $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$ is defined as

$$H_{\text{min}}(A|B)_\rho = -\inf_{\sigma \in \mathcal{D}_\leq(B)} D_{\text{max}}(\rho^{AB} \| I^A \otimes \sigma^B) .$$

(2.2)

The conditional max-entropy of $A$ given $B$ for $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$, with purification $\rho^{ABR} \in \mathcal{D}_\leq(A \otimes B \otimes R)$ for some system $R$, is defined as

$$H_{\text{max}}(A|B)_\rho = -H_{\text{min}}(A|R)_\rho .$$

(2.3)

Note that this definition does not depend on the choice of the purification. The max-information that $B$ has about $A$ for $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$ is defined as

$$I_{\text{max}}(A : B)_\rho = \inf_{\sigma \in \mathcal{D}_\leq(B)} D_{\text{max}}(\rho^{AB} \| \rho^A \otimes \sigma^B) .$$

(2.4)
To define smooth entropy measures, an optimization over a set of nearby states is performed. The distance measure used is the purified distance, defined for $\rho, \sigma \in \mathcal{D}_\leq(A)$ as \[ P(\rho, \sigma) = \sqrt{1 - \tilde{F}_2^2(\rho, \sigma)}, \] in which the generalized fidelity is defined in terms of the fidelity as \[ \tilde{F}(\rho, \sigma) = F(\rho, \sigma) + \sqrt{(1 - \text{Tr}(\rho))(1 - \text{Tr}(\sigma))}. \] We then define an $\varepsilon$-ball around $\rho \in \mathcal{D}_\leq(A)$ as \[ \mathcal{B}_\varepsilon(\rho) = \{ \tilde{\rho} \in \mathcal{D}_\leq(A) : P(\rho, \tilde{\rho}) \leq \varepsilon \}. \] For $\varepsilon \geq 0$, the smooth conditional min-entropy of $A$ given $B$ for $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$ is then defined as \[ H_{\min}^\varepsilon(A|B)_\rho = \sup_{\tilde{\rho} \in \mathcal{B}_\varepsilon(\rho^{AB})} H_{\min}(A|B)_{\tilde{\rho}}, \] and the smooth conditional max-entropy as \[ H_{\max}^\varepsilon(A|B)_\rho = \inf_{\tilde{\rho}^{AB} \in \mathcal{B}_\varepsilon(\rho^{AB})} H_{\max}(A|B)_{\tilde{\rho}}. \] The smooth max-information that $B$ has about $A$ for $\rho^{AB} \in \mathcal{D}_\leq(A \otimes B)$ is defined as \[ I_{\max}^\varepsilon(A : B)_\rho = \inf_{\tilde{\rho}^{AB} \in \mathcal{B}_\varepsilon(\rho^{AB})} I_{\max}(A : B)_{\tilde{\rho}}. \]

### 3 Decoupling Approach to State Redistribution

We want to make use of the following observation of Oppenheim [21]: quantum state redistribution can be optimally decomposed into two applications of quantum state merging by introducing a coherent relay, and applying an ebit repackaging sub-protocol. In more details, we consider four distinct parties, each holding a register. Charlie holds register $C$, that he wants to transmit to Bob, who holds register $B$, and to do so he may use help from Alice acting as a coherent relay, who holds register $A$. The state $\rho$ in registers $ABC$ is purified by state $|\rho\rangle_{ABCR}$ with the $R$ register held by some reference party Ray. The goal is to transmit $C$ to Bob while minimizing the communication from Alice to Bob, and while keeping the overall correlation with Ray. We might also keep track of communication between Charlie and Alice, as well as of the entanglement consumption and generation between both Charlie and Alice, and Alice and Bob, but here our main focus is the communication between Alice and Bob. A key observation is that applying a single decoupling unitary at Charlie’s side suffice to generate two hypothetical state merging protocols. Firstly, the state merging protocol that directly transmits the $C$ register to $B$ while considering both the $A$ and $R$ registers as reference. In an iid asymptotic setting, this state merging protocol requires quantum communication rate of $\frac{1}{2} I(C; AR)$ and generates ebits between Charlie and Bob at
a rate $\frac{1}{2} I(C; B)$. Secondly, if we instead consider the state merging protocol that transmits the $C$ register to Alice, this requires communication of $\frac{1}{2} I(C; RB)$ qubits between Charlie and Alice, and generates $\frac{1}{2} I(C; A)$ ebits between Charlie and Alice. As Oppenheim noted, this pure state entanglement between Alice and Charlie should not be communicated to Bob. The state redistribution protocol that uses Alice as a coherent relay then runs as follows.

Charlie merges his state with Alice’s, generating $\frac{1}{2} I(C; A)$ ebits between them. Alice then replaces these ebits by some pre-shared ebits between her and Bob. This is the ebit repackaging sub-protocol, which effectively acts as a communication of $I(C; A)$ qubits between Charlie and Bob in the direct merging protocol. Alice then transmits the remaining qubits required to complete the direct merging protocol between Charlie and Bob. A communication of

$$\frac{1}{2} I(C; AR) - \frac{1}{2} I(C; A) = \frac{1}{2} I(C; R|B)$$

is required to achieve this, which is asymptotically optimal [1.1]. We formalize this idea below while using it in a one-shot setting and expressing the relevant bounds in terms of smooth conditional entropies.

Following the decoupling approach to quantum information theory [17, 15, 16], quantum state merging is conveniently understood in terms of decoupling theorems. Here we first restate the central decoupling theorem of [6] in terms of smooth conditional min-entropy.

**Theorem 1** [6, Theorem III.1] For $\varepsilon > 0$, $\rho^{AR} \in D_{\leq} (A \otimes R)$, and any decomposition $A = A_1 \otimes A_2$, if

$$\log |A_1| \leq \frac{1}{2} \log |A| + \frac{1}{2} H_{\min}(A|R)_\rho - \log \frac{1}{\varepsilon},$$

then

$$\int_{U(A)} \left\| Tr_{A_2} \left[ U^{A \rightarrow A_1 A_2} (\rho^{AR}) \right] - \pi^{A_1} \otimes \rho^R \right\|_1 dU \leq \varepsilon,$$

where $dU$ is the Haar measure over the unitaries on system $A$, normalized to $\int dU = 1$, and $\pi^{A_1}$ is the completely mixed state on $A_1$.

For our purpose we need the following bi-decoupling result in terms of smooth conditional entropies, a direct generalization of Theorem [11].

**Corollary 1** For any $\varepsilon_1, \varepsilon_2 > 0$, $\rho_1^{CR_1} \in D_{\leq} (C \otimes R_1)$, $\rho_2^{CR_2} \in D(C \otimes R_2)$ and any decomposition $C = C_1 \otimes C_2 \otimes C_3$, if

$$\log |C_1| \leq \frac{1}{2} \log |C| + \frac{1}{2} H_{\min}(C|R_1)_{\rho_1} - \log \frac{1}{\varepsilon_1},$$

$$\log |C_2| \leq \frac{1}{2} \log |C| + \frac{1}{2} H_{\min}(C|R_2)_{\rho_2} - \log \frac{1}{\varepsilon_2},$$

\[\text{A similar bi-decoupling result appears in [31], with bounds in terms of register dimensions instead of smooth conditional entropies. It would be possible to apply ideas similar to theirs to obtain a different coding theorem achieving the same achievability bound [1.5] for one-shot quantum state redistribution.}\]
then there exists a unitary $U^{C\rightarrow C_1C_2C_3}$ such that
\[ \| \text{Tr}_{C_2C_3} [U(\rho_1^{CR_1})] - \pi^{C_1} \otimes \rho_1^{R_1} \|_1 \leq 3\varepsilon_1 \quad \text{and} \quad \| \text{Tr}_{C_1C_3} [U(\rho_2^{CR_2})] - \pi^{C_2} \otimes \rho_2^{R_2} \|_1 \leq 3\varepsilon_2 . \] (3.6)

**Proof.** By Markov’s inequality, if the condition on $|C_1|, |C_2|$ are satisfied, then Theorem 1 says that the probability over the Haar measure on $U(C)$ that $\| \text{Tr}_{C_2C_3}(U(\rho_1^{CR_1}) - \pi^{C_1} \otimes \rho_1^{R_1}) \| \geq 3\varepsilon_1$ is at most $\frac{1}{3}$, and similarly for $\| \text{Tr}_{C_1C_3}(U(\rho_2^{CR_2}) - \pi^{C_2} \otimes \rho_2^{R_2}) \| \geq 3\varepsilon_2$, so by the union bound there is at least probability $\frac{1}{3}$ that none of these is satisfied, and then the condition of the corollary are satisfied for all corresponding $U$’s. ■

## 4 Achievability Bounds

We now state formally the definition of one-shot quantum state redistribution. Let $\rho_{ABC}$ be the joint initial state of Alice and Bob’s systems, where $AC$ is with Alice and $B$ is with Bob. We can view this state as part of a larger pure state $|\rho\rangle^{ABCR}$ that includes a reference system $R$. In this picture quantum state redistribution means that Alice can send the $C$-part of $\rho_{ABC}$ to Bob’s side without altering the joint state. We consider a particular setting where we have free entanglement assistance between Alice and Bob, and the goal is to minimize the number of qubits communicated from Alice to Bob in order to achieve the state transfer.

**Definition 1 (One-Shot Quantum State Redistribution)** Let $\rho_{ABC} \in \mathcal{D}_\leq (A \otimes B \otimes C)$, and let $T_{A}^{in}T_{B}^{in}, T_{A}^{out}T_{B}^{out}$ be additional systems. A ctn map $\Pi : ACT_{A}^{in} \otimes BT_{B}^{in} \rightarrow AT_{A}^{out} \otimes C'BT_{B}^{out}$ is called quantum state redistribution of $\rho_{ABC}$ with error $\varepsilon \geq 0$, if it consists of local operations and sending $q(\Pi)$ qubits with respect to the bipartition $ACT_{A}^{in} \rightarrow AT_{A}^{out}$ vs. $BT_{B}^{in} \rightarrow C'BT_{B}^{out}$, and
\[ P\left( \left( \Pi^{ACT_{A}^{in}BT_{B}^{in} \rightarrow AT_{A}^{out}C'BT_{B}^{out}} \rho_{ABC}^{CR} \right), \Phi_{1}^{T_{A}^{in}T_{B}^{in}} \otimes \rho_{ABCR}^{CR}, \Phi_{2}^{T_{A}^{in}T_{B}^{out}} \otimes \rho_{ABC}^{CR} \right) \leq \varepsilon , \] (4.1)
where $\rho_{ABC}^{CR} = (I^{C\rightarrow C'} \otimes I^{\{ABR\}})\rho_{ABCR}$ for a purification $\rho_{ABCR}^{CR}$ of $\rho_{ABC}$, and $\Phi_{1}, \Phi_{2}$ are arbitrary states on $T_{A}^{in}T_{B}^{in}$ and $T_{A}^{out}T_{B}^{out}$, respectively. The number $q$ is called quantum communication cost of the protocol $\Pi$.

We obtain the following direct coding theorem for one-shot quantum state redistribution.

**Theorem 2** Let $\varepsilon_1, \varepsilon_2 \geq 0, \varepsilon_3, \varepsilon_4 > 0$, and $\rho_{ABC} \in \mathcal{D}_\leq (A \otimes B \otimes C)$ purified by $\rho_{ABCR}$ for some register $R$. Then, there exists a quantum state redistribution $\Pi$ of $\rho_{ABC}$ with error $(4\varepsilon_1 + 2\varepsilon_2 + 2\sqrt{3\varepsilon_3 + \sqrt{3\varepsilon_4}})$ and quantum communication cost $q(\Pi)$ satisfying
\[ q(\Pi) \leq \frac{1}{2}H_{\max}^{C}(C\mid B)_\rho - \frac{1}{2}H_{\min}^{C}(C\mid BR)_\rho + \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 2 . \] (4.2)

Moreover, $\Pi$ only uses EPR states as pre-shared entanglement and also generates EPR pairs. The net entanglement consumption cost $e(\Pi)$ satisfies
\[ e(\Pi) \leq \frac{1}{2}H_{\max}^{C}(C\mid B)_\rho + \frac{1}{2}H_{\min}^{C}(C\mid BR)_\rho - \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 1 . \] (4.3)
Proof. We first prove the theorem for the special case \( \varepsilon_1 = \varepsilon_2 = 0 \). In Corollary 1 we take \( R_1 = BR, R_2 = AR, \rho_1 = \rho^{BR}, \rho_2 = \rho^{CAR} \),

\[
\log |C_1| = \left[ \frac{1}{2} \log |C| + \frac{1}{2} H_{\min}(C|BR)_\rho - \log \frac{1}{\varepsilon_3} \right], \quad (4.4)
\]

\[
\log |C_2| = \left[ \frac{1}{2} \log |C| + \frac{1}{2} H_{\min}(C|AR)_\rho - \log \frac{1}{\varepsilon_4} \right], \quad (4.5)
\]

and then there exists a unitary \( U^{C \rightarrow C_1C_2C_3} \) satisfying

\[
\| \text{Tr}_{C_2C_3} \left[ U\left( \rho^{CBR} \right) \right] - \pi_{C_1} \otimes \rho^{BR} \|_1 \leq 3\varepsilon_3 \quad \text{and} \quad \| \text{Tr}_{C_1C_3} \left[ U\left( \rho^{CAR} \right) \right] - \pi_{C_2} \otimes \rho^{AR} \|_1 \leq 3\varepsilon_4. \quad (4.6)
\]

We transform these in purified distance bounds using a generalized Fuchs-van der Graaf inequality:

\[
P\left( \text{Tr}_{C_2C_3} \left[ U\left( \rho^{CBR} \right) \right], \pi_{C_1} \otimes \rho^{BR} \right) \leq \sqrt{3\varepsilon_3}, \quad (4.7)
\]

\[
P\left( \text{Tr}_{C_1C_3} \left[ U\left( \rho^{CAR} \right) \right], \pi_{C_2} \otimes \rho^{AR} \right) \leq \sqrt{3\varepsilon_4}. \quad (4.8)
\]

Let \( A', A'' \) be isomorphic to \( A \), \( B''' \) be isomorphic to \( B \), \( C', C'' \) be isomorphic to \( C \), and \( C_2', C_3'' \) be isomorphic to \( C_2, C_3 \), respectively. Then, Uhlmann’s theorem tells us that there exist partial isometries

\[
V_{1}^{C_2C_3A \rightarrow A_1A'C'} \quad \text{and} \quad V_{2}^{C_1C_3B \rightarrow B_2B'''C'''}
\]

satisfying

\[
P\left( V_{1}U\left( \rho^{ABCR} \right), |\phi_1\rangle\langle \phi_1| A_1C_1 \otimes I^{AC \rightarrow A'C'}(\rho^{ABCR}) \right) = P\left( \text{Tr}_{C_2C_3} \left[ U\left( \rho^{CBR} \right) \right], \pi_{C_1} \otimes \rho^{BR} \right) \]

\[
P\left( V_{2}U\left( \rho^{ABCR} \right), |\phi_2\rangle\langle \phi_2| B_2C_2 \otimes I^{BC \rightarrow B'''C'''}(\rho^{ABCR}) \right) = P\left( \text{Tr}_{C_1C_3} \left[ U\left( \rho^{CAR} \right) \right], \pi_{C_2} \otimes \rho^{AR} \right). \quad (4.10)
\]

Consider the unitary extension

\[
\tilde{V}_1^{D_0C_2C_3A \rightarrow D_1A_1A'C'} \quad \text{with} \quad \tilde{V}_1U\left( \rho \otimes |0\rangle\langle 0|^{D_0} \right) = V_{1}U\left( \rho \otimes |0\rangle\langle 0|^{D_1} \right) \quad (4.12)
\]

as well as

\[
\tilde{V}_2^{D_2C_1C_3B \rightarrow D_3B_2B'''C'''} \quad \text{with} \quad \tilde{V}_2U\left( \rho \otimes |0\rangle\langle 0|^{D_2} \right) = V_{2}U\left( \rho \otimes |0\rangle\langle 0|^{D_3} \right) \quad (4.13)
\]

for appropriate registers \( D_0, D_1, D_2, D_3 \). Let \( T_A, T_B \) be isomorphic to \( A_1, C_1 \), respectively, and \( D_0' \) be isomorphic to \( D_0 \). Also denote by

\[
\tilde{V}_1^{D_0'C_2'C_3''A'' \rightarrow D_1T_AT_A'A'C'} \quad \text{and} \quad \tilde{V}_2^{D_2'T_BC_3'B \rightarrow D_3B_2B'''C'''}
\]

a version of \( \tilde{V}_1 \) that maps registers \( D_0'C_2'C_3''A'' \) into registers \( D_1T_AT_A'A'C' \), and a version of \( \tilde{V}_2 \) that maps registers \( D_2'T_BC_3'B \) into registers \( D_3B_2B'''C''' \), respectively. We can now define our one-shot state redistribution protocol \( \Pi \) (also see Figure 1):
Figure 1: One-shot protocol for quantum state redistribution from the ebit repackaging sub-protocol. There are four distinct parties Alice, Bob, Charlie, and Ray each holding their register $ABCR$ of the overall pure state $|\rho_{ABCR}\rangle$, respectively. The goal is to transmit $C$ to Bob while minimizing the communication from Alice to Bob and keeping the overall correlation with Ray. The decoupling unitary $U$ at Charlie’s side generates two hypothetical state merging protocols: one that directly transmits the $C$ register to Bob (with decoding isometry $V_2$, while considering the $A$ and $R$ registers as the reference, and one that transmits the $C$ register to Alice while considering the $B$ and $R$ as the reference (with decoding isometry $V_1$). The state redistribution protocol that uses Alice as a coherent relay then runs as follows. Charlie first merges his state with Alice’s, generating ebits between them. Alice then replaces these ebits by some pre-shared ebits between her and Bob: the ebit repackaging sub-protocol. Finally, Alice transmits the remaining qubits required to complete the direct merging protocol between Charlie and Bob.
Protocol II for input $\rho^{ABCR}$ using ebits $\phi^{T_AT_B}_1$

1. Charlie applies $U$ on register $C$, keeps register $C_1$, and transmits the $C_2, C_3$ registers to Alice.

2. Alice initializes $D_0$, applies $\tilde{V}_1$ on $D_0C_2C_3A$, obtains registers $D_1A_1A’C’$, and then uses $T_A$ instead of $A_1$ along with $D_1A’C’$ to apply $\tilde{V}_1^\dagger$, obtains registers $D_0’A''C''_2C_3’’$, and discard $D_0’$.

3. Alice transmits the $C'_3$ register to Bob.

4. Bob initializes $D_2$, applies $\tilde{V}_2$ on $D_2T_BC'_3’’B$, obtains registers $D_3B_2B''_3’’C’’$, and discard $D_3$.

- The $B''_3, C''_3$ output registers held by Bob correspond to the $B, C$ input registers, respectively, while the $A''_3$ output register held by Alice corresponds to the $A$ input register. Together with the untouched reference register $R$, these should be close to $\rho^{ABCR}$.

- The $A_1C_1$ registers should be close to the maximally entangled state $|\phi_1\rangle^A_1C_1 = I^{T_AT_B \rightarrow A_1C_1} |\phi_1\rangle^{T_AT_B}$ shared between Alice and Charlie, while the $C''_2’’B_2$ registers should be close to the maximally entangled state $|\phi_2\rangle^{C''_2’’B_2}$ shared between Alice and Bob, with Alice holding the $C''_2$ share.

Note that Charlie only communicates with Alice, and the only register effectively transmitted between Alice and Bob is the $C''_3$ register, which is of the same size as the $C_3$ register. We then have the following bound on the communication:

$$q = \log |C_3| = \log |C| - \log |C_2| - \log |C_1|$$

$$\leq -\frac{1}{2} H_{\text{min}}(C|AR)_\rho - \frac{1}{2} H_{\text{min}}(C|BR)_\rho + \log \frac{1}{\varepsilon_4} + \log \frac{1}{\varepsilon_3} + 2$$

$$= \frac{1}{2} H_{\text{max}}(C|B)_\rho - \frac{1}{2} H_{\text{min}}(C|BR)_\rho + \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 2.$$  \hspace{1cm} (4.17)
\[
\frac{1}{2} H_{\text{min}}(C|AR)_{\rho} - \log \frac{1}{\epsilon_4} - 1. \]
The net entanglement cost \( e \) is then bounded by
\[
e = \log |C_1| - \log |C_2| \quad (4.18)
\]
\[
\leq \frac{1}{2} H_{\text{min}}(C|BR)_{\rho} - \log \frac{1}{\epsilon_3} - \frac{1}{2} H_{\text{min}}(C|AR)_{\rho} + \log \frac{1}{\epsilon_4} + 1 \quad (4.19)
\]
\[
= \frac{1}{2} H_{\text{max}}(C|B)_{\rho} + \frac{1}{2} H_{\text{min}}(C|BR)_{\rho} - \log \frac{1}{\epsilon_3} + \log \frac{1}{\epsilon_4} + 1 . \quad (4.20)
\]

It is left to verify that the final state is close enough to \( \rho^{ABCR} \). We prove a stronger result, that the global final state is close to \( \rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2'B_2} \). This is the criteria normally used in EPR-based state-redistribution. Properties of the purified distance that we use are proved in \([26, 24]\). We first use the triangle inequality to obtain the following 3 terms:

\[
P(\text{Tr}_{D_0D_3} [\hat{V}_2 \hat{V}_1^{-1} \hat{V}_1 U (\rho^{ABCR} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_0} \otimes |0\rangle\langle 0|_{D_2})],
I^{ABC \rightarrow A'^B'C''m'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2'B_2})
) \leq P(\text{Tr}_{D_0D_3} [\hat{V}_2 \hat{V}_1^{-1} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})],
I^{ABC \rightarrow A'^B'C''m'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2'B_2})
) + P(\text{Tr}_{D_0D_3} [\hat{V}_2 \hat{V}_1^{-1} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})],
I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})
) + P(\text{Tr}_{D_0D_3} [\hat{V}_2 \hat{V}_1^{-1} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})],
I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})
) ) . \quad (4.21)
\]

To bound the first term, we have

\[
P(\text{Tr}_{D_0D_3} [\hat{V}_2 \hat{V}_1^{-1} \hat{V}_1 U (\rho^{ABCR} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_0} \otimes |0\rangle\langle 0|_{D_2})],
I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})
) \leq P(\hat{V}_1 U (\rho^{ABCR} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_0} \otimes |0\rangle\langle 0|_{D_2}),
I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_1T_B} \otimes |0\rangle\langle 0|_{D_1} \otimes |0\rangle\langle 0|_{D_2})
) ) . \quad (4.22)
\]

The first inequality is by monotonicity of the purified distance, the first equality is because appending an uncorrelated system does not change the distance, and also by definition of the unitary extension of \( V_1 \), and finally the last inequality is again because uncorrelated systems do not change the distance, and also by combining \([4.7] \) and \([4.10] \). For the second term,
we have

$$P\left( \text{Tr}_{D_0'}D_3' \left[ \hat{V}_2 \hat{V}_1^{-1} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_1} \otimes |0\rangle_{D_2}) \right] \right)$$

$$\leq P\left( \hat{V}_2 \hat{V}_1^{-1} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_1} \otimes |0\rangle_{D_2} \right),$$

$$I^{D_0 \rightarrow D_0'}SWAP_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C''_3A_1U} (\rho^{ABCR} \otimes \phi^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_0} \otimes |0\rangle_{D_2})$$

$$= P\left( SWAP_{A_1C_1 \leftrightarrow T_AT_B} I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_1} \otimes |0\rangle_{D_2} \right),$$

$$SWAP_{A_1C_1 \leftrightarrow T_AT_B} \hat{V}_1 SWAP_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C''_3A_1U} (\rho^{ABCR} \otimes \phi^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_0} \otimes |0\rangle_{D_2})$$

$$= P\left( I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_1^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_1} \otimes |0\rangle_{D_2} \right),$$

$$\hat{V}_1 U (\rho^{ABCR} \otimes \phi^{T_AT_B} \otimes |0\rangle_0 |0\rangle_{D_0} \otimes |0\rangle_{D_2})$$

$$= P\left( I^{AC \rightarrow A'C'} (\rho^{ABCR} \otimes \phi_1^{A_1C_1} \otimes |0\rangle_0 |0\rangle_{D_1} \right), \hat{V}_1 U (\rho^{ABCR} \otimes |0\rangle_0 |0\rangle_{D_1})$$

$$\leq \sqrt{3\varepsilon_3}.$$  \hspace{1cm} (4.25)

The first inequality is because we can append and trace out uncorrelated register $D_0'$ to the second state without changing it, and then also by monotonicity of the purified distance, the first equality is by unitary invariance, the second is because $SWAP_{A_1C_1 \leftrightarrow T_AT_B}$ leaves the first state invariant and also because

$$SWAP_{A_1C_1 \leftrightarrow T_AT_B} V_1^{D_0'C_2'C_3'} A'' \rightarrow D_1'A'C'' SWAP_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C''_3A_1U}$$

$$= I^{T_AT_B C_1} V_1^{D_0'C_2'C_3A \rightarrow D_1'A_1A'C''} SWAP_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C''_3A_1U}$$

$$\leq \sqrt{3\varepsilon_3}.$$  \hspace{1cm} (4.30)

The next is by definition of the unitary extension of $V_1$ and the fact that appending uncorrelated systems do not change the distance, and finally the last inequality is again because uncorrelated systems do not change the distance, and also by combining (4.7) and (4.10).
For the third term, we have
\[
P\left( \text{Tr}_{D_3} \hat{V}_2 \text{SWAP}_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C'''_3A_1} U \left( \rho_{ABCR} \otimes \phi_1^{TA_T} \otimes |0\rangle \langle 0|_D^A \right), \\
I^{ABC \rightarrow A''B''C''} \left( \rho_{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2B_2} \otimes |0\rangle \langle 0|_D^3 \right) \right) 
\leq P\left( \hat{V}_2 \text{SWAP}_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C'''_3A_1} U \left( \rho_{ABCR} \otimes \phi_1^{TA_T} \otimes |0\rangle \langle 0|_D^2 \right), \\
I^{ABC \rightarrow A''B''C''} \left( \rho_{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2B_2} \otimes |0\rangle \langle 0|_D^3 \right) \right) \tag{4.31} 
\]
\[
= P\left( I^A^''C_2'' \rightarrow AC_2 \hat{V}_2 \text{SWAP}_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C'''_3A_1} U \left( \rho_{ABCR} \otimes \phi_1^{TA_T} \otimes |0\rangle \langle 0|_D^2 \right), \\
I^{ABC \rightarrow A''B''C''} \left( \rho_{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2B_2} \otimes |0\rangle \langle 0|_D^3 \right) \right) \tag{4.32} 
\]
\[
= P\left( I^{T_A T_B \rightarrow A_1 C_1} \hat{V}_2 U \left( \rho_{ABCR} \otimes \phi_1^{TA_T} \otimes |0\rangle \langle 0|_D^3 \right), \\
I^{BC \rightarrow B''C''} \left( \rho_{ABCR} \otimes \phi_1^{A_1C_1} \otimes \phi_2^{C_2B_2} \otimes |0\rangle \langle 0|_D^3 \right) \right) \tag{4.33} 
\]
\[
\leq \sqrt{3\varepsilon_4}. \tag{4.34} 
\]

The first inequality is because we can append and trace out uncorrelated register \( D_3 \) to the second state without changing it, and also by monotonicity of the purified distance, the first equality is by unitary invariance, the second is because
\[
I^{A''C_2'' \rightarrow AC_2 \hat{V}_2 D_2 T_B C_2'' B \rightarrow D_3 B_2 B''C''} \text{SWAP}_{C_1 \leftrightarrow T_B} I^{AC_2C_3T_A \rightarrow A''C''_2C'''_3A_1} 
\]
\[
= I^{AC_2} I^{T_A T_B \rightarrow A_1 C_1} \hat{V}_2 D_2 C_1 C_3 B \rightarrow D_3 B_2 B''C''} \tag{4.36} 
\]
the third is because appending an uncorrelated system does not change the distance and by definition of the unitary extension of \( V_2 \), and finally the last inequality is again because appending uncorrelated systems does not change the distance, and also by combining (4.8) and (4.11). Putting these three bounds together, we get the stated bound for \( \varepsilon_1, \varepsilon_2 = 0 \), and this completes the proof for this case.

We can now prove the smooth entropy version of the theorem by extending the above argument to the states achieving the extremum in the smooth entropies. Let \( \omega^{ABCR}_1 \in S_{\leq}^0(\mathcal{H}_{ABCR}) \) be such that \( P(\omega_1, \rho) \leq \varepsilon_1 \) and \( H^{\varepsilon_1}_\min(C|BR) = H^{\min}_\min(C|BR)_{\omega_1} \). Similarly, let \( \omega^{ABCR}_2 \in S_{\leq}(\mathcal{H}_{ABCR}) \) be such that \( P(\omega_2, \rho) \leq \varepsilon_2 \) and \( H^{\varepsilon_2}_\max(C|B) = H^{\max}_\max(C|B)_{\omega_2} \), and consider a purification \( \omega^{ABCRS_2}_2 \). In Corollary 1 we take \( R_2 = BR, R_2 = ARS_2, \rho_1 = \omega^{C|BR}_1, \rho_2 = \omega^{C|ARS_2}_2, \)
\[
\log |C_1| = \left[ \frac{1}{2} \log |C| + \frac{1}{2} H^{\varepsilon_1}_\min(C|BR)_{\omega_1} - \log \frac{1}{\varepsilon_3} \right], \tag{4.37} 
\]
\[
\log |C_2| = \left[ \frac{1}{2} \log |C| + \frac{1}{2} H^{\varepsilon_2}_\min(C|ARS_2)_{\omega_2} - \log \frac{1}{\varepsilon_4} \right], \tag{4.38} 
\]

12
and then there exists a unitary $U^{C\to C_1C_2C_3}$ satisfying

$$\| \text{Tr}_{C_2C_3} \left[ U \left( \omega_1^{CBR} \right) \right] - \pi^{C_1} \otimes \omega_1^{BR} \|_1 \leq 3\varepsilon_3$$

(4.39)

$$\| \text{Tr}_{C_1C_3} \left[ U \left( \omega_2^{CARS_2} \right) \right] - \pi^{C_2} \otimes \omega_2^{ARS_2} \|_1 \leq 3\varepsilon_4 .$$

(4.40)

Transforming these in purified distance bounds, we get

$$P \left( \text{Tr}_{C_2C_3} \left[ U \left( \omega_1^{CBR} \right) \right], \pi^{C_1} \otimes \omega_1^{BR} \right) \leq \sqrt{3\varepsilon_3}$$

(4.41)

$$P \left( \text{Tr}_{C_1C_3} \left[ U \left( \omega_2^{CAR} \right) \right], \pi^{C_2} \otimes \omega_2^{AR} \right) \leq \sqrt{3\varepsilon_4} ,$$

(4.42)

in which we also used monotonicity of the purified distance under partial trace of $S_2$. Since

$$P(\omega_1^{ABCR}, \rho^{ABCR}) \leq \varepsilon_1 \quad \text{and} \quad P(\omega_2^{ABCR}, \rho^{ABCR}) \leq \varepsilon_2 ,$$

(4.43)

the triangle inequality along with monotonicity of the purified distance and the fact that appending uncorrelated systems does not increase distance imply the bounds

$$P \left( \text{Tr}_{C_2C_3} \left[ U \left( \rho^{CBR} \right) \right], \pi^{C_1} \otimes \rho^{BR} \right) \leq \sqrt{3\varepsilon_3} + 2\varepsilon_1$$

(4.44)

$$P \left( \text{Tr}_{C_1C_3} \left[ U \left( \rho^{CAR} \right) \right], \pi^{C_2} \otimes \rho^{AR} \right) \leq \sqrt{3\varepsilon_4} + 2\varepsilon_2 .$$

(4.45)

Considering systems $A', A'', B'''', C', C''', C''_2, C''_3, T_A, T_B, D_0, D_1, D_2, D_3, D'_0$ as above, Uhlmann’s theorem tells us that there exist partial isometries

$$V_1^{C_2C_3A\to A_1A'C'} \quad \text{and} \quad V_2^{C_1C_3B\to B_2B'''C'''}$$

(4.46)

satisfying

$$P \left( V_1 U(\rho^{ABCR}), |\phi_1\rangle |\phi_1\rangle^{A_1C_1} \otimes I^{AC\to A'C'}(\rho^{ABCR}) \right) = P \left( \text{Tr}_{C_2C_3} \left[ U \left( \rho^{CBR} \right) \right], \pi^{C_1} \otimes \rho^{BR} \right)$$

(4.47)

$$P \left( V_2 U(\rho^{ABCR}), |\phi_2\rangle |\phi_2\rangle^{BC_2} \otimes I^{BC\to B'''C'''}(\rho^{ABCR}) \right) = P \left( \text{Tr}_{C_1C_3} \left[ U \left( \rho^{CAR} \right) \right], \pi^{C_2} \otimes \rho^{AR} \right) .$$

(4.48)

Also consider unitary extensions

$$\hat{V}_1^{D_0C_2C_3A\to D_1A_1A'C'} \quad \text{and} \quad \hat{V}_2^{D_2C_1C_3B\to D_3B_2B'''C'''}$$

(4.49)

as well as

$$\hat{V}_1^{D'_0C''_2C''_3A''\to D_1T_AA'C'} \quad \text{and} \quad \hat{V}_2^{D_2T_BC''_2B\to D_3B_2B'''C'''} ,$$

(4.50)

the versions of $\hat{V}_1, \hat{V}_2$ acting on the corresponding registers, as in the $\varepsilon_1, \varepsilon_2 = 0$ case. We can then take the smooth version of our one-shot state redistribution protocol $P$ to be formally
defined as the non-smooth version above, but using these \( U, \tilde{V}_1, \hat{V}_1, \hat{V}_2 \) instead. We then have the following bound on the communication:

\[
q = \log |C_3| = \log |C| - \log |C_2| - \log |C_1| \leq -\frac{1}{2} H_{\min}(C|ARS_2)_{\omega_2} - \frac{1}{2} H_{\min}(C|BR)_{\omega_1} + \log \frac{1}{\varepsilon_4} + \log \frac{1}{\varepsilon_3} + 2
\]

(4.51)

\[
= \frac{1}{2} H_{\max}(C|B)_{\omega_2} - \frac{1}{2} H_{\min}(C|BR)_{\omega_1} + \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 2 \quad \text{(4.52)}
\]

\[
= \frac{1}{2} H_{\max}^{\varepsilon_2}(C|B)_{\rho} - \frac{1}{2} H_{\min}^{\varepsilon_1}(C|BR)_{\rho} + \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 2 .
\]

(4.53)

Similarly, we have the following bound on the net entanglement cost \( e \):

\[
e = \log |C_1| - \log |C_2| \leq \frac{1}{2} H_{\max}^{\varepsilon_2}(C|B)_{\rho} + \frac{1}{2} H_{\min}^{\varepsilon_1}(C|BR)_{\rho} - \log \frac{1}{\varepsilon_3} + \log \frac{1}{\varepsilon_4} + 1 .
\]

(4.56)

Is left to verify that the final state is close enough to \( \rho^{ABC\tilde{R}} \). The analysis is the same as in the \( \varepsilon_1, \varepsilon_2 = 0 \) case, with the bounds (4.7) and (4.8) replaced by (4.44) and (4.45), yielding the desired bound

\[
P\left( \text{Tr}_{D_0D_3} \left[ \tilde{V}_2 \tilde{V}_1 U \left( \rho^{ABC\tilde{R}} \otimes \phi_1^{TA} \otimes |0\rangle\langle 0|_{D_0} \otimes |0\rangle\langle 0|_{D_2} \right) \right] \right)
\leq 4\varepsilon_1 + 2\varepsilon_2 + 2\sqrt{3\varepsilon_3} + \sqrt{3\varepsilon_4} .
\]

(4.57)

Note however that the above bound can not be tight in general (at least if we allow arbitrary shared entanglement). This can be seen by considering the situation where the \( B \) register is trivial, which corresponds to state splitting, and for which it is known [6] that we can succeed with communication \( I^{\varepsilon}_{\max}(C;R)_{\rho} \) using entanglement embezzling states. This can be much smaller than the bound we provide for some states \( \rho \). We provide an alternate protocol, using entanglement embezzling states rather than standard maximally entangled states, which achieves a communication rate that is upper bounded by the smooth max-information, up to small additive terms, in the case that either the \( A \) or the \( B \) register is trivial, and so this protocol has optimal communication for the special cases of state merging and state splitting.

The idea for the protocol with embezzling states is borrowed from [6], and is the following. At the outset of the protocol, before applying the above protocol as a sub-protocol, we first perform a coherent projective measurement in the eigenbasis of the \( C \) system, and discard the portion with eigenvalues smaller than \( |C|^2 \). We then coherently apply the above EPR-based protocol on each branch, with the state in branch \( i \) denoted \( \rho_i \), using an entanglement embezzling state between Charlie and Alice, and another between Alice and Bob, to provide the necessary EPR pairs, as well as to absorb any EPR pair created, up to small error. Different amount of EPR pairs are generated and consumed on each branch, hence the need for entanglement embezzling states. We also transmit the register containing the coherent
measurement outcomes, to allow to undo these. This procedure then flattens the eigenvalue spectra on the $C$ system, hence the min- and max-entropies $H_{\text{min}}^\varepsilon(C)_{\rho_i}, H_{\text{max}}^\varepsilon(C)_{\rho_i}$ are both equal to the rank of $\rho_i^C$, up to a small error. This allows us to replace the max-entropy term by a min entropy term when the $B$ register is trivial, and similarly when $A$ is trivial, and in such a case we can use the lemmas given in [6] to relate this to smooth max-information, and obtain a provably optimal rate. See [6] for a formal definition of the $\rho_i$'s. In general, the communication grows as

$$q(\Pi) \geq \frac{1}{2} \max_i \left( H_{\text{max}}^\varepsilon(C|B)_{\rho_i} - H_{\text{min}}^\varepsilon(C|BR)_{\rho_i} \right)$$

(4.58)

up to small additive terms. This is however not optimal in general, and it is still unclear whether this can be of any help for obtaining tight bounds for state redistribution (cf. Section 6). An approach that might hold some promise could be to allow for interaction in the state redistribution protocol. For example, in a two-message protocol in which Bob speaks first, this would then allow Bob to also do some preprocessing similar to what Alice does here, and possibly allow for improved flattening in the general case.

5 Converse Bounds

We also provide lower bounds on the amount of communication required for one-shot state redistribution. They do not match the upper bound given in the direct coding theorem in general, but in the asymptotic regime they also simplifies to the conditional mutual information $I(C;R|B)_{\rho}$.

Proposition 1 Let $\varepsilon_1, \varepsilon_2 \geq 0$ and $\rho \in D_\omega(A \otimes B \otimes C)$ purified by $\rho^{ABCR}$ for some register $R$. Then, the quantum communication cost $q(\Pi)$ of every quantum state redistribution $\Pi$ of $\rho_{ABC}$ with error $\varepsilon_1$ is lower bounded by

$$q(\Pi) \geq \frac{1}{2} I_{\text{max}}^{\varepsilon_1+\varepsilon_2}(R; BC)_{\rho} - \frac{1}{2} I_{\text{max}}^{\varepsilon_2}(R; B)_{\rho}$$

(5.1)

$$q(\Pi) \geq \frac{1}{2} H_{\text{min}}^{\varepsilon_2}(R|B)_{\rho} - \frac{1}{2} H_{\text{min}}^{\varepsilon_1+\varepsilon_2}(R|BC)_{\rho}$$

(5.2)

$$q(\Pi) \geq \frac{1}{2} H_{\text{max}}^{\varepsilon_1+\varepsilon_2}(R|B)_{\rho} - \frac{1}{2} H_{\text{max}}^{\varepsilon_2}(R|BC)_{\rho} ,$$

(5.3)

and the same bounds hold for $B$ replaced with $A$.

Note that the first bound is optimal in the case of a trivial $B$ register, for state splitting, while the corresponding bound with $A$ replacing $B$ is optimal in the case of a trivial $A$ register, for state merging. Also note that, in contrast to the direct coding bound, the time-reversal symmetry between the $A, B$ systems is not apparent here. Finally, note that these bound holds irrespective of the kind of entanglement used.

5 Using the pre-processing from [6] would only amount to a sub-linear communication cost from Bob to Alice, and thus vanishing back communication cost in the iid asymptotic setting.
Proof. (Proposition 1) Similar to the proof of the optimal bound on state splitting in [6], we
look at the correlations between Bob and Ray. To be able to use Lemma B.9 of [6], we look
at the max-information that Bob has about Ray at the end of any protocol for quantum state
redistribution. A one-message protocol for state redistribution necessarily has the following
structure: local operation on Alice’s side, followed by communication from Alice to Bob, and
then local operations on Bob’s side. In more details.

| General protocol \( \Pi \) for input \( \rho^{A^B C^D R} \) using entanglement \( \phi^{T_A^B T_B^D} \) |
|---|
| 1. Alice holds the \( A, C, T_A^B \) systems at the outset, and Bob the \( B, T_B^D \) systems. |
| 2. Alice applies a local operation on the \( ACT_A^B \) registers. Her registers are then \( T_A^B A'Q \). The joint state is \( \sigma^{T_A^B A'QBT_B^D R} \). |
| 3. Alice transmits the \( Q \) register to Bob. |
| 4. Bob applies a local operation on \( QBT_B^D \). His registers are then \( T_B^D B'C' \). The joint state is \( \theta^{T_A^B T_B^D A'B'C'R} \). |

- The requirement is that the \( A'B'C'R \) part is \( \varepsilon_1 \) close to \( \rho^{A'B'C'R} = I_{ABC \rightarrow A'B'C'}(\rho^{A^B C^D R}) \) in purified distance.

For the bound in terms of max-information, consider a state \( \hat{\theta}^{A'B'C'R} \in D_{\leq}(A' \otimes B' \otimes C' \otimes R) \) such that \( P(\hat{\theta}^{A'B'C'R}; \hat{\theta}^{A'B'C'R}) \leq \varepsilon_2 \) and \( I_{\max}^\varepsilon(R; B'C')_\theta = I_{\max}^\varepsilon(R; B'C')_{\hat{\theta}} \). Such a state must exist by the definition of smoothing and the properties of the purified distance. Then \( P(\rho^{A'B'C'R}; \hat{\theta}^{A'B'C'R}) \leq \varepsilon_1 + \varepsilon_2 \) by the triangle inequality since \( \theta^{A'B'C'R} \) must be \( \varepsilon_1 \) close to \( \rho^{A'B'C'R} \). We get the following chain of inequalities

\[
I_{\max}^{\varepsilon_1+\varepsilon_2}(R; BC)_\rho \leq I_{\max}(R; B'C')_{\theta} \leq I_{\max}^{\varepsilon_2}(R; QBT_B^D)_{\sigma} \leq I_{\max}^{\varepsilon_2}(R; BT_B^D)_{\sigma} + 2 \log |Q| \leq I_{\max}^{\varepsilon_2}(R; BT_B^D)_{\rho \otimes \phi} + 2 \log |Q| = I_{\max}^{\varepsilon_2}(R; B)_\rho + 2 \log |Q| ,
\]

in which the first inequality follows by definition of smooth max-information and monoton-
icty of purified distance, since \( \theta^{A'B'C'R} \) is within distance \( \varepsilon \) of \( \rho^{A'B'C'R} \), the first equality is by
the choice of \( \hat{\theta} \), the second inequality is because the max-information is monotone under local
operations, the third inequality follows by Lemma B.9 of [6], the second equality is because
local operations of Alice do not change the max-information of Bob about the reference, and
the last is because \( \phi^{T_A^B T_B^D} \) is uncorrelated to \( \rho^{A^B C^D R} \).
For the bound in term of conditional min-entropy, we similarly get, by taking an appropriate \( \hat{\theta} \) and using an unlockability property of min-entropy (Lemma 2, Appendix),

\[
H^{\varepsilon_1 + \varepsilon_2}_{\text{min}}(R|BC)_{\rho} \geq H^{\varepsilon_2}_{\text{min}}(R; BC')_{\theta} = H^{\varepsilon_2}_{\text{min}}(R; B'C')_{\theta}
\]

\[
\geq H^{\varepsilon_2}_{\text{min}}(R|QBT^in_B)_{\sigma}
\]

\[
\geq H^{\varepsilon_2}_{\text{min}}(R|BT^in_B)_{\sigma} - 2 \log |Q|
\]

\[
= H^{\varepsilon_2}_{\text{min}}(R|BT^in_B)_{\rho \otimes \phi} - 2 \log |Q|
\]

\[
= H^{\varepsilon_2}_{\text{min}}(R|B)_{\rho} - 2 \log |Q|.
\]

For the bound in term of the conditional max-entropy, we obtain the bound with the \( \mathcal{A} \) system instead of \( B \) by using the duality relation of conditional min- and max-entropy. We then get the remaining bounds by interchanging the \( \mathcal{A} \) and \( \mathcal{B} \) systems in those already proved, and by using the symmetry of state redistribution under time reversal. \( \blacksquare \)

## 6 Conclusion

We have proved that one-shot quantum state redistribution of \( \rho^{ABCR} \) up to error \( \varepsilon \) can be achieved at communication cost at most

\[
1/2 \left( H^{\varepsilon}_{\text{max}}(C|B)_{\rho} - H^{\varepsilon}_{\text{min}}(C|BR)_{\rho} \right) + O\left( \log(1/\varepsilon) \right).
\]

when free entanglement assistance is available (independently, this bound has also been derived in [12]). The structure of the protocol achieving this performs a decomposition of state redistribution into two state merging protocols. Such a decomposition was proposed in [21] in order to achieve asymptotically tight rates. Note that we could alternatively use a decomposition into a state merging and a state splitting protocol, as proposed in [31], to achieve similar bounds. An important technical ingredient for our proof is the bi-decoupling lemma that we prove as an extension of the well-known decoupling theorem [6]. A similar lemma was derived in [31], with bounds in terms of dimensions rather than conditional min-entropies. This lemma states that for two states on the same system \( C \), there exists at least one unitary on \( C \) that acts as a decoupling unitary for both states simultaneously, when parameters are appropriately chosen. Perhaps surprisingly, this idea allows us to smooth both the conditional min- and max-entropy terms appearing in our bounds, notwithstanding the fact that it is in general unknown how to simultaneously smooth marginals of overlapping quantum systems (see, e.g., [14] and references therein).

We emphasize again that our achievability bound (4.2) has already found applications. In particular, one of the authors obtained the first multi-round direct sum theorem in quantum communication complexity [27]. However, it is known from the work on one-shot state merging and splitting [6] that, for arbitrary shared entanglement, the bound (4.2) can in general not be optimal, and in fact for some states the achievable communication can be substantially lower. An interesting open problem is to obtain a tight characterization of the minimal quantum communication cost. Recent works on the Rényi generalizations of conditional mutual information in the quantum regime [7] might enable to shed some light
on this question. In particular, it would be of interest to link some version of our improved bound \((4.58)\) to a smooth version of the conditional max-information from [7],

\[ I_{\text{max}}(C; R|B)_{\rho} = D_{\text{max}}\left(\rho^{C|BR}\parallel (\rho^{BR})^{1/2}(\rho^{B})^{-1/2}\rho^{BC}(\rho^{B})^{-1/2}(\rho^{BR})^{1/2}\right). \] (6.2)

In turn this would also shine some light on the Rényi generalizations of the conditional mutual information in [7].

**Acknowledgements** We acknowledge discussions with Renato Renner and Jürg Wullschleger in connection with the preliminary results in [4]. MC was supported by a Sapere Aude grant of the Danish Council for Independent Research, an ERC Starting Grant, the CHIST-ERA project “CQC”, an SNSF Professorship, the Swiss NCCR “QSIT” and the Swiss SBFI in relation to COST action MP1006.

# A Miscellaneous Lemmas

The following bound holds on the smooth max information [6, Lemma B.9].

**Lemma 1** Let \( \varepsilon \geq 0 \) and \( \rho^{ABC} \in D_\varepsilon(A \otimes B \otimes C) \). Then, we have

\[ I_{\text{max}}^\varepsilon(A: BC)_{\rho} \leq I_{\text{max}}^\varepsilon(A: B)_{\rho} + 2 \log |C|. \] (A.1)

We also need the same type of bound for smooth conditional min-entropy.

**Lemma 2** Let \( \rho^{ABC} \in D_\varepsilon(A \otimes B \otimes C) \) and \( \varepsilon \geq 0 \). Then, we have

\[ H_{\text{min}}^\varepsilon(A|B)_{\rho} \leq H_{\text{min}}^\varepsilon(A|BC)_{\rho} + 2 \log |C|. \] (A.2)

**Proof.** Let \( \tilde{\rho}^{AB} \in B^\varepsilon(\rho^{AB}) \) and \( \sigma^B \in D_\varepsilon(B) \) such that \( H_{\text{min}}^\varepsilon(A|B)_{\rho} = -D_{\text{max}}(\tilde{\rho}^{AB}\parallel I^A \otimes \sigma^B) = -\log \lambda \). We have

\[ \lambda \cdot I^A \otimes \sigma^B \geq \tilde{\rho}^{AB} \Rightarrow \lambda \cdot I^A \otimes \sigma^B \otimes \frac{I^C}{|C|} \geq \tilde{\rho}^{AB} \otimes \frac{I^C}{|C|}. \] (A.3)

Now take \( \tilde{\rho}^{ABC} \in B^\varepsilon(\rho^{ABC}) \) and with [6, Lemma B.6], \( |C| \cdot \tilde{\rho}^{AB} \otimes I^C \geq \tilde{\rho}^{ABC} \) we get

\[ \lambda |C|^2 \cdot I^A \otimes \sigma^B \otimes \frac{I^C}{|C|} \geq \tilde{\rho}^{ABC}. \] (A.4)

Hence, we can conclude the claim

\[ H_{\text{min}}^\varepsilon(A|B)_{\rho} = -\log \lambda \leq -D_{\text{max}}(\tilde{\rho}^{ABC}\parallel I^A \otimes \sigma^B \otimes \frac{I^C}{|C|}) + 2 \log |C| \] (A.5)

\[ \leq \sup_{\tilde{\rho}^{ABC} \in B^\varepsilon(\rho^{ABC})} \sup_{\omega^{BC} \in D_\varepsilon(B \otimes C)} D_{\text{max}}(\tilde{\rho}^{ABC}\parallel I^A \otimes \omega^{BC}) + 2 \log |C| \] (A.6)

\[ = H_{\text{min}}^\varepsilon(A|BC)_{\rho} + 2 \log |C|. \] (A.7)

Note that by duality, a similar result holds for smooth conditional max-entropy. We also make use of the following variant of Uhlmann’s theorem.
Lemma 3 Let $\rho_1, \rho_2 \in \mathcal{D}_\leq(A)$ have purifications $\rho_1^{AR_1}, \rho_2^{AR_2}$. Then, there exists a partial isometry $V^{R_1 \to R_2}$ such that

$$P(\rho_1^A, \rho_2^A) = P(V(\rho_1^{AR_1}), \rho_2^{AR_2}). \quad (A.8)$$

References

[1] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information’s family tree. Proceedings of the Royal Society of London A 465, 2537-2563 (2009).

[2] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. The Quantum Reverse Shannon Theorem and Resource Tradeoffs for Simulating Quantum Channels. IEEE Transactions on Information Theory 60, 2926-2959 (2014).

[3] Mario Berta. Single-shot quantum state merging. Master’s thesis, ETH Zurich

[4] Mario Berta, Renato Renner, Andreas Winter, and Jürg Wullschleger. One-Shot Source Coding. Unpublished notes (2009).

[5] Mario Berta, and Matthias Christandl. One-Shot Quantum State Redistribution. Unpublished notes (2010).

[6] Mario Berta, Matthias Christandl, and Renato Renner. The Quantum Reverse Shannon Theorem based on One-Shot Information Theory. Communications in Mathematical Physics 306, 579 (2011).

[7] Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. Renyi generalizations of the conditional quantum mutual information. arXiv:quant-ph/1403.6102 (2014).

[8] Francesco Buscemi, Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. IEEE Transactions on Information Theory 56, 1447-1460 (2010).

[9] Nikola Ciganovi, Normand J. Beaudry, and Renato Renner. Smooth Max-Information as One-Shot Generalization for Mutual Information. IEEE Transactions on Information Theory 60, 1573-1581 (2014).

[10] Wim van Dam, and Patrick Hayden. Universal entanglement transformations without communication. Physical Review A 67, 060302(R) (2003).

[11] Nilanjana Datta, and Min-Hsiu Hsieh. The apex of the family tree of protocols: optimal rates and resource inequalities. New Journal of Physics 13, 093042 (2011).

[12] Nilanjana Datta, Min-Hsiu Hsieh, and Jonathan Oppenheim. Optimality of one-shot state redistribution. Stated as in preparation in [11]. To simultaneously appear on the arXiv as the current work.

[13] Igor Devetak, and Jon Yard. Exact cost of redistributing multipartite quantum states. Physical Review Letters 100, 230501 (2008).
[14] Lukas Drescher, Omar Fawzi. *On simultaneous min-entropy smoothing*. Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, 161-165 (2013).

[15] Frédéric Dupuis *The decoupling approach to quantum information theory*. Ph.D. thesis, Université de Montréal.

[16] Frédéric Dupuis, Mario Berta, Jrg Wullschleger, Renato Renner. *One-shot decoupling*. Communications in Mathematical Physics 328, 251 (2014).

[17] P. Hayden, M. Horodecki, J. Yard, and A.Winter. *A decoupling approach to the quantum capacity*. Open Systems and Information Dynamics 15, 7-19 (2008).

[18] Michal Horodecki, Jonathan Oppenheim, Andreas Winter. *Partial quantum information*. Nature 436, 673-676 (2005).

[19] Michal Horodecki, Jonathan Oppenheim, Andreas Winter. *Quantum state merging and negative information*. Communications in Mathematical Physics 269, 107 (2007).

[20] Zhicheng Luo, and Igor Devetak. *Channel Simulation With Quantum Side Information*. IEEE Transactions on Information Theory 55, 1331-1342 (2009).

[21] Jonathan Oppenheim. *State redistribution as merging: introducing the coherent relay*. arXiv: quant-ph/0805.1065 (2008).

[22] Renato Renner *Security of Quantum Key Distribution*. Ph.D. thesis, ETH Zurich.

[23] Benjamin Schumacher. *Quantum coding* Physical Review A 51, 2738-2747 (1995).

[24] Marco Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. Ph.D. thesis, ETH Zurich.

[25] Marco Tomamichel, Roger Colbeck, Renato Renner. *A Fully Quantum Asymptotic Equipartition Property*. IEEE Transactions on Information Theory 55, 5840 - 5847 (2009).

[26] Marco Tomamichel, Roger Colbeck, Renato Renner. *Duality Between Smooth Min- and Max-Entropies* IEEE Transactions on Information Theory 56, 4674-4681 (2010).

[27] Dave Touchette. *Direct Sum Theorem for Bounded Round Quantum Communication Complexity*. To simultaneously appear on the arXiv as the current work. (2014).

[28] Dave Touchette. *Smooth Entropy Bounds on One-Shot Quantum State Redistribution*. Unpublished notes (2014).

[29] Alexander Vitanov, Frederic Dupuis, Marco Tomamichel, and Renato Renner. *Chain Rules for Smooth Min- and Max-Entropies*. IEEE Transactions on Information Theory 59, 2603-2612 (2013).

[30] Jon T. Yard, and Igor Devetak. *Optimal Quantum Source Coding With Quantum Side Information at the Encoder and Decoder*. IEEE Transactions on Information Theory 55, 5339-5351 (2009).
[31] Ming-Yong Ye, Yan-Kui Bai, and Z. D. Wang. *Quantum state redistribution based on a generalized decoupling*. Physical Review A 78, 030302(R) (2008).