The apex of the family tree of protocols: optimal rates and resource inequalities

2011 New J. Phys. 13 093042

(http://iopscience.iop.org/1367-2630/13/9/093042)

New Journal of Physics
The open-access journal for physics

The apex of the family tree of protocols: optimal rates and resource inequalities

Nilanjana Datta and Min-Hsiu Hsieh
Statistical Laboratory, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail: n.datta@statslab.cam.ac.uk and minhsiuh@gmail.com

New Journal of Physics **13** (2011) 093042 (30pp)
Received 12 June 2011
Published 30 September 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/9/093042

Abstract. We establish bounds on the maximum entanglement gain and minimum quantum communication cost of the fully quantum Slepian–Wolf (FQSW) protocol in the one-shot regime, which is considered to be at the apex of the existing family tree in quantum information theory. These quantities, which are expressed in terms of smooth min- and max-entropies, reduce to the known rates of quantum communication cost and entanglement gain in the asymptotic independent and identically distributed scenario. We also provide an explicit proof of the optimality of these asymptotic rates. We introduce a resource inequality for the one-shot FQSW protocol, which in conjunction with our results yields achievable one-shot rates of its children protocols. In particular, it yields bounds on the one-shot quantum capacity of a noisy channel in terms of a single entropic quantity, unlike previous bounds. We also obtain an explicit expression for the achievable rate for one-shot state redistribution.

Contents

1. Introduction

An important problem in quantum information theory is the evaluation of optimal rates of various information processing tasks. These include data compression [1, 2], information transmission [3–8], entanglement manipulation [9–12], state merging [13, 14], channel simulation [15, 16] and a host of other protocols [15, 17–24]. Initially, all these different protocols were considered to be unrelated and each of them was studied individually. That was until the authors of [17] proposed two new protocols, namely the 'mother' and 'father' protocols, from which five of the previously studied protocols could be generated by direct application of teleportation and superdense coding. More precisely, entanglement distillation [11, 12], noisy teleportation [17] and noisy superdense coding [19] could be generated from the 'mother', whereas the transmission of quantum information through a quantum channel [6–8] and the entanglement-assisted transmission of classical information through a quantum channel [15, 20, 21] could be generated from the 'father'.

Within the *resource framework* developed in [17, 18], quantum Shannon theory can ultimately be viewed as the study of inter-conversions between non-local information-processing resources. These resources can be classified as either static (e.g. shared randomness or entanglement) or dynamic (e.g. communication channels). Further, they may be either noisy or noiseless, and finite or asymptotic. Noiseless resources are the fundamental ingredients of information theory because they can be employed to achieve essential tasks (e.g. information transmission, teleportation, etc) *perfectly*, that is, without any error. The basic unit of a noiseless quantum static resource is represented by an Einstein–Podolsky–Rosen (EPR) pair (an ebit), whereas the corresponding dynamic one is a noiseless single-qubit channel. At the most fundamental level, optimal rates of protocols hence characterize the quantity of noiseless resources that can be extracted from a given noisy one. The 'mother', which is a quantum communication-assisted entanglement distillation protocol, is a parent of protocols that involve 'static' resources, whereas the 'father', which is an entanglement-assisted quantum communication protocol, is a parent of protocols that involve 'dynamic' resources.

In 2006, yet another protocol, called the fully quantum Slepian–Wolf (FQSW) was proposed [25], which achieved the remarkable feat of unifying the family tree mentioned above. It is, hence, also referred to as 'the mother of all protocols'. It is a generalization of the 'mother' protocol since, in addition to quantum communication-assisted entanglement distillation, it accomplishes state transfer from the sender to the receiver. Moreover, the FQSW can also be transformed into the 'father' protocol by employing the Schmidt symmetry [25, 26]. In addition, the FQSW protocol can be used as a primitive for the following important protocols: state merging [13, 14], simulation of channels (a fully quantum reverse Shannon theorem) [15, 16, 27], quantum communication through broadcast channels [28, 29], distributed compression [25] and state redistribution [30–32]. It is, hence, evident that the FQSW protocol is at the heart of quantum Shannon theory. The FQSW protocol derives its name from its applicability to distributed compression, a problem that was solved in the classical case by Slepian and Wolf [33]. It is also referred to as state transfer [26] or the merging mother [34]. Note, however, that the family tree is not exhaustive since it does not cover all information-theoretic protocols. Also, the tree structure is not unique, since, for example, it is possible to obtain the FQSW from state merging via superdense coding [34].

Optimal rates of quantum information-processing tasks were originally evaluated in the so-called asymptotic independent and identically distributed (IID) scenario, i.e. in the limit of asymptotically many uses of the underlying resources, under the assumption that there was no correlation between successive uses. In other words, quantum channels employed in the protocols were assumed to be memoryless and entanglement resources were assumed to consist of states that were multiple copies (and hence tensor products) of a given entangled state.

In real-world applications, however, this assumption and the consideration of the asymptotic scenario are not necessarily justified. A more general theory of quantum information-processing protocols is obtained instead in the so-called one-shot scenario [27, 35–43], in which resources are considered to be finite and the information-processing tasks are required to be achieved only up to a finite accuracy. This also corresponds to the scenario in which experiments are performed, since channels and entanglement resources available for practical uses are typically finite and correlated, and transformations can only be achieved approximately. The fact that the one-shot scenario is more general than the asymptotic IID is further evident from the fact that optimal rates of protocols in the latter can be obtained directly from the corresponding one-shot rates. Further, one-shot rates also yield asymptotic rates for protocols involving correlated resources via the quantum information spectrum method (see, e.g., [44, 45] and references therein).

In this paper, we focus on the one-shot FQSW protocol and evaluate the upper and lower bounds on its optimal rates. In this protocol, one starts with a *single copy* of a tripartite pure state $|\psi\rangle^{ABR}$, where the system A is with Alice, B is with Bob and R denotes the purifying reference system. The aim is for Alice to transfer the A-part of the state 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 minimum quantum communication cost, i.e. 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 maximum resulting entanglement gain are referred to as the optimal rates of the one-shot FQSW protocol. Since this protocol is the one-shot version of the 'mother of all protocols', it can be viewed as the most basic building block of quantum Shannon theory and is at the *apex of the family tree of protocols*.

The one-shot FQSW was first introduced in [25] and studied in [27, 43]. Moreover, a classical-quantum version of it was treated in [36]. In [27], an expression for the achievable rates was obtained in terms of an unsmoothed min-entropy. However, the optimality of these rates or the analysis of the asymptotic case was not addressed. In contrast, we obtain both lower and upper bounds on the optimal rate of one-shot FQSW. Our achievable rates are expressible in terms of smooth min- and max-entropies [46–49], which have the advantage of directly yielding the known achievable rates of the FQSW in the asymptotic IID scenario (which are expressed in terms of the mutual information) [25]. Moreover, our one-shot results can be used to prove that these asymptotic rates of quantum communication cost and entanglement gain are indeed optimal [14]. Further, we introduce a resource inequality (RI) for the one-shot FQSW protocol. This leads to resource inequalities and achievable rates for the one-shot 'mother' and 'father' protocols and their children. In this paper we list some of these, a more exhaustive study of all the children protocols being deferred to a forthcoming paper. In particular, we obtain upper and lower bounds on the one-shot quantum capacity of a noisy channel in terms of the *same* entropic quantity, namely a smooth max-entropy, unlike previously obtained bounds [38]. As shown in [56], the FQSW protocol can be used as a primitive for state redistribution. Consequently, our results on the one-shot FQSW can be used to obtain an expression for the achievable rate for one-shot state redistribution. A more detailed analysis of this will be presented in [56]. The smooth min- and max-entropies appearing in our theorems have interesting properties and satisfy a series of useful inequalities (see, e.g., appendix A). These relations and a one-shot decoupling lemma are the main ingredients of our proofs.

The paper is organized as follows. We start with some definitions and notation in section 2. In section 3, we state our main results on the one-shot FQSW, the optimality of the rates of quantum communication cost and entanglement gain in the asymptotic IID scenario and the bounds on the one-shot quantum capacity of a noisy channel. In section 4 we introduce resource inequalities for the one-shot FQSW and some of its children protocols. Theorems 8–12 and the one-shot resource inequalities of section 4 constitute the main results of this paper. Proofs of theorems 8 and 9 are given in section 5, while the one-shot decoupling theorem, which is employed in the proof of theorem 8, is proved in appendix B. In appendix A, we list the various entropic inequalities we use.

2. Notation and definitions

Let $\mathcal{B}(\mathcal{H})$ denote the algebra of linear operators acting on a finite-dimensional Hilbert space $\mathcal{H}$, and let $\mathcal{D}(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ denote the set of positive operators of unit trace (states) on $\mathcal{H}$. Furthermore, let $\mathcal{D}_{\leqslant}(\mathcal{H})$ denote the set of subnormalized states. Throughout this paper, we restrict our consideration to finite-dimensional Hilbert spaces and denote the dimension of a Hilbert space $\mathcal{H}_A$ by $|A|$.

For any given pure state $|\psi\rangle \in \mathcal{H}$, we denote the projector $|\psi\rangle\langle\psi|$ simply as ψ. For a positive semi-definite operator $\omega^{AB} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, let $\omega^A := \mathrm{tr}_B\, \omega^{AB}$ denote its restriction to the subsystem A. For given orthonormal bases $\{|i^A\rangle\}_{i=1}^d$ and $\{|i^B\rangle\}_{i=1}^d$ in isomorphic Hilbert spaces $\mathcal{H}_A \simeq \mathcal{H}_B \simeq \mathcal{H}$ of dimension d, we define a maximally entangled state (MES) of Schmidt rank d to be

$$|\Phi\rangle^{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i^A\rangle \otimes |i^B\rangle. \tag{1}$$

Let $\mathbb{I}_A$ denote the identity operator in $\mathcal{B}(\mathcal{H}_A)$, and let $\tau^A := \mathbb{I}_A/|A|$ denote the completely mixed state in $\mathcal{D}(\mathcal{H}_A)$.

In the following, we denote a completely positive trace-preserving (CPTP) map $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_B)$ simply as $\mathcal{E}^{A\to B}$. Similarly, we denote an isometry $U : \mathcal{H}_A \mapsto \mathcal{H}_B \otimes \mathcal{H}_C$ simply as $U^{A\to BC}$.

The trace distance between two operators A and B is given by

$$\|A - B\|_1 := \mathrm{tr}[\{A \geqslant B\}(A - B)] - \mathrm{tr}[\{A < B\}(A - B)], \tag{2}$$

where $\{A \geqslant B\}$ denotes the projector on the subspace where the operator $(A - B)$ is non-negative, and $\{A < B\} := \mathbb{I} - \{A \geqslant B\}$. The fidelity of two states ρ and σ is defined as

$$F(\rho, \sigma) := \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} = \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1. \tag{3}$$

Note that the definition of fidelity can be naturally extended to subnormalized states. The trace distance between two states ρ and σ is related to the fidelity $F(\rho, \sigma)$ as follows (see e.g. [50]):

$$1 - F(\rho, \sigma) \leqslant \tfrac{1}{2}\|\rho - \sigma\|_1 \leqslant \sqrt{1 - F^2(\rho, \sigma)}, \tag{4}$$

where we use the notation $F^2(\rho, \sigma) = (F(\rho, \sigma))^2$. For $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{D}_{\leqslant}(\mathcal{H})$, we also use the quantity

$$C(\rho, \sigma) := \sqrt{1 - F^2(\rho, \sigma)}, \tag{5}$$

which was introduced in [51] and proved to be a metric. It is monotonic under any CPTP map $\mathcal{E}$, i.e.

$$C(\rho, \sigma) \geqslant C(\mathcal{E}(\rho), \mathcal{E}(\sigma)). \tag{6}$$

Moreover, if $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, then

$$C(\rho, \sigma) \leqslant \sqrt{\|\rho - \sigma\|_1}. \tag{7}$$

This follows by noting that $C(\rho, \sigma)$ is a special case of the purified distance $P(\rho, \sigma)$ (introduced in [48]), which satisfies these properties. We use the following lemma.

Lemma 1 (gentle measurement lemma [59, 60]). *For a state $\rho \in \mathcal{D}(\mathcal{H})$ and operator $0 \leqslant \Lambda \leqslant \mathbb{I}$, if $\mathrm{tr}\,\Lambda\rho \geqslant 1 - \delta$, then*

$$\|\rho - \sqrt{\Lambda}\rho\sqrt{\Lambda}\|_1 \leqslant 2\sqrt{\delta}.$$

The same holds if ρ is a subnormalized density operator.

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 $H(A)_\rho = -\mathrm{tr}\,\rho^A \log \rho^A$. Throughout this paper we take the logarithm to base 2. For any state $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the coherent information $I(A\rangle B)_\rho$ and the quantum mutual information $I(A : B)_\rho$ are defined, respectively, as

$$I(A\rangle B)_\rho := H(B)_\rho - H(AB)_\rho, \tag{8}$$

$$I(A : B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho. \tag{9}$$

In addition to the above entropic quantities, we make use of the following generalized relative entropy quantity, referred to as the max-relative entropy, introduced in [52]:

Definition 2. *The max-relative entropy of two operators $\rho \in \mathcal{D}_{\leqslant}(\mathcal{H})$ and $\sigma \in \mathcal{B}(\mathcal{H})$, $\sigma \geqslant 0$, is defined as*

$$D_{\max}(\rho||\sigma) := \log \min\{\lambda : \rho \leqslant \lambda\sigma\}. \tag{10}$$

We also use the following conditional min- and max-entropies defined in [46–48].

Definition 3. *Let $\rho^{AB} \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The min-entropy of A conditioned on B for the state ρ^{AB} is defined as*

$$H_{\min}(A|B)_\rho = \max_{\sigma^B \in \mathcal{D}(\mathcal{H}_B)} \left[-D_{\max}(\rho^{AB}||\mathbb{I}_A \otimes \sigma^B)\right].$$

Definition 4. *For any $0 \leqslant \varepsilon \leqslant 1$ and $\rho \in \mathcal{D}(\mathcal{H})$, we define the ε-ball around ρ as follows:*

$$\mathcal{B}^\varepsilon(\rho) = \{\bar{\rho} \in \mathcal{D}_{\leqslant}(\mathcal{H}) : F^2(\bar{\rho}, \rho) \geqslant 1 - \varepsilon^2\}.$$

Note that if $\bar{\rho} \in \mathcal{B}^\varepsilon(\rho)$ then $C(\bar{\rho}, \rho) \leqslant \varepsilon$.

Definition 5. *Let $0 \leqslant \varepsilon \leqslant 1$ and $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The ε-smooth min-entropy of A conditioned on B for the state ρ^{AB} is defined as*

$$H^\varepsilon_{\min}(A|B)_\rho = \max_{\bar{\rho}^{AB} \in \mathcal{B}^\varepsilon(\rho^{AB})} H_{\min}(A|B)_{\bar{\rho}}.$$

We also use the max-entropy that is defined in terms of the min-entropy via the following duality relation [47–49].

Definition 6 [48]. *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 $0 \leqslant \varepsilon \leqslant 1$,*

$$H^\varepsilon_{\max}(A|C)_\rho := -H^\varepsilon_{\min}(A|B)_\rho. \tag{11}$$

When ρ^{AB} is a pure state,

$$H^\varepsilon_{\min}(A|B)_\rho = -H^\varepsilon_{\max}(A)_\rho. \tag{12}$$

For any state $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ the ε-smooth conditional max-entropy can be equivalently expressed as [48, 49]

$$H^\varepsilon_{\max}(A|B)_\rho := \min_{\bar{\rho}^{AB} \in \mathcal{B}^\varepsilon(\rho^{AB})} H_{\max}(A|B)_{\bar{\rho}}, \tag{13}$$

where

$$H_{\max}(A|B)_{\bar{\rho}} = \max_{\sigma^B \in \mathcal{D}(\mathcal{H}_B)} 2 \log F(\bar{\rho}^{AB}, \mathbb{I}_A \otimes \sigma^B). \tag{14}$$

Moreover, for any $\rho^A \in \mathcal{D}_{\leqslant}(\mathcal{H}_A)$,

$$H_{\max}(A)_\rho = 2 \log \mathrm{tr}\sqrt{\rho^A}. \tag{15}$$

Other than the conditional min- and max-entropies, we also require the entropic quantity defined below.

Definition 7. *Given any $\rho^{AB} \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we define*

$$H_0(A|B)_\rho = \max_{\sigma^B \in \mathcal{D}(\mathcal{H}_B)} \log \operatorname{tr} \Pi_{\rho^{AB}}(\mathbb{I}_A \otimes \sigma^B), \tag{16}$$

where $\Pi_{\rho^{AB}}$ denotes the projector onto the support of ρ^{AB}. For any $0 \leqslant \varepsilon \leqslant 1$, define

$$\tilde{H}_0(A|B)_\rho := \min_{\bar{\rho}^{AB} \in \mathcal{B}^\varepsilon(\rho^{AB})} H_0(A|B)_{\bar{\rho}}. \tag{17}$$

When the system B is trivial, we have

$$H_0(A)_\rho = \log \operatorname{tr} \Pi_{\rho^A},$$

where Π_{ρ^A} denotes the projector onto the support of ρ^A.

We also use the following entropic quantity, which is obtained by a different smoothing of $H_0(A)_\rho$. For any $0 \leqslant \varepsilon \leqslant 1$ and any $\rho^A \in \mathcal{D}(\mathcal{H}_A)$, define

$$H_0^\varepsilon(A)_\rho := \min_{\substack{0 \leqslant Q \leqslant \mathbb{I}_A \\ \operatorname{tr} Q\rho^A \geqslant 1-\varepsilon}} H_0(A)_{\rho_Q^A}, \tag{18}$$

where ρ_Q^A is defined as

$$\rho_Q^A := \sqrt{Q}\rho^A\sqrt{Q}. \tag{19}$$

It follows from the gentle measurement lemma (lemma 1) that $\|\rho_Q^A - \rho^A\|_1 \leqslant 2\sqrt{\varepsilon}$ and simple calculation gives $\rho_Q^A \in \mathcal{B}^\delta(\rho^A)$, where $\delta = \sqrt{4\sqrt{\varepsilon} - 4\varepsilon}$. Various properties of the entropies defined above, which we employ in our proofs, are given in appendix A.

3. Main results

3.1. Optimal rates for the one-shot fully quantum Slepian–Wolf (FQSW) protocol

In the one-shot FQSW protocol, one starts with a *single copy* of a tripartite pure state $|\psi\rangle^{ABR}$, where the system A is with Alice, B is with Bob and R denotes the reference system. The aim is for Alice to transfer the A-part of the state to Bob and at the same time generate entanglement with him. The protocol is referred to as an ε-error one-shot FQSW protocol, if for any given $0 < \varepsilon \leqslant 1$, the error in achieving this aim is at most ε.

Any ε-error FQSW protocol for $|\psi\rangle^{ABR}$ can be assumed to have the following form. Alice does local operations on the system A and sends a quantum system (i.e. qubits) to Bob, who then performs local operations on the quantum systems in his possession. The final state of the protocol has to be ε-close (in a sense specified below) to the state $\Phi^{A_1B_1} \otimes \psi^{B'BR}$, where the subscripts have been chosen to denote which systems are in whose possession (i.e. B', B and B_1 are with Bob and A_1 is with Alice), $\Phi^{A_1B_1}$ is an MES of size $|A_1|$, and $\psi^{B'BR}$ is identical to the initial tripartite state ψ^{ABR} but with the system A now in Bob's possession. Consequently, the initial entanglement between A and R has been transferred to Bob.

The following two theorems, which together give upper and lower bounds on the minimum quantum communication cost and the maximum entanglement gain of an ε-error one-shot FQSW protocol, constitute the main results of this section.

Theorem 8 (achievability). *Fix $0 < \varepsilon \leqslant 1$. Then for any tripartite pure state ψ^{ABR}, there exists an ε-error one-shot FQSW protocol with an entanglement gain $e_\varepsilon^{(1)}$ and a quantum communication cost $q_\varepsilon^{(1)}$ bounded, respectively, by*

$$e_\varepsilon^{(1)} \geqslant \tfrac{1}{2}\left[H_0^\delta(A)_\psi + H_{\min}^\delta(A|R)_\psi\right] + \log\delta', \tag{20}$$

$$q_\varepsilon^{(1)} \leqslant \tfrac{1}{2}[H_0^\delta(A)_\psi - H_{\min}^\delta(A|R)_\psi] - \log\delta', \tag{21}$$

for some $\delta > 0$ such that $\varepsilon = 2\sqrt{5\delta'} + 2\sqrt{\delta}$ and $\delta' = \delta + \sqrt{4\sqrt{\delta} - 4\delta}$.

The proof of this theorem relies on the one-shot decoupling theorem (theorem 14), which is proved in appendix B.

Theorem 9 (converse). *Fix $0 < \varepsilon \leqslant 1$. Then, given a tripartite pure state ψ^{ABR}, the quantum communication cost $q_\varepsilon^{(1)}$ and the entanglement gain $e_\varepsilon^{(1)}$ of any ε-error one-shot FQSW protocol satisfies the following bounds:*

$$q_\varepsilon^{(1)} \geqslant \tfrac{1}{2}\left[H_{\min}^\varepsilon(A)_\psi - H_{\min}^{\bar\varepsilon}(A|R)_\psi\right] - \log\tfrac{\sqrt{2}}{\varepsilon}, \tag{22}$$

$$e_\varepsilon^{(1)} \leqslant q_\varepsilon^{(1)} + H_{\min}^{\bar\varepsilon}(A|R)_\psi + \log\frac{2}{\varepsilon^2}, \tag{23}$$

where $\bar\varepsilon := 3(\varepsilon + \sqrt{3\sqrt{\varepsilon}})$.

The proofs of theorems 8 and 9 are given in section 5.

3.2. Optimality of the rates in the asymptotic independent and identically distributed scenario

Here we prove how the known achievable rates for the FQSW in the asymptotic IID scenario can be recovered from theorems stated above. We also prove explicitly that these rates are indeed optimal [14].

Let $\psi_n^{ABR} := (\psi^{ABR})^{\otimes n}$ and let $q_{\varepsilon,n}^{(1)}$ and $e_{\varepsilon,n}^{(1)}$, respectively, denote the quantum communication cost and entanglement gain of an ε-error one-shot FQSW for the state ψ_n^{ABR}. Then the optimal rates of quantum communication and entanglement gain in the asymptotic IID scenario can be respectively defined in terms of $q_{\varepsilon,n}^{(1)}$ and $e_{\varepsilon,n}^{(1)}$ as follows:

$$q^\infty := \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}q_{\varepsilon,n}^{(1)} \tag{24}$$

and

$$e^\infty := \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}e_{\varepsilon,n}^{(1)}. \tag{25}$$

Theorem 10. *The optimal rates of quantum communication cost and entanglement gain for the FQSW protocol for a tripartite pure state ψ^{ABR} in the asymptotic IID scenario are, respectively, given by the following:*

$$q^\infty = \tfrac{1}{2}I(A:R)_\psi; \qquad e^\infty = \tfrac{1}{2}I(A:B)_\psi. \tag{26}$$

Proof.

To prove the above theorem we make use of the following relation (theorem 1 of [47]): $\forall \rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$,

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H^{\varepsilon}_{\min}(A|B)_{\rho^{\otimes n}} = H(A|B)_{\rho} \tag{27}$$

and the following identity given by lemma 16:

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H^{\varepsilon}_{0}(A)_{\rho^{\otimes n}} = H(A)_{\rho}. \tag{28}$$

In the above, $H(A)_\rho := -\mathrm{tr}\,\rho^A \log \rho^A$ is the von Neumann entropy of ρ^A, and $H(A|B)_\rho := H(AB)_\rho - H(A)_\rho$.

We first show that the upper and lower bounds for the quantum communication cost converge to the quantity $\frac{1}{2}I(A:R)_\psi$. We have

$$\begin{aligned} q^{\infty} :&= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}q^{(1)}_{\varepsilon,n} \\ &\leqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\tfrac{1}{2}[H^{\delta}_{0}(A)_{\psi_n} - H^{\delta}_{\min}(A|R)_{\psi_n}] - \log\delta'\right) \\ &= \tfrac{1}{2}[H(A)_\psi - H(A|R)_\psi] \\ &= \tfrac{1}{2}I(A:R)_\psi. \end{aligned} \tag{29}$$

The first line follows from the definition of q^{∞} in (24). The second line follows from the upper bound for $q^{(1)}_{\varepsilon,n}$ in theorem 8. The third line follows from the identities (27) and (28) and the fact that the $(\log\delta')/n$ term clearly vanishes as $n\to\infty$. Similarly, the lower bound for $q^{(1)}_{\varepsilon,n}$ in theorem 9 gives

$$\begin{aligned} q^{\infty} :&= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}q^{(1)}_{\varepsilon,n} \\ &\geqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}[H^{\varepsilon}_{\min}(A)_{\psi_n} - H^{\bar{\varepsilon}}_{\min}(A|R)_{\psi_n}] - \log\frac{\sqrt{2}}{\varepsilon}\right) \\ &= \tfrac{1}{2}I(A:R)_\psi. \end{aligned} \tag{30}$$

Next, we can show that the upper and lower bounds for entanglement gain converge to the quantity $\frac{1}{2}I(A:B)_\psi$. Similarly, from (25) and the lower bound for $e^{(1)}_{\varepsilon,n}$ in theorem 8, we have

$$\begin{aligned} e^{\infty} :&= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}e^{(1)}_{\varepsilon,n} \\ &\geqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}[H^{\delta}_{0}(A)_{\psi_n} + H^{\delta}_{\min}(A|R)_{\psi_n}] + \log\delta'\right) \\ &= \tfrac{1}{2}[H(A)_\psi + H(A|R)_\psi] \\ &= \tfrac{1}{2}I(A:B)_\psi. \end{aligned} \tag{31}$$

Finally, the upper bound for $e^{(1)}_{\varepsilon,n}$ in theorem 9 gives

$$
\begin{aligned}
e^{\infty} :&= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}e^{(1)}_{\varepsilon,n} \\
&\leqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\left[q^{(1)}_{\varepsilon,n}+H^{\bar{\varepsilon}}_{\min}(A|R)_{\psi_n}\right]+\log\frac{2}{\varepsilon^2}\right) \\
&= \tfrac{1}{2}I(A:R)_{\psi}+H(A|R)_{\psi} \qquad (32)\\
&= \tfrac{1}{2}I(A:B)_{\psi}. \qquad (33)
\end{aligned}
$$

□

3.3. Optimal rate of one-shot quantum communication

Our result (theorem 8) on the one-shot FQSW can be employed to provide a convenient characterization of the ε-error one-shot quantum capacity of a noisy channel, entirely in terms of the smooth max-entropy. We consider this result to be an improvement over previously obtained results [38] for reasons given in section 4. Before stating our result we first describe the protocol of quantum communication that we are considering, and define the ε-error one-shot quantum capacity.

The protocol [38]. Given a quantum channel $\mathcal{N}^{A'\to B}$, let $\mathcal{H}_M$ be an m-dimensional subspace of its input Hilbert space $\mathcal{H}_{A'}$, and let $0<\varepsilon\leqslant 1$ be a fixed positive constant. Alice prepares a MES $|\Phi^{A'A}_{\mathcal{M}}\rangle \in \mathcal{M}'\otimes\mathcal{M}$, where $\mathcal{M}'\simeq\mathcal{M}\subset\mathcal{H}_{A'}\simeq\mathcal{H}_A$, and sends the part A' through the channel $\mathcal{N}^{A'\to B}$ to Bob. Bob is allowed to perform any decoding operation (CPTP map) on the state that he receives. The final objective is for Alice and Bob to end up with a shared state that is nearly maximally entangled over $\mathcal{M}'\otimes\mathcal{M}$, its overlap with $|\Phi^{A'A}_{\mathcal{M}}\rangle$ being at least $(1-\varepsilon^2)$. There is no classical communication possible between Alice and Bob. In this scenario, the one-shot ε-error quantum capacity of the channel $\mathcal{N}^{A'\to B}$ is defined as follows.

Definition 11 (One-shot ε-error quantum capacity). *Given a quantum channel $\mathcal{N}:\mathcal{D}(\mathcal{H}_{A'})\mapsto\mathcal{D}(\mathcal{H}_B)$ and a real number $0<\varepsilon\leqslant 1$, the one-shot ε-error quantum capacity of $\mathcal{N}^{A'\to B}$ is defined as follows:*

$$Q^{(1)}_{\varepsilon}(\mathcal{N}) := \max\{\log m : \mathsf{F}_{\mathrm{ent}}(\mathcal{N};m)\geqslant 1-\varepsilon^2\}, \qquad (34)$$

where

$$\mathsf{F}_{\mathrm{ent}}(\mathcal{N};m) := \max_{\substack{\mathcal{H}_M\subseteq\mathcal{H}_A\\ \dim\mathcal{H}_M=m}}\max_{\mathcal{D}}\langle\Phi^{A'A}_{\mathcal{M}}|(\mathrm{id}\otimes\mathcal{D}\circ\mathcal{N})(\Phi^{A'A}_{\mathcal{M}})|\Phi^{A'A}_{\mathcal{M}}\rangle,$$

with $\mathcal{D}^{B\to A'}$ being a decoding CPTP map.

Theorem 12. *For any $0<\varepsilon\leqslant 1$, the one-shot ε-error quantum capacity of a noisy channel, $\mathcal{N}\equiv\mathcal{N}^{A'\to B}$, satisfies the following bounds:*

$$\max_{\mathcal{M}\subseteq\mathcal{H}_A}\left[-H^{\delta}_{\max}(A|B)_{\psi_{\mathcal{M}}}\right]+2\log\delta' \leqslant Q^{(1)}_{\varepsilon}(\mathcal{N}) \leqslant \max_{\mathcal{M}\subseteq\mathcal{H}_A}\left[-H^{\varepsilon}_{\max}(A|B)_{\psi_{\mathcal{M}}}\right], \qquad (35)$$

for some $\delta>0$ such that $\varepsilon := 2\sqrt{5\delta'}+2\sqrt{\delta}$ and $\delta'=\delta+\sqrt{4\sqrt{\delta}-4\delta}$, and $\psi_{\mathcal{M}}$ denotes the state

$$|\psi_{\mathcal{M}}\rangle^{ABE} := (\mathbb{I}_A\otimes U^{A'\to BE}_{\mathcal{N}})|\Phi^{AA'}_{\mathcal{M}}\rangle. \qquad (36)$$

In the above, $U_{\mathcal{N}}^{A'\to BE}$ *denotes a Stinespring isometry realizing the channel, and* $|\Phi_{\mathcal{M}}^{AA'}\rangle$ *is a MES of rank* m $(=\dim\mathcal{M})$ *in* $\mathcal{H}_A\otimes\mathcal{H}_{A'}$, $\mathcal{M}\subseteq\mathcal{H}_A$.

Proof.

The lower bound in (35) follows from the RI (60) given in section 4. The upper bound in (35) for the ε-error one-shot quantum capacity $Q_\varepsilon^{(1)}(\mathcal{N})$ can be proved as follows. Denote by $\omega^{AA'} := (\mathrm{id}_A\otimes\mathcal{D}^{B\to A'})(\psi_{\mathcal{M}}^{AB})$ Bob's decoded state, where $\psi_{\mathcal{M}}^{AB}$ is the channel output defined through (36). For any ε-error one-shot quantum communication, we have

$$\Phi_{\mathcal{M}}^{AA'}\in\mathcal{B}^\varepsilon(\omega^{AA'}). \tag{37}$$

Then an upper bound for $Q_\varepsilon^{(1)}(\mathcal{N})$ can be obtained as follows:

$$\begin{aligned}\log m &= -H_{\max}(A|A')_{\Phi_{\mathcal{M}}}\\ &\leqslant \max_{\bar{\sigma}^{AA'}\in\mathcal{B}^\varepsilon(\omega^{AA'})}\left[-H_{\max}(A|A')_{\bar{\sigma}}\right]\\ &= -H_{\max}^\varepsilon(A|A')_\omega\leqslant -H_{\max}^\varepsilon(A|B)_{\psi_{\mathcal{M}}}.\end{aligned} \tag{38}$$

The first inequality follows from (37), and the second inequality follows from the data-processing inequality for ε-smooth max-entropy (lemma 18). □

It is interesting to compare theorem 12 with theorem 1 of [38]. In the latter, the lower and upper bounds on the one-shot ε-error quantum capacity were given in terms of *different* smoothed versions of the entropic quantity $H_0(A|B)_\rho$ defined by (16). The lower bound was given in terms of the quantity $[-\tilde{H}_0^\varepsilon(A|B)_{\psi_{\mathcal{M}}}]$, where

$$\tilde{H}_0^\varepsilon(A|B)_\rho := \min_{\bar{\rho}^{AB}\in\mathcal{B}^\varepsilon(\rho^{AB})} H_0(A|B)_{\bar{\rho}} \tag{39}$$

is related to $H_{\max}^\varepsilon(A|B)_\rho$ through lemma 22, whereas the upper bound was given by an operator-smoothed version of $[-H_0(A|B)_{\psi_{\mathcal{M}}}]$ (for details see [38]). In contrast, our theorem 12 has the advantage of being given entirely in terms of a single quantity, namely $[-H_{\max}^\varepsilon(A|B)_{\psi_{\mathcal{M}}}]$.

We now consider the case of a memoryless quantum channel $\mathcal{N}^{A'\to B}$. Let us denote the output of n successive, independent uses of the channel, corresponding to the input state $|\Phi_{\mathcal{M}_n}^{A'A}\rangle\in\mathcal{M}_n'\otimes\mathcal{M}_n$, where $\mathcal{M}_n\subset\mathcal{H}_A^{\otimes n}$, by

$$\psi_{\mathcal{M}_n}^{ABE} := (\mathbb{I}_A\otimes U_{\mathcal{N}}^{A'\to BE})^{\otimes n}(\Phi_{\mathcal{M}_n}^{A'A}). \tag{40}$$

Let $Q_\varepsilon^{(1)}(\mathcal{N}^{\otimes n})$ denote the one-shot ε-error quantum capacity of the channel $\mathcal{N}^{\otimes n}$. The quantum capacity $Q^\infty(\mathcal{N})$ of a memoryless channel $\mathcal{N}$, which is evaluated in the limit of asymptotically many uses of the channel, can be defined in terms of $Q_\varepsilon^{(1)}(\mathcal{N})$ as follows:

$$Q^\infty(\mathcal{N}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}Q_\varepsilon^{(1)}(\mathcal{N}^{\otimes n}).$$

Next we prove how the known expression [6, 38] of the quantum capacity $Q^\infty(\mathcal{N})$ can be recovered from theorem 12.

Theorem 13. *The quantum capacity of a memoryless channel* $\mathcal{N}$ *is given by the following:*

$$Q^\infty(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_{\mathcal{M}_n\subseteq\mathcal{H}_A^{\otimes n}} I(A\rangle B)_{\psi_{\mathcal{M}_n}}, \tag{41}$$

where $\psi_{\mathcal{M}_n}^{ABE}$ *is defined in (40), and* $I(A\rangle B)_{\psi_{\mathcal{M}_n}}$ *is the coherent information (8) of the state* $\psi_{\mathcal{M}_n}$.

Proof.

Note that

$$
\begin{aligned}
Q^{\infty}(\mathcal{N}) &:= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}Q^{(1)}_{\varepsilon}(\mathcal{N}^{\otimes n})\\
&\leqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\max_{\mathcal{M}_n\subseteq\mathcal{H}_A^{\otimes n}}\left[-H^{\varepsilon}_{\max}(A|B)_{\psi_{\mathcal{M}_n}}\right]\right)\\
&\leqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\max_{\mathcal{M}_n\subseteq\mathcal{H}_A^{\otimes n}}\left[-H(A|B)_{\psi_{\mathcal{M}_n}}+8\varepsilon\log|A_{\mathcal{M}_n}|+2h(2\varepsilon)\right]\right)\\
&= \lim_{n\to\infty}\frac{1}{n}\left(\max_{\mathcal{M}_n\subseteq\mathcal{H}_A^{\otimes n}}\left[-H(A|B)_{\psi_{\mathcal{M}_n}}\right]\right).
\end{aligned}
\tag{42}
$$

The first inequality follows from the upper bound in theorem 12. The second inequality follows from the fact that $|A_{\mathcal{M}_n}|$ denotes the dimension of the Hilbert space on which the state $\psi^A_{\mathcal{M}_n}$ is supported and from lemma 5 in [37], which states that for $0<\varepsilon\leqslant 1$ and $\rho^{AB}\in\mathcal{D}(\mathcal{H}_A\otimes\mathcal{H}_B)$

$$H^{\varepsilon}_{\max}(A|B)_{\rho}\geqslant H(A|B)_{\rho}-8\varepsilon\log|A|-2h(2\varepsilon),$$

where $h(\varepsilon)=-\varepsilon\log\varepsilon-(1-\varepsilon)\log(1-\varepsilon)$.

Similarly, from the lower bound in theorem 5 we have

$$
\begin{aligned}
Q^{\infty}(\mathcal{N}) &:= \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}Q^{(1)}_{\varepsilon}(\mathcal{N}^{\otimes n})\\
&\geqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\max_{\mathcal{M}_n\subseteq\mathcal{H}_A^{\otimes n}}\left[-H^{\delta}_{\max}(A|B)_{\psi_{\mathcal{M}_n}}\right]+2\log\delta'\right)\\
&\geqslant \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left(\max_{\mathcal{M}^{\otimes n}\subseteq\mathcal{H}_A^{\otimes n}}\left[-H^{\delta}_{\max}(A|B)_{\psi_{\mathcal{M}}^{\otimes n}}\right]+2\log\delta'\right)\\
&= \max_{\mathcal{M}\subseteq\mathcal{H}_A}\left[-H(A|B)_{\psi_{\mathcal{M}}}\right].
\end{aligned}
\tag{43}
$$

The second inequality follows since the maximization is over a smaller set. The last equality follows from the fact that $(\log\delta')/n$ vanishes as $n\to\infty$, and from the following relation (theorem 1 of [47]): $\forall\rho^{AB}\in\mathcal{D}(\mathcal{H}_A\otimes\mathcal{H}_B)$,

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H^{\varepsilon}_{\max}(A|B)_{\rho^{\otimes n}}=H(A|B)_{\rho}. \tag{44}$$

We can then obtain the lower bound for (41) by noting that $I(A\rangle B)_{\psi_{\mathcal{M}_n}}=-H(A|B)_{\psi_{\mathcal{M}_n}}$ and using the standard blocking argument. □

4. Resource inequalities and the children protocols

As shown in [17, 25], the FQSW protocol in the asymptotic IID scenario can be conveniently expressed using a RI [17, 18, 25]. Before stating it, let us briefly recall the notation used in the RI framework and how one interprets the inequalities.

Some of the basic units (referred to as *unit* asymptotic resources) of the RI framework are the following: $[c\to c]$ represents one bit of classical communication from Alice (the sender) to Bob (the receiver); $[q \to q]$ represents one qubit of quantum communication from Alice to Bob; $[qq]$ represents an ebit shared between Alice and Bob. For a more complete list of units, see [18].

The original mother protocol (or quantum communication-assisted entanglement distillation), of which the FQSW is a generalization, is given by the following RI [17]:

$$\langle \psi^{AB} \rangle + \tfrac{1}{2} I(A:R)_\psi [q \to q] \geqslant \tfrac{1}{2} I(A:B)_\psi [qq]. \tag{45}$$

It states that n copies of a state ψ^{AB} shared between Alice and Bob (with purification ψ^{ABR}, where R denotes the reference system) can be converted into $\frac{1}{2} I(A:B)_\psi$ EPR pairs per copy, under the condition that Alice is allowed to communicate with Bob by sending him qubits at a rate $\frac{1}{2} I(A:R)_\psi$ per copy. Minor inaccuracies in the final state are allowed, provided they vanish asymptotically, i.e. as $n \to \infty$. The one-shot analogue of the RI (41) is given by (52) below. In contrast, the RI for the FQSW protocol is given by [25]

$$\langle U^{S\to AB} : \psi^S \rangle + \tfrac{1}{2} I(A:R)_\psi [q \to q] \geqslant \tfrac{1}{2} I(A:B)_\psi [qq] + \langle \mathrm{id}^{S\to B} : \psi^S \rangle. \tag{46}$$

In the above, $U^{S\to AB}$ is an isometry taking the system S to AB and signifies that a state is distributed between Alice and Bob, whereas the identity map $\mathrm{id}^{S\to B}$ on the right-hand side signifies that the same state is given to Bob alone. Thus the inequality expresses that Alice transfers her part of the initial state to Bob. More precisely, it states that starting from the state $|\psi^{ABR}\rangle^{\otimes n}$, Alice can transfer her part of the state (and hence also the entanglement that she shares with the reference system R) to Bob by using quantum communication at the rate of $\frac{1}{2} I(A:R)_\psi$, and they can simultaneously distill EPR pairs at the rate $\frac{1}{2} I(A:B)_\psi$. Again, minor inaccuracies in the final state are allowed, provided that they vanish asymptotically. The one-shot version of this RI is given by (47). Note that resource inequalities provide statements about achievable rates of protocols, but do not ensure the optimality of these rates.

Next we state one-shot resource inequalities for the FQSW and some of its children protocols. A more exhaustive study of one-shot resource inequalities of all the different children protocols will be carried out in a later paper [55].

The RI for the one-shot FQSW for the state $|\psi\rangle^{ABR}$ is given by

$$\langle U^{S\to AB} : \psi^S \rangle + q_\varepsilon^{(1)} [q \to q] \geqslant_\varepsilon e_\varepsilon^{(1)} [qq] + \langle \mathrm{id}^{S\to B} : \psi^S \rangle, \tag{47}$$

where the quantum communication cost $q_\varepsilon^{(1)}$ and entanglement gain $e_\varepsilon^{(1)}$ are given by

$$q_\varepsilon^{(1)} = \tfrac{1}{2} \left[H_0^\delta(A)_\psi - H_{\min}^\delta(A|R)_\psi \right] - \log \delta', \tag{48}$$

$$e_\varepsilon^{(1)} = \tfrac{1}{2} \left[H_0^\delta(A)_\psi + H_{\min}^\delta(A|R)_\psi \right] + \log \delta', \tag{49}$$

for some $\delta > 0$ such that $\varepsilon = 2\sqrt{5\delta'} + 2\sqrt{\delta}$ and $\delta' = \delta + \sqrt{4\sqrt{\delta} - 4\delta}$. This follows directly from theorem 8. Note that in (47) the notation $\geqslant_\varepsilon$ is used to denote that we are considering ε-error one-shot FQSW.

The RI for the one-shot FQSW in (47) yields the following RI for the one-shot state merging protocol when combined with the RI for teleportation, $2[c \to c] + [qq] \geqslant [q \to q]$ [18]:

$$\begin{aligned} \langle U^{S\to AB} : \psi^S \rangle + q_\varepsilon^{(1)} [q \to q] + 2q_\varepsilon^{(1)} [c \to c] &\geqslant_\varepsilon e_\varepsilon^{(1)} [qq] + \langle \mathrm{id}^{S\to B} : \psi^S \rangle + 2q_\varepsilon^{(1)} [c \to c], \\ &\geqslant_\varepsilon (e_\varepsilon^{(1)} - q_\varepsilon^{(1)}) [qq] + \langle \mathrm{id}^{S\to B} : \psi^S \rangle + q_\varepsilon^{(1)} [q \to q]. \end{aligned} \tag{50}$$

In the RI (50), the $q_\varepsilon^{(1)}$ qubits of quantum communication that are employed at the start of the protocol are recovered at the end. Hence they play the role of a catalyst. Thus we can obtain the achievable *entanglement gain* $(e_\varepsilon^{(1)} - q_\varepsilon^{(1)})$ for the one-shot state merging protocol in terms of the δ-smooth conditional min-entropy $H_{\min}^\delta(A|R)_\psi$, modulo additional ε-dependent terms. Note that the entanglement gain $(e_\varepsilon^{(1)} - q_\varepsilon^{(1)})$ in (50) can also be achieved using a one-shot state merging protocol without any catalyst, a result recently announced in [39]. That the quantity $H_{\min}^\delta(A|R)_\psi$ is optimal for the one-shot ε-error state merging protocol is further justified by a corresponding converse proof given in [39]. This leads us to write one-shot resource inequalities, modulo the consideration of the catalyst, as follows (for which we replace the symbol $\geqslant_\varepsilon$ by $\tilde{\geqslant}_\varepsilon$).

State merging:

$$\langle U^{S\to AB} : \psi^S\rangle + 2q_\varepsilon^{(1)}[c \to c] \tilde{\geqslant}_\varepsilon (e_\varepsilon^{(1)} - q_\varepsilon^{(1)})[qq] + \langle \mathrm{id}^{S\to B} : \psi^S\rangle. \tag{51}$$

The RI (47) for the one-shot FQSW directly leads to the RI for the one-shot mother for the state $|\psi\rangle^{ABR}$ (if one focuses on the entanglement distillation alone and ignores the additional task of state transfer which is required in FQSW):

Mother:

$$\langle \psi^{AB}\rangle + q_\varepsilon^{(1)}[q \to q] \geqslant_\varepsilon e_\varepsilon^{(1)}[qq]. \tag{52}$$

From (52), we can obtain the RI for one-shot entanglement distillation by combining it with the RI for teleportation as follows.

Entanglement distillation:

$$\begin{aligned}
\langle \psi^{AB}\rangle + q_\varepsilon^{(1)}[q \to q] + 2q_\varepsilon^{(1)}[c \to c] &\geqslant_\varepsilon e_\varepsilon^{(1)}[qq] + 2q_\varepsilon^{(1)}[c \to c] \\
&\geqslant_\varepsilon (e_\varepsilon^{(1)} - q_\varepsilon^{(1)})[qq] + q_\varepsilon^{(1)}[q \to q] \\
&\Rightarrow \langle \psi^{AB}\rangle + 2q_\varepsilon^{(1)}[c \to c] \tilde{\geqslant}_\varepsilon (e_\varepsilon^{(1)} - q_\varepsilon^{(1)})[qq].
\end{aligned} \tag{53}$$

The quantities $q_\varepsilon^{(1)}$ and $e_\varepsilon^{(1)}$ appearing in (52) and (53) are given by (48) and (49), respectively. We thus obtain an achievable one-shot entanglement distillation rate in terms of the δ-smooth max-entropy $[-H_{\max}^\delta(A|B)_\psi]$, modulo additional ε-dependent terms. Note that in [41] an expression for an achievable rate of the one-shot entanglement distillation, *without any catalyst*, was obtained in terms of $\tilde{H}_0^\varepsilon(A|B)_\psi$, an entropic quantity defined through (17).

Two children protocols of the mother are *noisy teleportation* and *noisy superdense coding*, which as their names suggest correspond to teleportation and superdense coding with a general entangled state ψ^{AB}. The one-shot resource inequalities for these protocols are easily obtained from (52) as follows.

Noisy teleportation:

$$\begin{aligned}
&\langle \psi^{AB}\rangle + q_\varepsilon^{(1)}[q \to q] + 2e_\varepsilon^{(1)}[c \to c] \geqslant_\varepsilon e_\varepsilon^{(1)}[qq] + 2e_\varepsilon^{(1)}[c \to c] \\
&\geqslant_\varepsilon e_\varepsilon^{(1)}[q \to q]. \\
&\Rightarrow \langle \psi^{AB}\rangle + 2e_\varepsilon^{(1)}[c \to c] \tilde{\geqslant}_\varepsilon (e_\varepsilon^{(1)} - q_\varepsilon^{(1)})[q \to q].
\end{aligned} \tag{54}$$

Noisy superdense coding:

$$\begin{aligned}
&\langle \psi^{AB}\rangle + q_\varepsilon^{(1)}[q \to q] + e_\varepsilon^{(1)}[q \to q] \geqslant_\varepsilon e_\varepsilon^{(1)}[qq] + e_\varepsilon^{(1)}[q \to q] \\
&\geqslant_\varepsilon 2e_\varepsilon^{(1)}[c \to c]. \\
&\Rightarrow \langle \psi^{AB}\rangle + (q_\varepsilon^{(1)} + e_\varepsilon^{(1)})[q \to q] \geqslant_\varepsilon 2\, e_\varepsilon^{(1)}[c \to c].
\end{aligned} \tag{55}$$

The second inequality in (54) follows from the RI for teleportation, whereas in obtaining the second inequality in (55) we have made use of the RI for superdense coding [18]:

$$[q \to q] + [qq] \geqslant 2[c \to c].$$

It has been proved in [17, 18] that the entanglement gain and quantum communication cost for the FQSW protocol in the case when asymptotically many copies of the tripartite state are shared between Alice, Bob and the reference yield the entanglement cost and the quantum communication gain for the so-called *father protocol*, which is the protocol for entanglement-assisted quantum communication through a noisy channel. This is also the case for the one-shot regime, as explained below. Applying superdense coding after executing one instance of the father protocol allows us to trade quantum for classical communication and therefore results in one-shot entanglement-assisted classical communication through the noisy channel and yields a lower bound on the corresponding capacity. This mimics the method of determining an achievable rate for entanglement-assisted classical communication in the asymptotic scenario within the RI framework [17, 18]. As is natural in the one-shot scenario, we allow for a finite error (say ε) for both the FQSW and father protocols.

The RI for the one-shot FQSW yields a RI for the following entanglement-assisted quantum communication (or father) protocol. Alice initially shares two MESs—one ($\Phi^{A_1B_1}$) with Bob and the other (Φ^{A_0R}) with a reference system R that is inaccessible to both her and Bob. The MES $\Phi^{A_1B_1}$ acts as a resource of prior shared entanglement between Alice and Bob. Alice's goal is to send the quantum system A_0 to Bob through a noisy quantum channel $\mathcal{N}^{A'\to B}$ so that finally Bob shares a MES with the reference system. To achieve this goal she does an encoding isometry W on the systems A_0 and A_1 in her possession (see figure 1(a)). The output A' of this isometry is subjected to the Stinespring isometry $U_{\mathcal{N}}^{A'\to BE}$ realizing the noisy channel $\mathcal{N}^{A'\to B}$. Let us denote the resulting pure state by ψ^{ABE}, where $A \equiv RB_1$.

In order to see how one can relate the one-shot father protocol to the one-shot FQSW protocol, let us consider the state ψ^{ABE} of the one-shot father protocol to be the initial tripartite state of an ε-error one-shot FQSW protocol.

The one-shot FQSW theorem (theorem 8) tells us that there exists a unitary operator $U^{A\to B_1R}$ and an isometry $V^{B_1B\to B_0B'}$, such that the state resulting from their successive actions, i.e. the state

$$(V^{B_1B\to B_0B'} \circ U^{A\to B_1R})\psi^{ABE}(V^{B_1B\to B_0B'} \circ U^{A\to B_1R})^{\dagger},$$

is ε-close to the state

$$\Phi^{B_0R} \otimes \psi^{B'E},$$

with the systems B_0 and B' being in Bob's possession, and $\psi^{B'E}$ being a purification of the state $\psi^E := \mathrm{tr}_{AB}\psi^{ABE}$. [2] The protocol corresponding to this theorem consists of performing the unitary $U^{A\to B_1R}$ on the system A and sending the system B_1 to Bob, who then performs the isometry $V^{B_1B\to B_0B'}$ on the composite system BB_1. The number of qubits sent in the protocol is hence equal to $\log|B_1|$ and the number of ebits distilled is $\log|A_0| = \log|B_0|$. [3] Note that at the end of the protocol, Bob shares a state with the reference system R which is ε-close to a MES,

[2] Here the system B' denotes the composite systems AB of the state ψ^{ABE}. Furthermore, one can think of the state $\psi^{B'E}$ as identical to the state ψ^{ABE}.

[3] Note that in the setting of figure 1(a), sending the quantum register B_1 to Bob is not necessary since it is already in Bob's possession.

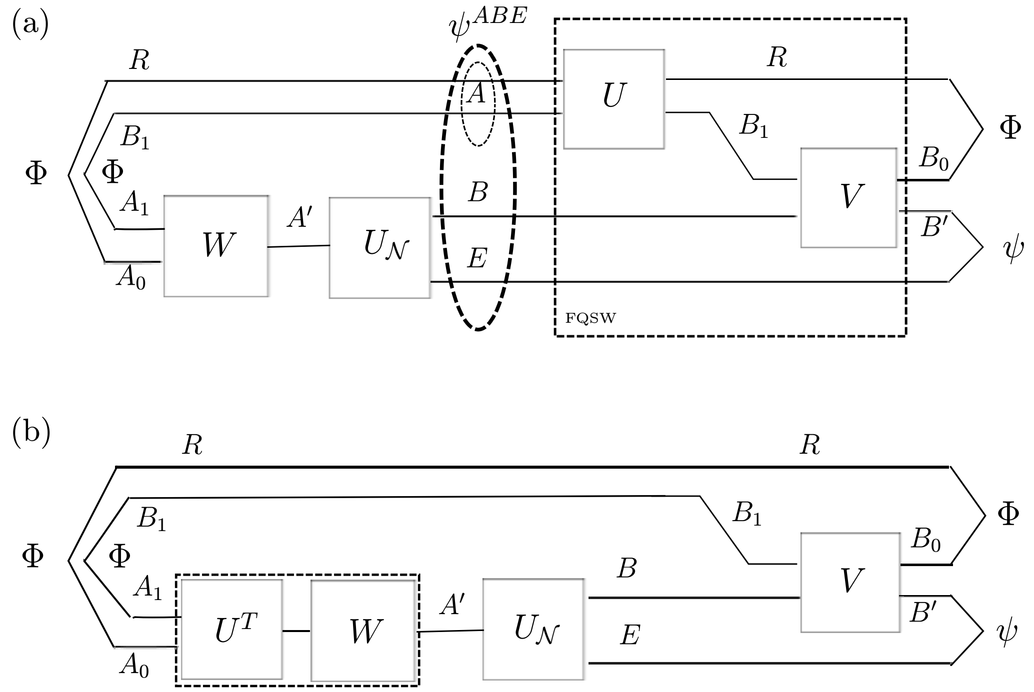

Figure 1. Relating the one-shot FQSW and father protocols. (a) Applying the one-shot FQSW protocol to the channel output state ψ^{ABE} of the father protocol results in Bob and the reference system R sharing a state Φ^{RB_0} (the superscript B_0 denotes that the A_0 system has been transferred to Bob), which is ε-close to a MES—the desired outcome of the father protocol. However, the FQSW protocol requires acting on the reference system, which is inaccessible to Alice and Bob. (b) Circumventing the problem of implementing the unitary U: note that performing the unitary U on system $A \equiv RB_1$ in the one-shot ε-error FQSW protocol in (a) is equivalent to Alice performing U^T on system A_0A_1 (since RB_1 and A_0A_1 are in an MES) before employing her encoding isometry W.

and thus by using the ε-error one-shot FQSW protocol on the state ψ^{ABE} of the father protocol, the aim of the father protocol is achieved. Effectively, $\log|A_0|$ qubits have been transmitted from Alice to Bob and this therefore quantifies the quantum communication gain of the protocol.

Note, however, that there is a caveat to the above argument. Since $A \equiv B_1R$, the unitary $U \equiv U^{A\to B_1R}$ requires acting on the reference system R. However, R is inaccessible to Alice and Bob and hence the unitary cannot be implemented. This problem is easily overcome by noting that performing the unitary U on system $A \equiv RB_1$ in the one-shot ε-error FQSW protocol in figure 1(a) is equivalent to Alice performing U^T on system A_0A_1 since RB_1 and A_0A_1 are in a MES. In this way, a complete one-shot ε-error entanglement-assisted quantum communication protocol with encoding $W \circ U^T$ and decoding V is established (see figure 1(b)). Note that the entanglement cost of this protocol (i.e. the required prior shared entanglement between Alice and Bob) is $\log|B_1|$ ebits, which is equal to the quantum communication cost of the one-shot FQSW protocol, and the quantum communication gain of the one-shot father protocol is equal to $\log|A_0|$, which in turn is equal to the entanglement gain of the one-shot FQSW. These considerations yield the following RI for the one-shot ε-error father protocol through a noisy quantum channel $\mathcal{N}^{A'\to B}$.

Father:

$$\langle \mathcal{N} \rangle + \tilde{e}_\varepsilon^{(1)}[qq] \geqslant_\varepsilon \tilde{q}_\varepsilon^{(1)}[q \to q], \tag{56}$$

where

$$\tilde{e}_\varepsilon^{(1)} = \tfrac{1}{2}\left[H_0^\delta(A)_\psi - H_{\min}^\delta(A|E)_\psi\right] - \log \delta', \tag{57}$$

$$\tilde{q}_\varepsilon^{(1)} = \tfrac{1}{2}\left[H_0^\delta(A)_\psi + H_{\min}^\delta(A|E)_\psi\right] + \log \delta'. \tag{58}$$

Here, ψ denotes the state $|\psi\rangle^{ABE} = U_{\mathcal{N}}^{A'\to BE}|\varphi\rangle^{AA'}$, with $U_{\mathcal{N}}^{A'\to BE}$ being a Stinespring isometry realizing the channel, and $|\varphi\rangle^{AA'}$ being some pure state in $\mathcal{H}_A \otimes \mathcal{H}_{A'}$.

The RI (56) for the one-shot father protocol readily yields an RI for the one-shot entanglement-assisted classical communication through a noisy quantum channel, which in turn yields a lower bound on the one-shot entanglement-assisted classical capacity. This can be seen as follows. Combining (56) with the RI for superdense coding, yields the following RI for one-shot entanglement-assisted classical communication through a noisy channel $\mathcal{N} \equiv \mathcal{N}^{A'\to B}$.

Entanglement-assisted classical communication:

$$\begin{aligned}\langle \mathcal{N} \rangle + \tilde{q}_\varepsilon^{(1)}[qq] + \tilde{e}_\varepsilon^{(1)}[qq] &\geqslant_\varepsilon \tilde{q}_\varepsilon^{(1)}[q \to q] + \tilde{q}_\varepsilon^{(1)}[qq] \\ &\geqslant_\varepsilon 2\tilde{q}_\varepsilon^{(1)}[c \to c] \\ \Rightarrow \langle \mathcal{N} \rangle + (\tilde{q}_\varepsilon^{(1)} + \tilde{e}_\varepsilon^{(1)})[qq] &\geqslant_\varepsilon 2\tilde{q}_\varepsilon^{(1)}[c \to c].\end{aligned} \tag{59}$$

Combining (56) with the trivial RI $[q \to q] \geqslant [qq]$, we can also obtain the RI for the one-shot quantum communication through a noisy channel $\mathcal{N} \equiv \mathcal{N}^{A'\to B}$.

Quantum communication:

$$\langle \mathcal{N} \rangle \tilde{\geqslant}_\varepsilon Q_\varepsilon^{(1)}[q \to q], \tag{60}$$

where

$$\begin{aligned}Q_\varepsilon^{(1)} :&= \tilde{q}_\varepsilon^{(1)} - \tilde{e}_\varepsilon^{(1)} \\ &= H_{\min}^\delta(A|E)_\psi + 2\log\delta' \\ &= -H_{\max}^\delta(A|B)_\psi + 2\log\delta'.\end{aligned} \tag{61}$$

In (61) the last equality follows from the duality relation (11) between min- and max-entropy. By using a decoupling theorem analogous to theorem 14, we can prove that $Q_\varepsilon^{(1)}$ is indeed an achievable rate for the one-shot ε-error quantum communication through the channel $\mathcal{N}$, and this leads to the lower bound in theorem 12.

Another important protocol, of which the FQSW is a primitive, is state redistribution. In its one-shot version, the protocol is as follows. Alice and Bob share a tripartite state ρ^{ABC}, where Alice holds systems A and C, and Bob holds system B. Let the state ρ^{ABC} be purified by a reference system R, the pure state being denoted as $|\psi\rangle^{ABCR}$. The task is for Alice to transfer her system A to Bob while keeping the overall purification $|\psi\rangle^{ABCR}$ unchanged (possibly with the help of prior shared entanglement). Our results on the one-shot FQSW imply that Alice can achieve this task (up to a finite accuracy $(1-\varepsilon)$) by sending

$$\tfrac{1}{2}I_{\max}^\varepsilon(A:R|B)_\psi := \tfrac{1}{2}\left[H_{\max}^\varepsilon(A|B)_\psi - H_{\min}^\varepsilon(A|RB)_\psi\right]$$

number of qubits to Bob, modulo an additional ε-dependent factor. The proof of this statement and its optimality will be presented in a forthcoming paper [56].

5. Proofs of theorems 8 and 9

5.1. Achievability proof of the one-shot FQSW protocol

The proof employs the following one-shot decoupling theorem, which is proved in appendix B for completeness. Various versions of the proofs can be found in, e.g. [27, 38, 39, 43].

Theorem 14 (one-shot decoupling). *Fix $0 < \varepsilon \leqslant 1$, and $\rho^{AR} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_R)$. Let A_1A_2 be a decomposition of the system A. Define*

$$\sigma^{A_1R}(U) = \mathrm{tr}_{A_2}\left[(U \otimes \mathbb{I}_R)\rho^{AR}(U \otimes \mathbb{I}_R)^\dagger\right], \tag{62}$$

where U be a unitary acting on system A. If

$$\log|A_1| \leqslant \tfrac{1}{2}[\log|A| + H_{\min}^{\varepsilon}(A|R)_\rho] + \log\varepsilon \tag{63}$$

then

$$\int_{U(A)} \|\sigma^{A_1R}(U) - \tau^{A_1} \otimes \rho^R\|_1 \, \mathrm{d}U \leqslant 5\varepsilon, \tag{64}$$

where dU is the Haar measure over the unitaries on system A.

Proof of theorem 8. Fix $0 < \varepsilon \leqslant 1$ and a pure state $|\psi\rangle^{ABR}$. For any $0 < \delta \leqslant 1$ to be specified later, let Q be the operator for which the minimum in the definition

$$H_0^\delta(A)_\psi := \min_{\substack{0 \leqslant Q \leqslant \mathbb{I}_A \\ \mathrm{tr}Q\psi^A \geqslant 1-\delta}} \log \mathrm{tr}\, \Pi_{\sqrt{Q}\psi^A\sqrt{Q}} \tag{65}$$

is achieved. Define

$$\psi_Q^{ABR} := (\sqrt{Q} \otimes \mathbb{I}_{BR})\psi^{ABR}(\sqrt{Q} \otimes \mathbb{I}_{BR}),$$

and let ψ_Q^{AR}, ψ_Q^A denote its reduced states. It follows from the gentle measurement lemma, lemma 1, that

$$\|\psi_Q^{ABR} - \psi^{ABR}\| \leqslant 2\sqrt{\delta},$$

since $\mathrm{tr}[(Q \otimes \mathbb{I}_{BR})\psi^{ABR}] \geqslant 1 - \delta$.

Denote the dimension of Hilbert space on which the state ψ_Q^A is supported by $|A_Q|$. Due to the choice of Q in (65), we have

$$\log|A_Q| := \log \mathrm{tr}\, \Pi_{\psi_Q^A} = H_0^\delta(A)_\psi,$$

where $\Pi_{\psi_Q^A}$ denotes the projector onto the support of ψ_Q^A. Applying the one-shot decoupling theorem (theorem 14) to the state ψ_Q^{AR} shows that, for any $\delta' \equiv \delta + \sqrt{4\sqrt{\delta} - 4\delta}$,

$$\log|A_1| \leqslant \tfrac{1}{2}\left[\log|A_Q| + H_{\min}^{\delta'}(A|R)_{\psi_Q}\right] + \log\delta',$$

there exists an isometry $U^{A\to A_1A_2}$ such that if Alice acts on her share of the tripartite pure state ψ_Q^{ABR} with it and sends the system A_2 to Bob, then the state of the system A_1, which she retains, is decoupled from the state of the reference system R, i.e.

$$\|\Omega_Q^{A_1R}-\tau^{A_1}\otimes\psi_Q^R\|_1\leqslant 5\delta',$$

where $\Omega_Q^{A_1R}$ is the reduced density matrix of the following pure state:

$$|\psi_Q\rangle^{A_1A_2BR}=U^{A\to A_1A_2}|\psi_Q\rangle^{ABR}.$$

Note that to send the system A_2 to Bob, Alice needs to transmit $\log|A_2|$ qubits to Bob. We denote the resulting pure state by $|\Omega_Q\rangle^{A_1B_2BR}$, where we have replaced A_2 by B_2 since it is now in Bob's possession.

Note that since $\Phi^{A_1B_1}\otimes\psi_Q^{ABR}$ is a purification of the state $\tau^{A_1}\otimes\psi_Q^R$, and all purifications are related by isometries, it follows from Uhlmann's theorem [54] that there must exist an isometry $\mathcal{V}^{B_2B\to B_1B'B}$, with $\mathcal{H}_{B_1}\simeq\mathcal{H}_{A_1}$, which Bob can employ on the systems B_2 and B now in his possession to obtain the following decoded state

$$|\hat{\Omega}_Q\rangle^{A_1B_1B'BR}=\mathcal{V}^{BB_2\to B_1B'B}|\Omega_Q\rangle^{A_1B_2BR},$$

such that it is ε-close to the optimal state $\Phi^{A_1B_1}\otimes\psi^{B'BR}$:

$$\begin{aligned}\|\hat{\Omega}_Q^{A_1B_1B'BR}-\Phi^{A_1B_1}\otimes\psi^{B'BR}\|&\leqslant\|\hat{\Omega}_Q^{A_1B_1B'BR}-\Phi^{A_1B_1}\otimes\psi_Q^{B'BR}\|\\&+\|\Phi^{A_1B_1}\otimes\psi_Q^{B'BR}-\Phi^{A_1B_1}\otimes\psi^{B'BR}\|\leqslant 2\sqrt{5\delta'}+2\sqrt{\delta}:=\varepsilon.\end{aligned}\tag{66}$$

Note that since systems A_1 and B_1 are in an MES, the protocol results in the generation of $e_\varepsilon^{(1)}$ ebits of entanglement, where

$$\begin{aligned}e_\varepsilon^{(1)}:=&\ \log|A_1|=\tfrac{1}{2}[\log|A_Q|+H_{\min}^{\delta'}(A|R)_{\psi_Q}]+\log\delta'\\\geqslant&\ \tfrac{1}{2}[H_0^\delta(A)_\psi+H_{\min}^\delta(A|R)_\psi]+\log\delta'.\end{aligned}\tag{67}$$

The above inequality follows because $\mathcal{B}^\delta(\psi^{AR})\subset\mathcal{B}^{\delta'}(\psi_Q^{AR})$. Further, the number of qubits that Alice needs to transmit to Bob is given by

$$\begin{aligned}q_\varepsilon^{(1)}:=&\ \log|A_2|=\log|A_Q|-\tfrac{1}{2}[\log|A_Q|+H_{\min}^{\delta'}(A|R)_{\psi_Q}]-\log\delta'\\\leqslant&\ \tfrac{1}{2}[H_0^\delta(A)_\psi-H_{\min}^\delta(A|R)_\psi]-\log\delta'.\end{aligned}\tag{68}$$

□

5.2. *Converse proof of the one-shot FQSW protocol*

Proof of theorem 9. Without loss of generality, any ε-error FQSW protocol for a tripartite pure state ψ^{ABR} can be described by a pair of encoding and decoding operations (i.e. CPTP maps)

$(\mathcal{E}, \mathcal{D})$ as follows.

(i) Alice's encoding operation $\mathcal{E}^{A\to A_1A_2}$ on the state $\psi^A = \mathrm{tr}_{BR}\,\psi^{ABR}$. Denote the state after Alice's operation by

$$|\Omega\rangle^{A_1A_2E_1BR} = U_{\mathcal{E}}^{A\to A_1A_2E_1}|\psi\rangle^{ABR}, \tag{69}$$

where $U_{\mathcal{E}}^{A\to A_1A_2E_1}$ is a Stinespring isometry of the map $\mathcal{E}^{A\to A_1A_2}$. Alice then sends system A_2 to Bob. This results in the state $|\Omega\rangle^{A_1B_2E_1BR}$, where we have replaced A_2 by B_2 since it is now in Bob's possession.

(ii) Bob's decoding map $\mathcal{D}^{B_2B\to B_1B'B}$. Denote Bob's output state by $\hat{\Omega}^{A_1B_1B'BR} := \mathcal{D}^{B_2B\to B_1B'B}(\Omega^{A_1B_2BR})$, where $\Omega^{A_1B_2BR} := \mathrm{tr}_{E_1}\,\Omega^{A_1B_2E_1BR}$ and $\hat{\Omega}^{A_1B_1B'BR}$ is the reduced density matrix of the following pure state,

$$|\hat{\Omega}\rangle^{A_1B_1B'BRE_1E_2} = U_{\mathcal{D}}^{B_2B\to B_1B'BE_2}|\Omega\rangle^{A_1B_2E_1BR}, \tag{70}$$

with $U_{\mathcal{D}}^{B_2B\to B_1B'BE_2}$ being a Stinespring isometry of $\mathcal{D}^{B_2B\to B_1B'B}$, such that

$$\|\Phi^{A_1B_1}\otimes\psi^{B'BR} - \hat{\Omega}^{A_1B_1B'BR}\|_1 \leqslant \varepsilon, \tag{71}$$

where $|\Phi\rangle^{A_1B_1}$ is the MES on systems A_1B_1.

By Uhlmann's theorem [54], there exists a pure state $\varphi^{E_1E_2}\in\mathcal{D}(\mathcal{H}_{E_1}\otimes\mathcal{H}_{E_2})$ such that

$$\|\Phi^{A_1B_1}\otimes\psi^{B'BR}\otimes\varphi^{E_1E_2} - \hat{\Omega}^{A_1B_1B'BRE_1E_2}\|_1 \leqslant 2\sqrt{\varepsilon}. \tag{72}$$

Combining (72) with the monotonicity of the trace distance under partial trace, we have

$$\|\tau^{A_1}\otimes\psi^{R}\otimes\varphi^{E_1} - \hat{\Omega}^{A_1RE_1}\|_1 \leqslant 2\sqrt{\varepsilon}, \tag{73}$$

where $\tau^{A_1} = \mathrm{tr}_{B_1}\,\Phi^{A_1B_1}$ is the completely mixed state on system A_1, $\psi^R = \mathrm{tr}_{B'B}\,\psi^{B'BR}$, and $\varphi^{E_1} = \mathrm{tr}_{E_2}\,\varphi^{E_1E_2}$. Note that $\Omega^{A_1RE_1} = \hat{\Omega}^{A_1RE_1}$ because Bob's decoding operation $\mathcal{D}^{B_2B\to B_1B'B}$ (or its corresponding isometry $U_{\mathcal{D}}^{B_2B\to B_1B'BE_2}$, which relates the pure states $|\Omega\rangle^{A_1B_2E_1BR}$ and $|\hat{\Omega}\rangle^{A_1B_1B'BRE_1E_2}$) does not affect systems A_1, R and E_1. Hence we can rewrite (73) as

$$\|\tau^{A_1}\otimes\psi^{R}\otimes\varphi^{E_1} - \Omega^{A_1RE_1}\|_1 \leqslant 2\sqrt{\varepsilon}. \tag{74}$$

□

We make use of the following lemma.

Lemma 15. *Fix $\delta \geqslant 0$ and let $\kappa := 2\sqrt{\varepsilon}$, then*

$$H_{\min}^{\delta+2\sqrt{\kappa}}(A_1E_1|R)_\Omega \geqslant H_{\min}^{\delta}(A_1E_1)_\Omega, \tag{75}$$

where $\Omega^{A_1E_1R}$ is the reduced density matrix of the pure state defined in (69).

Proof.

Using (7), we infer from (74) that

$$C(\tau^{A_1}\otimes\psi^{R}\otimes\varphi^{E_1}, \Omega^{A_1RE_1}) \leqslant \sqrt{\kappa}, \tag{76}$$

where $C(\rho,\sigma)$ is defined by (5) for any $\rho\in\mathcal{D}(\mathcal{H})$ and $\sigma\in\mathcal{D}_{\leqslant}(\mathcal{H})$. Furthermore, the monotonicity property (6) under partial trace yields

$$C(\tau^{A_1}\otimes\varphi^{E_1}, \Omega^{A_1E_1}) \leqslant C(\tau^{A_1}\otimes\psi^{R}\otimes\varphi^{E_1}, \Omega^{A_1RE_1}) \leqslant \sqrt{\kappa}. \tag{77}$$

Then, for any $\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\omega^{A_1E_1})$

$$C(\bar{\omega}^{A_1E_1}, \tau^{A_1} \otimes \varphi^{E_1}) \leqslant C(\bar{\omega}^{A_1E_1}, \Omega^{A_1E_1}) + C(\tau^{A_1} \otimes \varphi^{E_1}, \Omega^{A_1E_1}) \leqslant \delta + \sqrt{\kappa},$$

where the first inequality follows from the fact that $C(\rho, \sigma)$ is a metric and hence satisfies the triangle inequality. Further,

$$C(\bar{\omega}^{A_1E_1} \otimes \psi^R, \tau^{A_1} \otimes \varphi^{E_1} \otimes \psi^R) = C(\bar{\omega}^{A_1E_1}, \tau^{A_1} \otimes \varphi^{E_1}) \leqslant \delta + \sqrt{\kappa}. \tag{78}$$

Applying the triangle inequality once again and using (76) and (78) yields

$$\begin{aligned} C(\bar{\omega}^{A_1E_1} \otimes \psi^R, \Omega^{A_1E_1R}) &\leqslant C(\bar{\omega}^{A_1E_1} \otimes \psi^R, \tau^{A_1} \otimes \varphi^{E_1} \otimes \psi^R) + C(\tau^{A_1} \otimes \varphi^{E_1} \otimes \psi^R, \Omega^{A_1E_1R}) \\ &\leqslant \delta + 2\sqrt{\kappa}. \end{aligned}$$

In other words, $\forall\, \bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\omega^{A_1E_1})$, the following is true:

$$\bar{\omega}^{A_1E_1} \otimes \psi^R \in \mathcal{B}^{\delta+2\sqrt{\kappa}}(\Omega^{A_1E_1R}).$$

We then have

$$\begin{aligned} H_{\min}^{\delta+2\sqrt{\kappa}}(A_1E_1|R)_\Omega &= \max_{\bar{\sigma}^{A_1E_1R} \in \mathcal{B}^{\delta+2\sqrt{\kappa}}(\Omega^{A_1E_1R})} H_{\min}(A_1E_1|R)_{\bar{\sigma}} \\ &\geqslant \max_{\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\Omega^{A_1E_1})} H_{\min}(A_1E_1|R)_{\bar{\omega}^{A_1E_1} \otimes \psi^R} \\ &= \max_{\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\Omega^{A_1E_1})} \max_{\varrho^R \in \mathcal{D}(\mathcal{H}_R)} \left[-D_{\max}(\bar{\omega}^{A_1E_1} \otimes \psi^R || \mathbb{I}_{A_1E_1} \otimes \varrho^R)\right] \\ &\geqslant \max_{\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\Omega^{A_1E_1})} \left[-D_{\max}(\bar{\omega}^{A_1E_1} \otimes \psi^R || \mathbb{I}_{A_1E_1} \otimes \psi^R)\right] \\ &= \max_{\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\Omega^{A_1E_1})} H_{\min}(A_1E_1)_{\bar{\omega}^{A_1E_1}} \\ &= H_{\min}^\delta(A_1E_1)_\Omega. \end{aligned} \tag{79}$$

The first inequality follows because $\bar{\omega}^{A_1E_1} \otimes \psi^R \in \mathcal{B}^{\delta+2\sqrt{\kappa}}(\omega^{A_1RE_1})$ for any $\bar{\omega}^{A_1E_1} \in \mathcal{B}^\delta(\omega^{A_1E_1})$. The second inequality follows because we choose a particular $\varrho^R = \psi^R$. □

We can now obtain a lower bound for the one-shot quantum communication cost, $q_\varepsilon^{(1)}$, as follows. Let $\kappa := 2\sqrt{\varepsilon}$. Then, for any $\varepsilon' > 0$ and $\varepsilon'', \varepsilon''' \geqslant 0$, we have

$$\begin{aligned} q_\varepsilon^{(1)} &= \log|A_2| \\ &\geqslant H_{\max}^{\varepsilon''}(A_2|B)_\Omega \\ &\geqslant H_{\max}^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}(A_2A_1E_1|B)_\Omega - H_{\max}^{\varepsilon'''+2\sqrt{\kappa}}(A_1E_1|A_2B)_\Omega - \log\frac{2}{\varepsilon'^2} \\ &\geqslant H_{\max}^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}(A|B)_\psi - H_{\max}^{\varepsilon'''}(A_1E_1|A_2BR)_\Omega - \log\frac{2}{\varepsilon'^2} \\ &\geqslant H_{\max}^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}(A|B)_\psi - H_{\max}^{\varepsilon'''}(A_1A_2E_1|BR)_\Omega - \log|A_2| - \log\frac{2}{\varepsilon'^2} \\ &= -H_{\min}^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}(A|R)_\psi - H_{\max}^{\varepsilon'''}(A|BR)_\psi - \log|A_2| - \log\frac{2}{\varepsilon'^2} \\ &= -H_{\min}^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}(A|R)_\psi + H_{\min}^{\varepsilon'''}(A)_\psi - \log|A_2| - \log\frac{2}{\varepsilon'^2}. \end{aligned} \tag{80}$$

The first inequality follows from lemma 20 of [48]. The second inequality follows from the chain rule for smooth max-entropy (lemma 19). The third inequality follows from the fact that, for any $\delta \geqslant 0$, $H^{\delta}_{\max}(A|R)_{\psi} = H^{\delta}_{\max}(A_1A_2E_1|R)_{\Omega}$ since the two states $|\psi\rangle^{ABR}$ and $|\Omega\rangle^{A_1A_2E_1BR}$ are related by an isometry $U_{\varepsilon}^{A\to A_1A_2E_1}$ (lemma 17), and by a simple application of the duality relation (11) and lemma 15, which yields

$$\begin{aligned}-H^{\varepsilon'''+2\sqrt{\kappa}}_{\max}(A_1E_1|A_2B)_{\Omega} &= H^{\varepsilon'''+2\sqrt{\kappa}}_{\min}(A_1E_1|R)_{\Omega}\\ &\geqslant H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega}\\ &= -H^{\varepsilon'''}_{\max}(A_1E_1|A_2BR)_{\Omega}.\end{aligned}$$

The fourth inequality of (80) follows from Lemma 21. The second equality follows from the duality relation (11) and the fact that, for any $\delta \geqslant 0$, $H^{\delta}_{\max}(A|BR)_{\psi} = H^{\delta}_{\max}(A_1A_2E_1|BR)_{\Omega}$, since the two states $|\psi\rangle^{ABR}$ and $|\Omega\rangle^{A_1A_2E_1BR}$ are related by an isometry $U_{\varepsilon}^{A\to A_1A_2E_1}$ (lemma 17). The final equality follows from the duality relation (11) and the fact that ψ^{ABR} is pure.

Therefore, by choosing $\varepsilon' = \varepsilon''' = \varepsilon$ and $2\varepsilon'' = \varepsilon + \sqrt{\kappa}$, we have

$$q^{(1)}_{\varepsilon} = \log|A_2| \geqslant \tfrac{1}{2}[H^{\varepsilon}_{\min}(A)_{\psi} - H^{3\varepsilon+3\sqrt{\kappa}}_{\min}(A|R)_{\psi}] - \log\tfrac{\sqrt{2}}{\varepsilon}. \tag{81}$$

We can also obtain an upper bound for entanglement gain. We start with

$$\begin{aligned}H^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}_{\min}(A|R)_{\psi} &= H^{\varepsilon'+2\varepsilon''+\varepsilon'''+2\sqrt{\kappa}}_{\min}(A_1A_2E_1|R)_{\Omega}\\ &\geqslant H^{\varepsilon'''+2\sqrt{\kappa}}_{\min}(A_1E_1|R)_{\Omega} + H^{\varepsilon''}_{\min}(A_2|A_1E_1R)_{\Omega} - \log\frac{2}{\varepsilon'^2}\\ &\geqslant H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega} + H^{\varepsilon''}_{\min}(A_2|A_1E_1BR)_{\Omega} - \log\frac{2}{\varepsilon'^2}\\ &= H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega} - H^{\varepsilon''}_{\max}(A_2)_{\Omega} - \log\frac{2}{\varepsilon'^2}\\ &\geqslant H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega} - q^{(1)}_{\varepsilon} - \log\frac{2}{\varepsilon'^2}.\end{aligned} \tag{82}$$

The first equality holds because systems A and $A_1A_2E_1$ are related by an isometry (lemma 17). The first inequality follows from the chain rule for smooth min-entropy (lemma 19. The second inequality follows from the lemmas 15 and 20. The second inequality follows from the duality relation (11) and the fact that $\Omega^{A_1A_2E_1RB}$ is a pure state. The last inequality holds because

$$q^{(1)}_{\varepsilon} = \log|A_2| \geqslant H^{\varepsilon''}_{\max}(A_2)_{\Omega}.$$

Let us choose $\varepsilon''' = \sqrt{\kappa}$. We can then find a lower bound for $H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega}$ on the right-hand side of (82) as follows:

$$\begin{aligned}H^{\varepsilon'''}_{\min}(A_1E_1)_{\Omega} = H^{\sqrt{\kappa}}_{\min}(A_1E_1)_{\Omega} &= \max_{\bar{\sigma}^{A_1E_1}\in\mathcal{B}^{\sqrt{\kappa}}(\Omega^{A_1E_1})} H_{\min}(A_1E_1)_{\bar{\sigma}^{A_1E_1}}\\ &\geqslant H_{\min}(A_1E_1)_{\tau^{A_1}\otimes\varphi^{E_1}}\\ &= H_{\min}(A_1)_{\tau^{A_1}} + H_{\min}(E_1)_{\varphi^{E_1}}\\ &\geqslant \log|A_1|\\ &= e^{(1)}_{\varepsilon}.\end{aligned} \tag{83}$$

The first inequality follows because (74) implies that $\| \tau^{A_1}\otimes\varphi^{E_1} - \Omega^{A_1E_1} \|_1 \leqslant \kappa$, which in turn implies that $\tau^{A_1}\otimes\varphi^{E_1} \in \mathcal{B}^{\sqrt{\kappa}}(\Omega^{A_1E_1})$. The last inequality follows because $H_{\min}(E_1)_{\varphi^{E_1}}$ is non-negative, since φ^{E_1} is a state. Putting (82) and (83) together and choosing $\varepsilon' = \varepsilon'' = \varepsilon$, we have

$$e_\varepsilon^{(1)} \leqslant q_\varepsilon^{(1)} + H_{\min}^{3\varepsilon+3\sqrt{\kappa}}(A|R)_\psi + \log \frac{2}{\varepsilon^2}. \tag{84}$$

□

6. Conclusions and discussions

In this paper we obtain bounds on the quantum communication cost and the entanglement gain for the one-shot FQSW in terms of smooth min- and max-entropies. The one-shot FQSW can be considered to be at the apex of the existing family tree of protocols, since it yields the optimal rates of the (asymptotic) FQSW, which in turn is known to be the mother of all protocols in this tree. We also employ our one-shot results to explicitly prove the optimality of the asymptotic rates. We introduce a RI framework in the one-shot regime that yields achievable rates for the children protocols of the one-shot FQSW. We also obtain bounds on the one-shot quantum capacity of a noisy channel in terms of the same entropic quantity, namely a smooth conditional max-entropy, unlike previously obtained bounds [38].

Note that the entropic quantities characterizing the upper and lower bounds on the quantum communication cost for the one-shot FQSW are different. The reason behind this can be understood through the following examples pointed out to us by Berta *et al* [58]. For the case in which Alice and Bob initially share a state that is not correlated with the reference, perfect state transfer can be achieved without any quantum communication. This agrees with the lower bound on the quantum communication cost (in theorem 9), which (modulo the ε-dependent factor) vanishes for such a state. In contrast, there exist examples of genuine tripartite entangled states (in which Alice's system is classically correlated with the reference) for which one requires the quantum communication cost to be of the order of the dimension of the Hilbert space of Alice's system. This in turn agrees with the upper bound on the quantum communication cost in theorem 8.

Acknowledgments

We are grateful to M M Wilde for a careful reading of an earlier version of this paper and for pointing out an error in its appendix. We thank K Audenaert, R Colbeck, M Mosonyi, and J Oppenheim for helpful discussions. We also thank M Berta, M Christandl and R Renner, whose insightful comments and examples helped us to appreciate the complexity of the problem and correct some errors. The research leading to these results received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 213681.

Appendix A. Useful lemmas

Lemma 16. *For $\varepsilon > 0$ and $\rho^A \in \mathcal{D}(\mathcal{H}_A)$, we have*

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty} \frac{1}{n} H_0^\varepsilon(A)_{\rho^{\otimes n}} = H(A)_\rho.$$

Proof.

To show that

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_0^\varepsilon(A)_{\rho^{\otimes n}}\leqslant H(A)_\rho, \tag{A.1}$$

we resort to the following more general inequality, for a sequence of states $\hat{\rho}^A:=\{\rho_n^A\}_{n=1}^\infty$:

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_0^\varepsilon(A)_{\rho_n}\leqslant \bar{S}(A)_{\hat{\rho}}. \tag{A.2}$$

In the above, $\bar{S}(A)_{\hat{\rho}}$ denotes the *sup-spectral entropy rate*, which is defined as

$$\bar{S}(A)_{\hat{\rho}}:=\inf\{\gamma:\liminf_{n\to\infty}\mathrm{tr}[P_n^\gamma\rho_n^A]=1\},$$

where P_n^γ is a projector defined as

$$P_n^\gamma:=\{\rho_n^A\geqslant 2^{-n\gamma}\mathbb{I}_{A_n}\}.$$

Equation (A.2) holds because for every $\gamma\geqslant\bar{S}(A)_{\hat{\rho}}$ and every $\delta>0$ there exists a positive integer n_0 such that for every $n\geqslant n_0$

$$\mathrm{tr}[P_n^\gamma\rho_n^A]\geqslant 1-\delta.$$

Let $\tilde{\rho}_n^A:=P_n^\gamma\rho_n^A P_n^\gamma$. The gentle measurement lemma (lemma 1) gives

$$\|\tilde{\rho}_n^A-\rho_n^A\|_1\leqslant 2\sqrt{\delta}.$$

Equivalently, $\tilde{\rho}_n^A\in\mathcal{B}^{\delta'}(\rho_n^A)$, where $\delta'=\sqrt{4\sqrt{\delta}-4\delta}$. Then

$$\begin{aligned}H_0^\delta(A)_{\rho_n}&\leqslant H_0(A)_{\tilde{\rho}_n}\\&=\log\mathrm{tr}\Pi_{\tilde{\rho}_n}\\&\leqslant\log\mathrm{tr}P_n^\delta\\&=\log\mathrm{tr}[\{\rho_n^A\geqslant 2^{-n\gamma}\mathbb{I}_{A_n}\}\mathbb{I}_{A_n}]\\&\leqslant n\gamma,\end{aligned} \tag{A.3}$$

and therefore (A.2) holds. When we restrict our considerations to a sequence $\hat{\rho}^A:=\{\rho^{\otimes n}\}_{n=1}^\infty$, $\bar{S}(A)_{\hat{\rho}}=H(A)_\rho$ [61], and we obtain (A.1).

The opposite inequality

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_0^\varepsilon(A)_{\rho^{\otimes n}}\geqslant H(A)_\rho \tag{A.4}$$

follows directly from

$$H_0^{2\sqrt{\varepsilon}}(A)_\rho\geqslant\min_{\bar{\rho}\in\mathcal{B}^{2\sqrt{\varepsilon}}(\rho^A)}H_0(A)_{\bar{\rho}}$$

and

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\left[\min_{\bar{\rho}\in\mathcal{B}^{2\sqrt{\varepsilon}}((\rho^A)^{\otimes n})}H_0(A)_{\bar{\rho}}\right]=H(A)_\rho.$$

□

We make use of the following properties of the min- and max-entropies that were proved in [39, 48].

Lemma 17. *Let* $0 < \varepsilon \leqslant 1$, $\rho^{AB} \in \mathcal{D}_{\leqslant}(\mathcal{H}_{AB})$, *and let* $U^{A\to C}$ *and* $V^{B\to D}$ *be two isometries with* $\omega^{CD} := (U \otimes V)\rho^{AB}(U^\dagger \otimes V^\dagger)$; *then*

$$H^{\varepsilon}_{\min}(A|B)_\rho = H^{\varepsilon}_{\min}(C|D)_\omega,$$
$$H^{\varepsilon}_{\max}(A|B)_\rho = H^{\varepsilon}_{\max}(C|D)_\omega.$$

Lemma 18 (data-processing inequality for smooth max-entropy) [48]. *Let* $0 \leqslant \varepsilon \leqslant 1$ *and* $\rho^{AB} \in \mathcal{D}(\mathcal{H}_{AB})$, *and let* $\mathcal{E}^{B\to C}$ *be a CPTP map with* $\sigma^{AC} := (\mathrm{id}_A \otimes \mathcal{E}^{B\to C})\rho^{AB}$. *Then*

$$H^{\varepsilon}_{\max}(A|B)_\rho \leqslant H^{\varepsilon}_{\max}(A|C)_\sigma.$$

Lemma 19 (chain rule for smooth min- and max-entropies) [39]. *Let* $0 < \varepsilon \leqslant 1$, $\varepsilon', \varepsilon'' \geqslant 0$ *and* $\rho^{ABC} \in \mathcal{D}(\mathcal{H}_{ABC})$. *Then*

$$H^{\varepsilon+2\varepsilon'+\varepsilon''}_{\min}(AB|C)_\rho \geqslant H^{\varepsilon'}_{\min}(A|BC)_\rho + H^{\varepsilon''}_{\min}(B|C)_\rho - \log\frac{2}{\varepsilon^2}.$$

Let φ^{ABCR} *be a purification of* ρ^{ABC}. *Furthermore, through the duality relation (11), we have*

$$H^{\varepsilon'}_{\max}(A|R)_\varphi \geqslant H^{\varepsilon+2\varepsilon'+\varepsilon''}_{\max}(AB|R)_\varphi - H^{\varepsilon''}_{\max}(B|AR)_\varphi - \log\frac{2}{\varepsilon^2}.$$

Lemma 20 [48]. *Let* $0 < \varepsilon \leqslant 1$ *and* $\rho^{ABC} \in \mathcal{D}_{\leqslant}(\mathcal{H}_{ABC})$. *Then*

$$H^{\varepsilon}_{\min}(A|BC)_\rho \leqslant H^{\varepsilon}_{\min}(A|B)_\rho,$$
$$H^{\varepsilon}_{\max}(A|BC)_\rho \leqslant H^{\varepsilon}_{\max}(A|B)_\rho.$$

Lemma 21 [39]. *Let* $0 < \varepsilon \leqslant 1$ *and* $\rho^{ABC} \in \mathcal{D}_{\leqslant}(\mathcal{H}_{ABC})$. *Then*

$$H^{\varepsilon}_{\min}(AB|C)_\rho \leqslant H^{\varepsilon}_{\min}(A|C)_\rho + \log|B|.$$

Let φ^{ABCR} *be a purification of* ρ^{ABC}. *Furthermore, through the duality relation (11), we have*

$$-H^{\varepsilon}_{\max}(A|BR)_\varphi \geqslant -H^{\varepsilon}_{\max}(AB|R)_\varphi - \log|B|.$$

Lemma 22 [57]. *For any* $0 < \varepsilon \leqslant 1$, *and* $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$,

$$H^{\varepsilon}_{\max}(A|B)_\rho \leqslant \tilde{H}^{\varepsilon}_0(A|B)_\rho, \tag{A.5}$$

where $\tilde{H}^{\varepsilon}_0(A|B)_\rho$ *is defined through (17).*

Proof.

Let $\omega^{AB} \in \mathcal{B}^{\varepsilon}(\rho^{AB})$ be an operator for which the minimum in (17) is achieved, and let ω^{ABE} be its purification. Then

$$\begin{aligned}
H^{\varepsilon}_{\max}(A|B)_\rho &= \min_{\bar\rho^{AB}\in\mathcal{B}^{\varepsilon}(\rho^{AB})} H_{\max}(A|B)_{\bar\rho} \\
&\leqslant H_{\max}(A|B)_\omega \\
&= -H_{\min}(A|E)_\omega \\
&\leqslant \min_{\nu^E}[-H_{\min}(\omega^{AE}|\nu^E)] \\
&\leqslant -H_{\min}(\omega^{AE}|\omega^E) \\
&= \tilde{H}_0(A|B)_\omega \\
&= \tilde{H}^{\varepsilon}_0(A|B)_\omega,
\end{aligned} \tag{A.6}$$

where $H_{\min}(\omega^{AE}|\nu^E) = -D_{\max}(\omega^{AE}||\mathbb{I}_A \otimes \nu^E)$. The second equality in (A.6) follows from the duality relation (11) and the third equality follows from proposition 3.1 of [42] (extended to subnormalized states), which states that for any tripartite pure state ω^{ABE}, $H_{\min}(\omega^{AE}|\omega^E) = -H_0(A|B)_\omega$. □

Appendix B. Proof of the one-shot decoupling theorem

Here we provide a proof of the decoupling theorem, theorem 5.1, for sake of completeness. Various versions of the proof can be found in, e.g., [27, 38, 39, 43].

Proof.

For any fixed $0 < \varepsilon \leqslant 1$, let $\bar{\rho}^{AR} \in \mathcal{B}^\varepsilon(\rho^{AR})$ and let

$$\bar{\sigma}^{A_1R}(U) = \mathrm{tr}_{A_2}[(U \otimes \mathbb{I}_R)\bar{\rho}^{AR}(U \otimes \mathbb{I}_R)^\dagger].$$

Since the unitary operator only acts on system A, we have that $\bar{\sigma}^R(U) = \bar{\rho}^R$. Similarly, taking the partial trace over A_1 on both sides of (62) yields $\sigma^R(U) = \rho^R$. By the triangle inequality,

$$\begin{aligned}
&\|\sigma^{A_1R}(U) - \tau^{A_1} \otimes \rho^R\|_1 \\
&\leqslant \|\sigma^{A_1R}(U) - \bar{\sigma}^{A_1R}(U)\|_1 + \|\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R\|_1 + \|\tau^{A_1} \otimes \bar{\rho}^R - \tau^{A_1} \otimes \rho^R\|_1 \\
&= \|\sigma^{A_1R}(U) - \bar{\sigma}^{A_1R}(U)\|_1 + \|\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R\|_1 + \|\bar{\rho}^R - \rho^R\|_1 \\
&\leqslant \|\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R\|_1 + 2\|\bar{\sigma}^{A_1R}(U) - \sigma^{A_1R}(U)\|_1,
\end{aligned} \tag{B.1}$$

where the last inequality follows from the monotonicity of the trace distance under partial trace:

$$\|\bar{\rho}^R - \rho^R\|_1 = \|\bar{\sigma}^R(U) - \sigma^R(U)\|_1 \leqslant \|\bar{\sigma}^{A_1R}(U) - \sigma^{A_1R}(U)\|_1.$$

Now by lemma 3.2 of [53], we have

$$\begin{aligned}
\int_{U(A)} \|\sigma^{A_1R}(U) - \bar{\sigma}^{A_1R}(U)\|_1 \,\mathrm{d}U &\leqslant \|\bar{\rho}^{A_1R} - \rho^{A_1R}\|_1, \\
&\leqslant 2\varepsilon
\end{aligned} \tag{B.2}$$

where the last inequality follows because $\bar{\rho}^{A_1R} \in \mathcal{B}^\varepsilon(\rho^{A_1R})$. Substituting (B.2) into (B.1) yields

$$\int_{U(A)} \|\sigma^{A_1R}(U) - \tau^{A_1} \otimes \rho^R\|_1 \,\mathrm{d}U \leqslant \int_{U(A)} \|\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R\|_1 \,\mathrm{d}U + 4\varepsilon. \tag{B.3}$$

Next we use the following inequalities (lemma 5.1.3 of [46]): let H be a Hermitian operator in $\mathcal{B}(\mathcal{H})$, and $\Omega \in \mathcal{B}(\mathcal{H})$. Then

$$\|H\|_1 \leqslant \sqrt{\mathrm{tr}\,\Omega}\,\|\Omega^{-1/4} H \Omega^{-1/4}\|_2, \tag{B.4}$$

$$\|H\|_1^2 \leqslant \mathrm{tr}\,\Omega\,\|\Omega^{-1/4} H \Omega^{-1/4}\|_2^2. \tag{B.5}$$

Hence

$$\begin{aligned}
&\int_{U(A)} \|\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R\|_1 \,\mathrm{d}U \\
&\leqslant \int_{U(A)} \sqrt{\mathrm{tr}\,\Omega}\sqrt{\|\Omega^{-1/4}(\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R)\Omega^{-1/4}\|_2^2}\,\mathrm{d}U \\
&\leqslant \sqrt{\mathrm{tr}\,\Omega}\sqrt{\int_{U(A)} \|\Omega^{-1/4}(\bar{\sigma}^{A_1R}(U) - \tau^{A_1} \otimes \bar{\rho}^R)\Omega^{-1/4}\|_2^2\,\mathrm{d}U}.
\end{aligned} \tag{B.6}$$

The first inequality follows from (B.5). The second inequality follows from the concavity of the function $f(x)=\sqrt{x}$. Choose $\Omega=\mathbb{I}_{A_1}\otimes\omega_R$, where $\omega_R\in\mathcal{D}(\mathcal{H}_R)$, and let

$$\begin{aligned}\tilde{\sigma}^{A_1R}(U)&=\Omega^{-1/4}\bar{\sigma}^{A_1R}(U)\Omega^{-1/4}\\&=(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\bar{\sigma}^{A_1R}(U)(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\\&=(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\mathrm{tr}_{A_2}[(U\otimes\mathbb{I}_R)\bar{\rho}^{AR}(U\otimes\mathbb{I}_R)^\dagger](\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\\&=\mathrm{tr}_{A_2}[(U\otimes\mathbb{I}_R)(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\bar{\rho}^{AR}(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})(U\otimes\mathbb{I}_R)^\dagger]\\&=\mathrm{tr}_{A_2}[(U\otimes\mathbb{I}_R)\tilde{\rho}^{AR}(U\otimes\mathbb{I}_R)^\dagger],\end{aligned}\tag{B.7}$$

with $\tilde{\rho}^{AR}:=(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})\bar{\rho}^{AR}(\mathbb{I}_{A_1}\otimes\omega_R^{-1/4})$ in the last equality. Note that $\tilde{\rho}^R=\mathrm{tr}_A\tilde{\rho}^{AR}=\omega_R^{-1/4}\bar{\rho}^R\omega_R^{-1/4}$. Continuing from (B.6),

$$\begin{aligned}&\int_{U(A)}\|\tilde{\sigma}^{-1/4}(\bar{\sigma}^{A_1R}(U)-\tau^{A_1}\otimes\bar{\rho}^R)\Omega^{-1/4}\|_2^2\,\mathrm{d}U\\&=\int_{U(A)}\|\tilde{\sigma}^{A_1R}(U)-\tau^{A_1}\otimes\tilde{\rho}^R\|_2^2\,\mathrm{d}U\\&=\int_{U(A)}\mathrm{tr}[(\tilde{\sigma}^{A_1R}(U)-\tau^{A_1}\otimes\tilde{\rho}^R)^2]\,\mathrm{d}U\\&=\int_{U(A)}(\mathrm{tr}[\tilde{\sigma}^{A_1R}(U)^2]-2\mathrm{tr}[\tilde{\sigma}^{A_1R}(U)(\tau^{A_1}\otimes\tilde{\rho}^R)]+\mathrm{tr}[(\tau^{A_1}\otimes\tilde{\rho}^R)^2])\,\mathrm{d}U\\&=\int_{U(A)}\mathrm{tr}[\tilde{\sigma}^{A_1R}(U)^2]\,\mathrm{d}U-\mathrm{tr}[(\tau^{A_1}\otimes\tilde{\rho}^R)^2]\\&=\int_{U(A)}\mathrm{tr}[\tilde{\sigma}^{A_1R}(U)^2]\,\mathrm{d}U-\frac{1}{|A_1|}\mathrm{tr}[(\tilde{\rho}^R)^2]\\&\leqslant\frac{1}{|A_2|}\mathrm{tr}[(\tilde{\rho}^{AR})^2].\end{aligned}\tag{B.8}$$

The last inequality follows from lemma C.2 of [27], which states that

$$\int_{U(A)}\mathrm{tr}[\tilde{\sigma}^{A_1R}(U)^2]\,\mathrm{d}U\leqslant\frac{1}{|A_1|}\mathrm{tr}[(\tilde{\rho}^R)^2]+\frac{1}{|A_2|}\mathrm{tr}[(\tilde{\rho}^{AR})^2].$$

Let $\bar{\rho}^{AR}\in\mathcal{D}_\leqslant(\mathcal{H}_{AR})$ and $\omega_R\in\mathcal{D}(\mathcal{H}_R)$ be such that

$$\begin{aligned}H^\varepsilon_{\min}(A|R)_\rho&=-D_{\max}(\bar{\rho}_{AR}||\mathbb{I}_A\otimes\omega_R)\\&=H_{\min}(A|R)_{\bar{\rho}|\omega}\\&\leqslant H_{\mathrm{C}}(A|R)_{\bar{\rho}|\omega},\end{aligned}\tag{B.9}$$

where $H_{\mathrm{C}}(A|R)_{\bar{\rho}|\omega}$ is the quantum collision entropy of $\bar{\rho}_{AR}$ relative to ω_R:

$$\begin{aligned}H_{\mathrm{C}}(A|R)_{\bar{\rho}|\omega}&:=-\log\mathrm{tr}[((\mathbb{I}_A\otimes\omega_R^{-1/4})\bar{\rho}^{AR}(\mathbb{I}_A\otimes\omega_R^{-1/4}))^2]\\&=-\log\mathrm{tr}[(\tilde{\rho}^{AR})^2].\end{aligned}\tag{B.10}$$

The last inequality in (B.9) follows from lemma B.16 of [27]. Now suppose we choose

$$\begin{aligned}\log|A_1|&\leqslant\tfrac{1}{2}[\log|A|+H^\varepsilon_{\min}(A|R)_\rho]+\log\varepsilon\\&\leqslant\tfrac{1}{2}[\log|A|+H_{\mathrm{C}}(A|R)_{\bar{\rho}|\omega}]+\log\varepsilon\\&=\tfrac{1}{2}[\log|A|-\log\mathrm{tr}[(\tilde{\rho}^{AR})^2]]+\log\varepsilon.\end{aligned}\tag{B.11}$$

Equation (B.11) then implies that

$$\begin{aligned}\log\left(\frac{|A_1|}{\varepsilon}\right)^2 &\leqslant \log|A| - \log \mathrm{tr}[(\tilde{\rho}^{AR})^2] \\ &= \log\frac{|A|}{\mathrm{tr}[(\tilde{\rho}^{AR})^2]}.\end{aligned} \tag{B.12}$$

From (B.3), (B.6) and (B.8) we obtain

$$\begin{aligned}\int_{U(A)} \|\sigma_{A_1R}(U) - \tau_{A_1}\otimes\rho_R\|_1\,\mathrm{d}U &\leqslant 4\varepsilon + \sqrt{|A_1|}\sqrt{\frac{1}{|A_2|}\mathrm{tr}[(\tilde{\rho}_{AR})^2]} \\ &= 4\varepsilon + |A_1|\sqrt{\frac{1}{|A|}\mathrm{tr}[(\tilde{\rho}_{AR})^2]} \\ &\leqslant 4\varepsilon + |A_1|\sqrt{\frac{\varepsilon^2}{|A_1|^2}} \\ &\leqslant 5\varepsilon,\end{aligned} \tag{B.13}$$

where the last inequality follows from (B.12). □

References

[1] Schumacher B 1995 Quantum coding *Phys. Rev.* A **51** 2738–47

[2] Jozsa R and Schumacher B 1994 A new proof of the quantum noiseless coding theorem *J. Mod. Opt.* **41** 2343–9

[3] Holevo A S 1973 Bounds for the quantity of information transmitted by a quantum communication channel *Probl. Peredachi Inf.* **9** 3–11

[4] Holevo A S 1998 The capacity of the quantum channel with general signal states *IEEE Trans. Inf. Theory* **44** 269–73

[5] Schumacher B and Westmoreland M D 1997 Sending classical information via noisy quantum channels *Phys. Rev.* A **56** 131–8

[6] Devetak I 2005 The private classical capacity and quantum capacity of a quantum channel *IEEE Trans. Inf. Theory* **51** 44–55

[7] Lloyd S 1997 The capacity of a noisy quantum channel *Phys. Rev.* A **55** 1613–22

[8] Shor P W 2002 The quantum channel capacity and coherent information *MSRI Workshop on Quantum Computation* http://www.msri.org//publications/ln/msri/2002/quantumcrypto/shor/1/

[9] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 Concentrating partial entanglement by local operations *Phys. Rev.* A **53** 2046–52

[10] Lo H-K and Popescu S 1999 The classical communication cost of entanglement manipulation: is entanglement an inter-convertible resource? *Phys. Rev. Lett.* **83** 1459–62

[11] Devetak I and Winter A 2004 Relating quantum privacy and quantum coherence: an operational approach *Phys. Rev. Lett.* **93** 080501

[12] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.* A **461** 207–35

[13] Horodecki M, Oppenheim J and Winter A 2005 Partial quantum information *Nature* **436** 673–6

[14] Horodecki M, Oppenheim J and Winter A 2006 Quantum State merging and negative information *Commun. Math. Phys.* **269** 107–36

[15] Bennett C H, Shor P W, Smolin J A and Thapliyal A V 2002 Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem *IEEE Trans. Inf. Theory* **48** 2637–55
[16] Bennett C H, Devetak I, Harrow A W, Shor P W and Winter A 2009 Quantum reverse Shannon theorem arXiv:0912.5537
[17] Devetak I, Harrow A W and Winter A 2004 A family of quantum protocols *Phys. Rev. Lett.* **93** 230504
[18] Devetak I, Harrow A W and Winter A 2008 A resource framework for quantum shannon theory *IEEE Trans. Inf. Theory* **54** 4587–618
[19] Horodecki M, Horodecki P, Horodecki R, Leung D W and Terhal B M 2001 Classical capacity of a noiseless quantum channel assisted by noisy entanglement *Quantum Inf. Comput.* **1** 70–8
[20] Holevo A S 2002 On entanglement assisted classical capacity *J. Math. Phys.* **43** 4326–33
[21] Hsieh M-H, Devetak I and Winter A 2008 The entanglement-assisted capacity of quantum multiple access channels *IEEE Trans. Inf. Theory* **54** 3078–90
[22] Hsieh M-H and Wilde M M 2010 Entanglement-assisted communication of classical and quantum information *IEEE Trans. Inf. Theory* **56** 4682–704
[23] Hsieh M-H and Wilde M M 2010 Trading classical communication, quantum communication and entanglement in quantum Shannon theory *IEEE Trans. Inf. Theory* **56** 4705–30
[24] Hsieh M-H and Wilde M M 2009 Public and private communication with a quantum channel and a secret key *Phys. Rev.* A **80** 022306
[25] Abeyesinghe A, Devetak I, Hayden P and Winter A 2009 The mother of all protocols: restructing quantum information's family tree *Proc. R. Soc.* A **465** 2537–63
[26] Hayden P 2011 Quantum information theory via decoupling *14th Workshop on Quantum Information Processing* http://qip2011.quantumlah.org/images/QIPtutorial1.pdf
[27] Berta M, Christandl M and Renner R 2009 The quantum reverse Shannon theorem based on one-shot information theory arXiv:0912.3805
[28] Yard J, Hayden P and Devetak I 2006 Quantum broadcast channels arXiv:quant-ph/0603098
[29] Dupuis F, Hayden P and Li K 2010 A father protocol for quantum broadcast channels *IEEE Trans. Inf. Theory* **56** 2946–56
[30] Yard J T and Devetak I 2009 Optimal quantum source coding with quantum side information at the encoder and decoder *IEEE Trans. Inf. Theory* **55** 5339–51
[31] Devetak I and Yard J 2008 Exact cost of redistributing multipartite quantum states *Phys. Rev. Lett.* **100** 230501
[32] Ye M-Y, Bai Y-K and Wang Z D 2008 Quantum state redistribution based on a generalized decoupling *Phys. Rev.* A **78** 030302
[33] Slepian D and Wolf J K 1971 Noiseless coding of correlated information sources *IEEE Trans. Inf. Theory* **19** 471–80
[34] Oppenheim J 2008 State redistribution as merging: introducing the coherent relay arXiv:0805.1065
[35] Wang L and Renner R 2010 One-shot classical-quantum capacity and hypothesis testing arXiv:1007.5456
[36] Renes J M and Renner R 2010 One-shot classical data compression with quantum side information and the distillation of common randomness and secret keys arXiv:1008.0452v2
[37] Renes J M and Renner R 2010 Noisy channel coding via privacy amplification and information reconciliation arXiv:1012.4814
[38] Buscemi F and Datta N 2010 The quantum capacity of channels with arbitrarily correlated noise *IEEE Trans. Inf. Theory* **56** 1447–60
[39] Dupuis F, Berta M, Wullschleger J and Renner R 2010 The decoupling theorem arXiv:1012.6044
[40] Buscemi F and Datta N 2010 General theory of assisted entanglement distillation arXiv:1009.4464
[41] Buscemi F and Datta N 2010 Distilling entanglement from arbitrary resources *J. Math. Phys.* **51** 102201
[42] Berta M 2008 Single-shot quantum state merging *Diploma Thesis* ETH Zurich, Switzerland
[43] Dupuis F 2009 The decoupling approach to quantum information theory *PhD Thesis* Université de Montréal (arXiv:1004.1641v1)

[44] Hayashi M and Nagaoka H 2003 General formulas for capacity of classical-quantum channels *IEEE Trans. Inf. Theory* **49** 1753–68
[45] Bowen G and Datta N 2008 Asymptotic entanglement manipulation of bipartite pure states *IEEE Trans. Inf. Theory* **54** 3677–86
[46] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zurich, Switzerland
[47] Tomamichel M, Colbeck R and Renner R 2009 A fully asymptotic equipartition property *IEEE Trans. Inf. Theory* **55** 5840–7
[48] Tomamichel M, Colbeck R and Renner R 2010 Duality between smooth min- and max-entropies *IEEE Trans. Inf. Theory* **56** 4674–81
[49] König R, Renner R and Schaffner C 2009 The operational meaning of min- and max-entropy *IEEE Trans. Inf. Theory* **55** 4337–47
[50] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (New York: Cambridge University Press)
[51] Gilchrist A, Langford N K and Nielsen M A 2005 Distance measures to compare real and ideal quantum processes *Phys. Rev.* A **71** 062310
[52] Datta N 2009 Min- and max-relative entropies and a new entanglement monotone *IEEE Trans. Inf. Theory* **55** 2816–26
[53] Hayden P, Horodecki M, Yard J and Winter A 2008 A decoupling approach to the quantum capacity *Open Syst. Inf. Dyn.* **15** 7–19
[54] Uhlmann A 1976 The 'transition probability' in the state space of a $*$-algebra *Rep. Math. Phys.* **9** 273–9
[55] Datta N and Hsieh M-H in preparation
[56] Datta N, Hsieh M-H and Oppenheim J Optimality of one-shot state redistribution in preparation
[57] Colbeck R 2011 private communication
[58] Berta M, Christandl M and Renner R 2011 private communication
[59] Ogawa T and Nagaoka H 2002 New proof of the channel coding theorem via hypothesis testing in quantum information theory *Proc. Int. Symp. Information Theory, ISIT* p 73
[60] Winter A 1999 Coding theorem and strong converse for quantum channels *IEEE Trans. Inf. Theory* **45** 2481–5
[61] Bowen G and Datta N 2006 Beyond i.i.d. in quantum information theory *Proc. Int. Symp. Information Theory, ISIT'*06 p 451