An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution

Nilanjana Datta,[1, a)] Min-Hsiu Hsieh,[2, b)] and Jonathan Oppenheim[3, 4, c)]

[1)] *Statistical Laboratory, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.*

[2)] *Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

[3)] *Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom*

[4)] *Department of Computer Science and Centre for Quantum Technologies, National University of Singapore, Singapore 119615*

(Dated: Resubmitted on April 22, 2016)

State redistribution is the protocol in which, given an arbitrary tripartite quantum state, with two of the subsystems initially being with Alice and one being with Bob, the goal is for Alice to send one of her subsystems to Bob, possibly with the help of prior shared entanglement. We derive an upper bound on the second order asymptotic expansion for the quantum communication cost of achieving state redistribution with a given finite accuracy. In proving our result, we also obtain an upper bound on the quantum communication cost of this protocol in the one-shot setting, by using the protocol of coherent state merging as a primitive.

[a)] Electronic mail: n.datta@statslab.cam.ac.uk

[b)] Electronic mail: Min-Hsiu.Hsieh@uts.edu.au

[c)] Electronic mail: j.oppenheim@ucl.ac.uk

I. INTRODUCTION

State redistribution is a fundamental protocol in quantum information theory and serves as a primitive for various other information theoretic protocols, such as state merging, coherent state merging, and quantum channel simulation and rate distortion in the presence of quantum side information (see for e.g.[1,2] and references therein). It can be described as follows. Suppose Alice and Bob share a tripartite state ρ_{ABC} with the systems A and C being with Alice and the system B being with Bob. Let ψ_{ABCR} denote a purification of ρ_{ABC}, with R being the inaccessible, purifying reference system. In addition, Alice and Bob are allowed to share entangled states. The task is for Alice to transfer the state of her system A to Bob, possibly with the help of the prior shared entanglement, such that the purity of the global state is preserved. Alice and Bob can both do local operations (LO) on systems in their possession and Alice can send qubits to Bob, i.e., she is allowed one-way quantum communication (QC) with Bob. The minimum number of qubits needed for this task is referred to as the *quantum communication cost* of the protocol.

This protocol was first introduced by Devetak and Luo[3], but only an outer bound was proved. It was studied by Devetak and Yard[4,5] in the so-called 'asymptotic i.i.d. setting', in which Alice and Bob share multiple (say n) identical copies of the state ρ_{ABC}, instead of just one. The quantum communication cost, Q, in this setting is defined as the minimum rate of quantum communication from Alice to Bob needed so that the error incurred in achieving the goal (of transferring the states of the systems labelled by A from Alice to Bob) vanishes in the asymptotic limit ($n \to \infty$). Let the corresponding rate of entanglement consumption[18] be denoted as E. Devetak and Yard[4] proved that state redistrubution is possible in this setting if and only if Q and E satisfy the following bounds:

$$Q \geq \frac{1}{2} I(A;R|B); \quad Q + E \geq H(A|B). \tag{1}$$

Here $I(A;R|B)$ denotes the conditional mutual information of the state $\rho_{ABR} := \mathrm{Tr}_C \psi_{ABCR}$, and $H(A|B)$ is the conditional entropy of ρ_{AB}. In fact, this provided the

first operational interpretation of the quantum conditional mutual information[1,4].

In this paper, we first consider state redistribution in the 'one-shot setting' in which Alice and Bob share a *single copy* of the state ρ_{ABC}. Instead of requiring that the error incurred in the protocol vanishes asymptotically, it is natural in this case to allow for a small but non-zero error $\varepsilon > 0$. We refer to the minimum number of qubits which are needed to be transferred in this case as the *ε-error one-shot quantum communication cost*. We derive an upper bound on this quantity in terms of the smooth min- and max-entropies of One-shot Information Theory (see e.g.[9,10] and references therein).

Our ultimate goal is to derive an upper bound on the *second order asymptotic expansion* for the quantum communication cost of state redistribution, for n identical copies of the state ρ_{ABC}, with an error of at most ε. We establish that, for any tripartite state ρ_{ABC}, and any given $\varepsilon \in (0, 1)$, an upper bound on the quantum communication cost of achieving quantum state redistribution of $\rho_{ABC}^{\otimes n}$, with an error of at most ε, can be expressed in the form

$$an + b\sqrt{n} + \mathcal{O}(\log n);$$

here the first order coefficient a is equal to $\frac{1}{2}I(A; R|B)$ (as expected from the result of Devetak and Yard[4]). We obtain an explicit expression for the second order coefficient b, which depends on both the state ρ_{ABC} and the allowed error threshold ε.

A simple corollary of the above expansion is the following result: in the asymptotic i.i.d. setting[4], state redistribution can be achieved if Alice sends qubits at a rate $(1/2)I(A; R|B)$ to Bob (as is implied by (1)).

Our result employs the protocol of *coherent state merging*[19] which is described in the one-shot setting as follows. One starts with a tripartite pure state ψ_{ABR}, where the system A is with Alice, B is with Bob and R denotes the purifying reference system. Alice and Bob do not share any entanglement at the start of the protocol. The aim is for Alice to transfer the state of the system A to Bob and at the same time generate entanglement with him. Alice and Bob can both do local operations on systems in their possession and Alice can send qubits to Bob. The quantities of

interest are the quantum communication cost and the entanglement gain: the former is the minimum number of qubits that Alice needs to send to Bob in order to achieve the state transfer (up to a given finite accuracy) and the latter is the maximum entanglement created in this process. In previous work[8] we obtained bounds on these quantities under the constraint that the error incurred in the protocol was at most ε (for an arbitrary but fixed $\varepsilon \in (0, 1)$).

It is easy to see that this protocol can be considered as a special case of state redistribution: the system C which Alice has at the start of state redistribution can be viewed as quantum side information; then coherent state merging corresponds to the case in which no such side information is available to Alice. In this sense, state redistribution can be used as a primitive for coherent state merging. However, Oppenheim[7] proved that the reverse is also true: state redistribution can be achieved in the asymptotic i.i.d. setting by using coherent state merging as a primitive. In this paper we make use of this idea, and employ the bounds on the quantum communication cost and entanglement gain for one-shot coherent state merging[8], to obtain an upper bound on the quantum communication cost for one-shot state redistribution. We would like to point out that the same upper bound derived in this paper here was also independently obtained in the work by Berta, Christandl and Touchette[17].

In Section II we define the entropic quantities in terms of which our results, Theorem 1 and Theorem 3, are expressed, and state some of their relevant properties. In addition, we define the operational quantities of one-shot coherent state merging which we employ in our proof of Theorem 1. In Section III we give a precise definition of the operational quantity that we study, namely, the quantum communication cost of ε-error one-shot state redistribution and state our first theorem (Theorem 1) which consists of an upper bound on this cost. In Section IV we recall the protocol of coherent state merging, which we use as a primitive in our proof of Theorem 1, which is given in Section V. The statement and proof of our main result (Theorem 3), which consists of an upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution, is given in Section VI.

II. NOTATIONS AND DEFINITIONS

Let $\mathcal{P}(\mathcal{H})$ denote the set of positive semi-definite operators acting on a finite-dimensional Hilbert space $\mathcal{H}$, and let $\mathcal{D}(\mathcal{H}) \subset \mathcal{P}(\mathcal{H})$ denote the set of density matrices (states) on $\mathcal{H}$. Furthermore, let $\mathcal{D}_{\leq}(\mathcal{H})$ denote the set of subnormalized states[20]. For any given pure state $|\psi\rangle \in \mathcal{H}$, we denote the projector $|\psi\rangle\langle\psi|$ simply as ψ. For $\omega_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$, let $\omega_A := \mathrm{Tr}_B \omega_{AB}$ denote its restriction to the subsystem A. For $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, the fidelity is defined as $F(\rho, \sigma) := \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$. We use the same expression for fidelity when either one of ρ or σ is subnormalized. For simplicity, we denote a quantum operation (i.e., a completely positive trace-preserving (CPTP) map) $\Lambda : \mathcal{D}(\mathcal{H}_A) \mapsto \mathcal{D}(\mathcal{H}_B)$ as $\Lambda : A \mapsto B$. The identity map is denoted as id. A quantum operation on a bipartite system, shared between two distant parties (say, Alice and Bob), which consists of local operations on the two subsystems and quantum communication from Alice to Bob is said to be a (one-way) LOQC map.

The results in this paper involve various entropic quantities. The von Neumann entropy of a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ is given by $H(A)_\rho = -\mathrm{Tr}\rho_A \log \rho_A$. For a bipartite system, ρ_{AB} the conditional entropy of the subsystem A given B is defined as $H(A|B) = H(\rho_{AB}) - H(\rho_B)$. For a tripartite state ρ_{ABC}, the conditional mutual information of the subsystems A and B given C is defined as:

$$I(A; B|C) = H(B|C) - H(B|AC).$$

In addition to the above entropic quantities, we make use of the following generalized entropies[9,11] which arise naturally in one-shot quantum information theory:

Let $\rho_{AB} \in \mathcal{D}_{\leq}(\mathcal{H}_A \otimes \mathcal{H}_B)$. For a bipartite state ρ_{AB}, the min-entropy of A conditioned on B is defined as

$$H_{\min}(A|B)_\rho = \max_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} \left[-D_{\max}(\rho_{AB}||I_A \otimes \sigma_B)\right],$$

where for any $\rho \in \mathcal{D}_{\leq}(\mathcal{H})$ and $\omega \in \mathcal{P}(\mathcal{H})$, $D_{\max}(\rho||\omega)$ is the max-relative entropy[12]:

$$D_{\max}(\rho||\omega) := \inf\{\gamma : \rho \leq 2^\gamma \omega\}.$$

For any $\varepsilon \in (0,1)$, a smooth version of these quantities are given by

$$D^{\varepsilon}_{\max}(\rho||\omega) := \min_{\overline{\rho}\in\mathcal{B}_{\varepsilon}(\rho)} D_{\max}(\overline{\rho}||\omega)$$
$$H^{\varepsilon}_{\min}(A|B)_{\rho} := \max_{\overline{\rho}_{AB}\in\mathcal{B}_{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\overline{\rho}}, \tag{2}$$

where for any state $\rho \in \mathcal{D}(\mathcal{H})$, $\mathcal{B}_{\varepsilon}(\rho)$ denotes the ε-ball around ρ and is defined as

$$\mathcal{B}_{\varepsilon}(\rho) := \{\overline{\rho} \in \mathcal{D}_{\leq}(\mathcal{H}) : F^2(\overline{\rho},\rho) \geq 1-\varepsilon^2\}.$$

The smooth conditional max-entropy is given in terms of the smooth conditional min-entropy via the following duality relation[11,14,15]:

Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\rho_{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be an arbitrary purification of ρ_{AB}. Then for any $0 \leq \varepsilon \leq 1$,

$$H^{\varepsilon}_{\max}(A|C)_{\rho} := -H^{\varepsilon}_{\min}(A|B)_{\rho}. \tag{3}$$

We also make use of the Rényi entropy of order zero, which for a state $\rho \in \mathcal{D}(\mathcal{H})$ is defined as

$$H_0(A)_{\rho} = \log(\mathrm{rk}\rho_A),$$

where $\mathrm{rk}\rho_A$ denotes the rank of ρ_A. Its smooth version for any $\varepsilon \in (0,1)$ is given by

$$H^{\varepsilon}_0(A)_{\rho} = \min_{\overline{\rho}\in\mathcal{B}_{\varepsilon}(\rho)} H_0(A)_{\overline{\rho}}.$$

In order to obtain an upper bound on the second order asymptotic expansion for the quantum communication cost, we make use of the second order asymptotic expansion for the smooth max-relative entropy which was derived by Tomamichel and Hayashi in[13]: for any $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{P}(\mathcal{H})$ with $\mathrm{supp}\rho \subseteq \mathrm{supp}\sigma$, $\forall\, \varepsilon \in (0,1)$:

$$D^{\varepsilon}_{\max}(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) - \sqrt{n}\,\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon^2) + \mathcal{O}(\log n), \tag{4}$$

where $D(\rho\|\sigma) := \mathrm{Tr}\,(\rho\log\rho - \rho\log\sigma)$ is the quantum relative entropy,

$$\mathfrak{s}(\rho\|\sigma) := \sqrt{V(\rho\|\sigma)}, \quad \text{with} \quad V(\rho\|\sigma) := \mathrm{Tr}\left[\rho(\log\rho - \log\sigma)^2\right] - D(\rho\|\sigma)^2, \tag{5}$$

being the *quantum information variance*, and $\Phi^{-1}(\varepsilon) := \sup\{x \in \mathbb{R} \mid \Phi(x) \leq \varepsilon\}$ is the inverse of the cumulative distribution function of a standard normal random variable.

III. ONE-SHOT STATE REDISTRIBUTION

Our first result is an upper bound on the ε-error quantum communication cost and the ε-error entanglement cost of state redistribution. It is given by Theorem 1 below. Before stating it we need the following definition.

Definition 1. (One-shot state redistribution)
Consider a tripartite state ρ_{ABC} shared between two parties Alice and Bob, with the systems A and C being with Alice and the system B being with Bob. Let ψ_{ABCR} denote a purification of ρ_{ABC}, with R being the inaccessible, purifying reference system. Let Alice and Bob have further registers A_0, A_1 and B_0, B_1, respectively. A *one-shot ε-error state redistribution* protocol is then defined as a joint quantum operation $\Lambda : ACA_0 \otimes BB_0 \to CA_1 \otimes B_1B'B$, which is one-way LOQC (with the quantum communication being from Alice to Bob) and such that

$$F\left(\rho_{CA_1B_1B'BR}, \Phi^m_{A_1B_1} \otimes \psi_{CB'BR}\right) \geq 1 - \varepsilon, \tag{6}$$

where $\rho_{CA_1B_1B'BR} := (\Lambda \otimes \mathrm{id}_R)\left(\psi_{ABCR} \otimes \Phi^k_{A_0B_0}\right)$ and $\Phi^k_{A_0B_0}$, $\Phi^m_{A_1B_1}$ are maximally entangled states of Schmidt rank k, m, respectively. Here, B' is a local ancilla of Bob's of the same size as A. The quantum communication cost of the protocol, which we denote as $q^{(1)}_\varepsilon(\rho_{ABC}, \Lambda)$, is the minimum number of qubits that Alice needs to send to Bob for (6) to hold. Moreover, the number $(\log k - \log m) := e^{(1)}_\varepsilon(\rho_{ABC}, \Lambda)$ is called the entanglement cost of the protocol.

The quantum communication and entanglement cost of ε-error one-shot state redistribution for a state ρ_{ABC} are then defined as

$$q^{(1)}_\varepsilon(\rho_{ABC}) := \min_\Lambda q^{(1)}_\varepsilon(\rho_{ABC}, \Lambda), \tag{7}$$

$$e^{(1)}_\varepsilon(\rho_{ABC}) := \min_\Lambda e^{(1)}_\varepsilon(\rho_{ABC}, \Lambda), \tag{8}$$

where the minimum is taken over all ε-error one-shot state redistribution protocols Λ.

Our first main result in this paper is given by the following theorem.

Theorem 1. *Fix $\varepsilon \in (0,1)$. Then for any tripartite state ρ_{ABC}, there exists an ε-error one-shot state redistribution protocol Λ, with quantum communication and entanglement cost given by*

$$q_\varepsilon^{(1)}(\rho_{ABC},\Lambda) = \frac{1}{2}\left(H_{\max}^{\varepsilon'}(A|B)_\psi - H_{\min}^{\varepsilon'}(A|RB)_\psi\right) - 2\log\varepsilon', \tag{9}$$

$$e_\varepsilon^{(1)}(\rho_{ABC},\Lambda) = \frac{1}{2}\left(H_{\max}^{\varepsilon'}(A|B)_\psi - H_{\max}^{\varepsilon'}(A|C)_\psi\right), \tag{10}$$

where $\varepsilon' = \varepsilon^2/(\sqrt{5}+1)^2$, and ψ_{AB} and ψ_{ABR} are the reduced states of a purification ψ_{ABCR} of the state ρ_{ABC}.

In particular, the RHS of (9) and (10) provides an upper bound on the quantum communication cost $q_\varepsilon^{(1)}(\rho_{ABC})$ defined by (7) and the entanglement cost $q_\varepsilon^{(1)}(\rho_{ABC})$ defined by (8), respectively.

IV. ONE-SHOT COHERENT STATE MERGING: A PRIMITIVE FOR ONE-SHOT STATE REDISTRIBUTION

The proof of Theorem 1 employs a result on one-shot coherent state merging (or FQSW) proved in[8], which is given by Theorem 2 below. Before stating it, we need to introduce the following definition.

Definition 2 (One-shot coherent state merging or FQSW)**.** Consider a bipartite state ρ_{AB} shared between Alice and Bob, with the system A being with Alice and the system B being with Bob. Let ψ_{ABR} denote its purification, with R being the inaccessible, purifying reference system. We call a quantum operation $\tilde{\Lambda} : A\otimes B \to A_1 \otimes B_1 B' B$ *one-shot ε-error coherent state merging* of ρ_{AB} if it is one-way LOQC (with the quantum communication being from Alice to Bob) and the state $\Omega_{A_1B_1B'BR} := \left(\tilde{\Lambda}\otimes \mathrm{id}_R\right)\psi_{ABR}$, is such that

$$F\left(\Omega_{A_1B_1B'BR}, \Phi_{A_1B_1}^m \otimes \Psi_{B'BR}\right) \geq 1-\varepsilon, \tag{11}$$

where $\Phi_{A_1B_1}^m$ denotes a maximally entangled state of Schmidt rank m. Here, B' is a local ancilla of Bob's of the same size as A. The number $\log m$ is called the *entanglement gain* of the protocol and denoted as $\tilde{e}_\varepsilon^{(1)}(\rho_{AB},\tilde{\Lambda})$. Let $\tilde{q}_\varepsilon^{(1)}(\rho_{AB},\tilde{\Lambda})$ denote

the corresponding quantum communication cost, that is the minimum number of qubits that Alice needs to send to Bob for (11) to hold.

Theorem 2. [8] *Fix $\varepsilon \in (0,1)$. Then for any bipartite state ρ_{AB}, there exists an ε-error one-shot coherent state merging protocol, $\tilde{\Lambda}$, with entanglement gain and quantum communication cost respectively given by*[21]*,*

$$\tilde{e}_{\varepsilon}^{(1)}(\rho_{AB}, \tilde{\Lambda}) = \frac{1}{2}\left[H_0^{\varepsilon'}(A)_\psi + H_{\min}^{\varepsilon'}(A|R)_\psi\right] + \log \varepsilon' \tag{12}$$

$$\tilde{q}_{\varepsilon}^{(1)}(\rho_{AB}, \tilde{\Lambda}) = \frac{1}{2}\left[H_0^{\varepsilon'}(A)_\psi - H_{\min}^{\varepsilon'}(A|R)_\psi\right] - \log \varepsilon' \tag{13}$$

where $\varepsilon' = \varepsilon^2/(\sqrt{5}+1)^2$, and ψ_A and ψ_{AR} are the reduced states of a purification ψ_{ABR} of the state ρ_{AB}.

Remark: The proof of the above theorem[8] relies on a decoupling argument and ensures the existence of a unitary operator U and an isometry V, such that ε-error one-shot coherent state merging is achieved if (i) Alice acts on the state of her system A with U, (ii) sends $\tilde{q}_{\varepsilon}^{(1)}$ qubits to Bob, and (iii) Bob acts on the composite state of the qubits that he receives from Alice and the state of his system B by the isometry V.

V. PROOF OF THEOREM 1

For any tripartite state ρ_{ABC}, an expression for the quantum communication cost of an ε-error one-shot state redistribution protocol, for any fixed $\varepsilon \in (0,1)$, can be obtained by a direct application of one-shot coherent state merging, if we simply consider Alice to transfer the state of her system A to Bob, without exploiting the additional system C which is in her possession. In this case, we can consider C to be part of the reference system. From eq.(13) of Theorem 2 we then infer that state redistribution can be achieved by the transfer of the following number of qubits from Alice to Bob:

$$\Delta q = \frac{1}{2}[H_0^{\varepsilon'}(A)_\psi - H_{\min}^{\varepsilon'}(A|CR)_\psi] - \log \varepsilon', \tag{14}$$

where ε' is as stated in Theorem 1. Meanwhile, from eq.(12) of Theorem 2, the amount of entanglement generated is

$$\Delta e_1 = \frac{1}{2}[H_0^{\varepsilon'}(A)_\psi + H_{\min}^{\varepsilon'}(A|CR)_\psi] + \log \varepsilon'. \tag{15}$$

However, one-shot state redistribution can be achieved at a lower quantum communication cost than that given by (14) above. A simple way to see this is by employing the one-shot version of a novel construction which was introduced by Oppenheim[7] in the asymptotic i.i.d. setting. In it the system C plays the role of a coherent relay as explained below (see also Figure 1). For this construction, it is convenient to split the

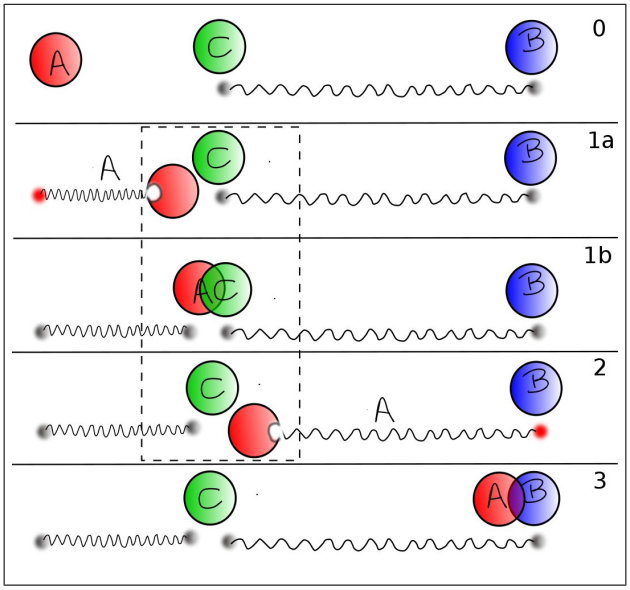

FIG. 1. *The ε-error one-shot state redistribution protocol using one-shot coherent state merging and ebit repackaging. Shares of the state ρ_{ABC} are represented by circles, while shared entanglement is represented by wiggly lines. The protocol of ebit repackaging is contained in the dashed rectangle. Due to the ebit repackaging, $\tilde{e}_\varepsilon^{(1)}(\rho_{AB}, \tilde{\Lambda})$ qubits (highlighted in red and given by (12) of Theorem 2) are effectively sent to Bob without being physically transferred. Here $\tilde{\Lambda}$ denotes the coherent state merging protocol from Alice to Charlie.*

two-party protocol between Alice and Bob into a three-party protocol, by considering the system C to be in the possession of a third party (say, Charlie). The construction

is implemented through the following steps:

Step 1. One-shot ε-error coherent state merging from Alice to Charlie: Let us denote this protocol by $\tilde{\Lambda}$. It results in the transfer of Alice's state ρ_A to Charlie (with an error of atmost ε), with the simultaneous generation of entanglement between them. By eq.(12) of Theorem 2, the number of ebits of entanglement generated at this stage is given by

$$\Delta e_2 := \frac{1}{2}\left[H_0^{\varepsilon'}(A)_\psi + H_{\min}^{\varepsilon'}(A|BR)_\psi\right] + \log\varepsilon'. \tag{16}$$

From the remark given after Theorem (2) it follows that this step can itself be broken down into two steps[7]: (i) Alice applies a unitary transformation denoted by a unitary operator U (say) on her system A and sends the required number of qubits (needed to implement a one-shot ε-error coherent state merging protocol $\tilde{\Lambda}$) to Charlie. This number is given by the right hand side of eq.(13) of Theorem 2, with the replacement of R by BR. This is because in this case BR play the role of the reference. (ii) Charlie then does the corresponding decoding isometry V (say) on the composite state of the qubits that he receives from Alice and the system C in his possession. After applying V, the resulting output will be Δe_2 ebits, shared between him and Alice, and a remaining subsytem S in Charlie's possession.

Step 2. Ebit repackaging: Charlie sets aside his share of the ebits that were generated from the previous step and replaces them by those that he shared with Bob at the start of the protocol. He then applies $V^\dagger$ to the joint state of the latter and S.

Note that the above steps effectively result in the transfer of Δe_2 qubits from Alice to Bob. Hence, instead of sending Δq qubits (given by (14)), Alice (or, in this three-party description, Charlie) only needs to physically send $(\Delta q - \Delta e_2)$ qubits to Bob, in order to achieve ε-error one-shot state redistribution. From (14) and (16) we then infer that there exists an ε-error one-shot state redistribution protocol, Λ, with

quantum communication cost:

$$\begin{aligned} q_{\varepsilon}^{(1)}(\rho_{ABC}, \Lambda) &= \Delta q - \Delta e_2 \\ &= \frac{1}{2}\left(-H_{\min}^{\varepsilon'}(A|CR)_{\psi} - H_{\min}^{\varepsilon'}(A|BR)_{\psi}\right) - 2\log\varepsilon', \\ &= \frac{1}{2}\left(H_{\max}^{\varepsilon'}(A|B)_{\psi} - H_{\min}^{\varepsilon'}(A|BR)_{\psi}\right) - 2\log\varepsilon', \end{aligned} \tag{17}$$

where the last line follows from the duality relation (3), since ψ_{ABCR} is a pure state.

To show the entanglement cost of the ε-error one-shot state redistribution protocol, note that the naive protocol (that treats C as part of a reference system) generates Δe_1 amount of entanglement. However, the protocol of *ebit repackaging* trades Δe_2 amount of generated entanglement into quantum communication. Thus the entanglement cost of the ε-error one-shot state redistribution protocol is

$$\begin{aligned} e_{\varepsilon}^{(1)}(\rho_{ABC}, \Lambda) &= -(\Delta e_1 - \Delta e_2) \\ &= \frac{1}{2}\left(-H_{\min}^{\varepsilon'}(A|CR)_{\psi} + H_{\min}^{\varepsilon'}(A|BR)_{\psi}\right), \\ &= \frac{1}{2}\left(H_{\max}^{\varepsilon'}(A|B)_{\psi} - H_{\max}^{\varepsilon'}(A|C)_{\psi}\right). \end{aligned} \tag{18}$$

This completes the proof of Theorem 1.

VI. SECOND ORDER ASYMPTOTICS

Consider the situation in which Alice and Bob share n identical copies of the state ρ_{ABC}. In this case, it follows from Theorem 1 that an upper bound on the quantum

communication cost, $q_\varepsilon^{(1)}(\rho_{ABC}^{\otimes n})$, for state redistribution is given by the following:

$$\begin{aligned}
q_\varepsilon^{(1)}(\rho_{ABC}^{\otimes n}) &\leq \frac{1}{2}\left[H_{\max}^{\varepsilon'}(A_n|B_n)_\psi - H_{\min}^{\varepsilon'}(A_n|R_nB_n)_\psi\right] - 2\log\varepsilon', \\
&= \frac{1}{2}\left[-H_{\min}^{\varepsilon'}(A_n|C_nR_n)_\psi - H_{\min}^{\varepsilon'}(A_n|R_nB_n)_\psi\right] - 2\log\varepsilon', \\
&= \frac{1}{2}[\min_{\sigma_{C_nR_n}} D_{\max}^{\varepsilon'}(\psi_{A_nC_nR_n}||I_{A_n}\otimes\sigma_{C_nR_n}) \\
&\quad + \min_{\omega_{B_nR_n}} D_{\max}^{\varepsilon'}(\psi_{A_nB_nR_n}||I_{A_n}\otimes\omega_{B_nR_n})] - 2\log\varepsilon' \\
&\leq \frac{1}{2}[\min_{\sigma_{CR}} D_{\max}^{\varepsilon'}(\psi_{ACR}^{\otimes n}||I_A^{\otimes n}\otimes\sigma_{CR}^{\otimes n}) \\
&\quad + \min_{\omega_{BR}} D_{\max}^{\varepsilon'}(\psi_{ABR}^{\otimes n}||I_A^{\otimes n}\otimes\omega_{BR}^{\otimes n})] - 2\log\varepsilon', \qquad (19)
\end{aligned}$$

where $\psi_{A_nB_nC_nR_n} \equiv \psi_{ABCR}^{\otimes n}$, with ψ_{ABCR} being a purification of ρ_{ABC}. The first equality follows from the duality relation (3), the second equality follows from the definition (2) of the smooth conditional min-entropy, the second inequality follows from the restriction of the minimization to a smaller set, and the fact that the reduced states of $\psi_{A_nB_nC_nR_n}$ are tensor-power states. The minimizations in the above equation are all over (normalized) states.

We now employ the second order asymptotic expansion of the max-relative entropy, given by (4), which we recall here for convenience:

$$D_{\max}^{\varepsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) - \sqrt{n}\,\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon^2) + \mathcal{O}(\log n).$$

Note that for $\varepsilon \in (0, \frac{1}{2})$, $\Phi^{-1}(\varepsilon) < 0$ and hence the second term on the right hand side of the above equation is positive.

Substituting the above expansion for the smooth max-relative entropies, with the smoothing parameter given by $\varepsilon' = \varepsilon^2/(\sqrt{5}+1)^2$, in the last line of (19), we obtain:

for any $\varepsilon \in (0, 1/2)$,

$$\begin{aligned} q_\varepsilon^{(1)}(\rho_{ABC}^{\otimes n}) &\leq n\Big[\frac{1}{2}\big[\min_{\sigma_{CR}} D(\psi_{ACR}||I_A \otimes \sigma_{CR}) + \min_{\omega_{BR}} D(\psi_{ABR}||I_A \otimes \omega_{BR})\big]\Big] \\ &\quad + \frac{1}{2}\min_{\sigma_{CR}}\Big[\big(-\sqrt{n}\Phi^{-1}(\varepsilon'^2)\big)\mathfrak{s}(\psi_{ACR}||I_A \otimes \sigma_{CR})\Big] \\ &\quad + \frac{1}{2}\min_{\omega_{BR}}\Big[\big(-\sqrt{n}\Phi^{-1}(\varepsilon'^2)\big)\mathfrak{s}(\psi_{ABR}||I_A \otimes \omega_{BR})\Big] + \mathcal{O}(\log n), \\ &\leq n\big[\frac{1}{2}I(A;R|B)_\psi\big] - \sqrt{n}\Phi^{-1}(\varepsilon'^2)\Big[\frac{1}{2}\big[\mathfrak{s}(\psi_{ACR}||I_A \otimes \psi_{CR}) + \mathfrak{s}(\psi_{ABR}||I_A \otimes \psi_{BR})\big]\Big] \\ &\quad + \mathcal{O}(\log n). \end{aligned} \tag{20}$$

To arrive at the last line of (20), we used the following facts:
(*i*) $\varepsilon' < \varepsilon$ and hence $\Phi^{-1}(\varepsilon'^2) < 0$;
(*ii*) for any bipartite state ρ_{AB}, $\min_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} D(\rho_{AB}||I_A \otimes \sigma_B) = D(\rho_{AB}||I_A \otimes \rho_B)$, which simply follows from the fact that the relative entropy of two states is non-negative (see e.g. Lemma 6 of[16])
(*iii*) For a pure state ψ_{ABCR}, $H(A|CR)_\psi = -H(A|B)_\psi$, where ψ_{ACR} and ψ_{ABR} are the reduced states of ψ_{ABCR}.
(*iv*) $I(A;R|B) = H(A|B) - H(A|BR)$.

Thus we have proved the following theorem, which constitutes our second main result:

Theorem 3. *Fix $\varepsilon \in (0, 1/2)$. Then for any tripartite state ρ_{ABC}, an upper bound on the second order asymptotic expansion for the quantum communication cost of achieving state redistribution with an error of at most ε, is given by*

$$n\big[\frac{1}{2}I(A;R|B)_\psi\big] - \sqrt{n}\Phi^{-1}(\varepsilon'^2)\Big[\frac{1}{2}\big[\mathfrak{s}(\psi_{ACR}||I_A \otimes \psi_{CR}) + \mathfrak{s}(\psi_{ABR}||I_A \otimes \psi_{BR})\big]\Big] + \mathcal{O}(\log n), \tag{21}$$

where $\varepsilon' = \varepsilon^2/(\sqrt{5}+1)^2$, and $\mathfrak{s}(\cdot||\cdot)$, defined by (5), denotes the square root of the quantum information variance.

As a corollary of this theorem we recover the following result of Devetak and Yard[4] stated earlier: *in the asymptotic i.i.d. setting, state redistribution for a tripartite state ρ_{ABC} can be achieved if Alice sends qubits at a rate $(1/2)I(A;R|B)$ to Bob.* This

immediately follows from Theorem 3 since the quantum communication cost Q in the asymptotic i.i.d. setting can be expressed in terms of $q_\varepsilon^{(1)}(\rho_{ABC}^{\otimes n})$ as follows:

$$Q \equiv Q(\rho_{ABC}) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} q_\varepsilon^{(1)}(\rho_{ABC}^{\otimes n}). \tag{22}$$

ACKNOWLEDGEMENTS

We had stated the one-shot result given in Theorem 1 in an earlier paper[8]. We are grateful to Mario Berta, Matthias Christandl and Dave Touchette for getting us to finally write up its proof. We are also grateful to Felix Leditzky for his comments on a first draft of this paper. MH is supported by an ARC Future Fellowship under Grant FT140100574.

REFERENCES

[1]I. Devetak and J. Yard, The operational meaning of quantum conditional information, arXiv:quant-ph/0612050.

[2]M. M. Wilde, N. Datta, M-H. Hsieh, A. Winter, Quantum rate distortion coding with auxiliary resources, IEEE Transactions on Information Theory, vol. 59, no. 10, pp. 6755-6773 (October 2013).

[3]Z. Luo and I. Devetak, Channel simulation with quantum side information, IEEE Transactions on Information Theory, vol. 55, no. 3, pp. 13311342, March 2009, arXiv:quant-ph/0611008.

[4]J. Yard and I. Devetak, Optimal quantum source coding with quantum side information at the encoder and decoder, IEEE Transactions in Information Theory, vol. 55, no. 11, pp. 53395351, November 2009, arXiv:0706.2907.

[5]I. Devetak and J. Yard, Exact cost of redistributing multipartite quantum states, Physical Review Letters, vol. 100, no. 23, p. 230501, June 2008.

[6]A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, The mother of all protocols: restructing quantum information's family tree, Proceedings of the Royal Society A, vol. 465, pp. 2537-2563, 2009.

[7]J. Oppenheim, State redistribution as merging: introducing the coherent relay, arXiv:0805.1065, (2008).

[8]N. Datta and M.-H. Hsieh, The apex of the family tree of protocols: optimal rates and resource inequalities, New Journal of Physics, vol. 13, p. 093042 (2011).

[9]R. Renner, Security of quantum key distribution, PhD thesis, arXiv:quant-ph/0512258.

[10]M. Tomamichel, A Framework for Non-Asymptotic Quantum Information Theory, PhD Thesis, Department of Physics, ETH Zurich, arXiv:1203.2142.

[11]R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, Transactions on Information Theory, vol. 55, pp.4337-4347 (2009).

[12]N. Datta, Min- and Max- Relative Entropies and a New Entanglement Monotone, IEEE Transactions on Information Theory, vol. 55, p. 2816-2826 (2009).

[13]M. Tomamichel and M. Hayashi, A hierarchy of information quantities for finite block length analysis of quantum tasks, IEEE Transactions on Information Theory vol. 59 pp. 7693-7710 (2013).

[14]M. Tomamichel, R. Colbeck, and R. Renner, Fully Asymptotic Equipartition Property, IEEE Transactions on Information Theory, vol. 55, pp. 5840-5847 (2009).

[15]M. Tomamichel, R. Colbeck, and R. Renner, Duality between smooth min- and max-entropies, IEEE Transactions on Information Theory, vol. 56, pp. 4674-4681 (2010).

[16]F. Buscemi and N. Datta, The quantum capacity of channels with arbitrarily correlated noise, IEEE Transactions on Information Theory, vol. 56, pp. 1447-1460 (2010).

[17]M. Berta, M. Christandl and D. Touchette, Smooth Entropy Bounds on One-Shot Quantum State Redistribution, arXiv: 1409.4338, 2014.

[18]A negative entanglement consumption rate implies that entanglement is instead generated.

[19]This protocol is also known as FQSW, which is an acronym for Fully Quantum Slepian Wolf[6].

[20]Throughout this paper, we restrict our considerations to finite-dimensional Hilbert spaces and take the logarithm to base 2.

[21]The choice of the smoothing parameter ε' here is different from that in[8] because here we choose the figure of merit for the coherent state merging protocol to be given by the fidelity, whereas in[8] we chose it to be the trace distance.