Resource Cost Results for Entanglement Distillation and State Merging under Source Uncertainties

Holger Boche and Gisbert Janßen

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany
Email:{boche, gisbert.janssen}@tum.de

Abstract—We introduce one-way LOCC protocols for quantum state merging for compound sources, which have asymptotically optimal entanglement as well as classical communication resource costs. For the arbitrarily varying quantum source (AVQS) model, we determine the one-way entanglement distillation capacity, where we utilize the robustification and elimination techniques, well-known from classical as well as quantum channel coding under assumption of arbitrarily varying noise. Investigating quantum state merging for AVQS, we demonstrate by example, that the usual robustification procedure leads to suboptimal resource costs in this case.

I. INTRODUCTION

Communication tasks on two-party quantum sources have been investigated with extensive results. Especially protocols restricted to local operations and classical communication (LOCC) and potential use of pure entanglement as communication resource are of special interest for quantum communication as well as entanglement theory.

Quantum state merging and entanglement distillation, two prominent instances within this paradigm, are considered in this work. For the asymptotic scenario, where large block-lengths are considered, optimal resource cost results for i.i.d. quantum sources with perfectly known bipartite density matrix ρ_{AB} have been determined in [10] for entanglement distillation and in [11] for quantum state merging. Generalizations of these results to the compound source model, where the source describing density matrix is not perfectly known, but only identified as a member of a set $\mathcal{X}$ of states, were partly given in [7]. While the optimal asymptotic entanglement cost of one-way state merging for compound sources was determined in [7], the classical side communication cost of the protocols introduced there was suboptimal in general. The present work contributes protocols which are optimal regarding the entanglement as well as classical cost.

We mention here, that it seems tractable, to combine techniques from [7] with one-shot results for quantum state merging given in [6] to establish optimal universal protocols for quantum state merging of compound sources also in the regime of finite blocklengths.

From the communication perspective, it is highly desirable, to consider these protocols under more general source scenarios. In this work, we consider the AVQS source model, where the source density matrix is allowed to vary from output to output in an arbitrary manner over a set $\mathcal{X}$ of possible states.

This source model might imagined as result of a powerful communication attack, where an adversarial party is allowed to choose any state from $\mathcal{X}$ for each output of the source, forcing the communication parties to perform protocols which simultaneously work well for each possible output sequence. Communication settings with arbitrarily varying channels (AVCs) and sources were first investigated in classical Shannon theory, where the famous robustification and elimination techniques introduced by Ahlswede [1], [2] were demonstrated to be useful. Considering message transmission under the average error criterion, the mentioned techniques allow to derive asymptotically errorless coding schemes for a given AVC from coding schemes with exponentially decreasing error for a certain compound channel. Concerning channel coding scenarios assuming arbitrarily varying quantum channels, coding theorems were shown in e.g. in [5], [4].

In this work, we utilize the robustification and elimination techniques to determine the optimal entanglement rates for one-way entanglement distillation, and therefore generalize results from [10] and [7] to the AVQS scenario. We also consider quantum state merging for AVQS, and demonstrate, that the robustification approach to the arbitrarily varying setting is of limited usage in this case. We give an example, which shows, that actually, better (i.e. lower) entanglement, as well as classical communication rates are possible, than delivered by the robustification-based approach.

Due to space limitations in this paper, we restrict ourselves to brief proof sketches of the results. The full arguments and further explanations can be gathered in [8] accompanying this work.

II. NOTATION AND CONVENTIONS

All Hilbert spaces appearing in this work are considered to be finite dimensional complex vector spaces. In our notation $\mathcal{L}(\mathcal{H})$ is the set of linear maps and $\mathcal{S}(\mathcal{H})$ the set of states (density matrices) on a Hilbert space $\mathcal{H}$, while we denote the set of quantum channels (i.e. completely positive (cp) and trace preserving maps) from $\mathcal{L}(\mathcal{H})$ to $\mathcal{L}(\mathcal{K})$ by $\mathcal{C}(\mathcal{H}, \mathcal{K})$ and the set of trace-nonincreasing cp maps by $\mathcal{C}^{\downarrow}(\mathcal{H}, \mathcal{K})$ for two Hilbert spaces $\mathcal{H}, \mathcal{K}$. Regarding states on multiparty systems, we freely make use of the following convention for a system consisting of some parties X, Y, Z, for instance, we denote $\mathcal{H}_{XYZ} := \mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_Z$, and denote the marginals by

the letters assigned to subsystems, i.e. $\sigma_{XZ} := \mathrm{tr}_{\mathcal{H}_Y}(\sigma)$ for $\sigma \in \mathcal{S}(\mathcal{H}_{XYZ})$ and so on. For a bipartite pure state $|\psi\rangle\langle\psi|$ on a Hilbert space $\mathcal{H}_{XY}$, we denote its Schmidt rank (i.e. number of nonzero coefficients in the Schmidt representation of ψ) by $\mathrm{sr}(\psi)$. We use the definition $F(a,b) := \|\sqrt{a}\sqrt{b}\|_1^2$ for matrices $a, b \geq 0$ (F is the quantum fidelity in case that a, b are density matrices).

The von Neumann entropy is denoted $S(\cdot)$. The usual notation for entropic quantities extended here to indicate state dependency, we write $I(X;Y,\rho)$ $(I_c(X\rangle Y,\rho)$, $S(X|Y,\rho))$ for the quantum mutual information (coherent information, conditional entropy) of a bipartite state ρ shared by parties X and Y. The protocols we consider are build from one-way LOCC channels, which we define concisely in the following (see also the appendix of [7] and references therein).

A quantum instrument $\mathcal{T}$ on a Hilbert space $\mathcal{H}$ is given by a set $\{\mathcal{T}_k\}_{k=1}^K \subset \mathcal{C}^\downarrow(\mathcal{H},\mathcal{K})$ of trace non-increasing cp maps, such that $\sum_{k=1}^K \mathcal{T}_k$ is a channel. With bipartite Hilbert spaces $\mathcal{H}_{AB}$ and $\mathcal{K}_{AB}$, a channel $\mathcal{N} \in \mathcal{C}(\mathcal{H}_{AB}, \mathcal{K}_{AB})$ is an $A \to B$ (one-way) LOCC channel, if it is a combination of an instrument $\{\mathcal{T}_k\}_{k=1}^K \subset \mathcal{C}^\downarrow(\mathcal{H}_A, \mathcal{K}_A)$ and a family $\{\mathcal{R}_k\}_{k=1}^K \subset \mathcal{C}(\mathcal{H}_B, \mathcal{K}_B)$ of channels in the sense, that it can be written in the form

$$\mathcal{N}(a) = \sum_{k=1}^K (\mathcal{T}_k \otimes \mathcal{R}_k)(a) \qquad (a \in \mathcal{L}(\mathcal{H}_{AB})). \quad (1)$$

The number of different messages which A has to send to B within the application of $\mathcal{N}$ is K (interchanging parties gives the definition of $B \to A$ LOCC channels).

We denote the set of classical probability distributions on a set $\mathbf{S}$ by $\mathfrak{P}(\mathbf{S})$. The l-fold cartesian product of $\mathbf{S}$ will be denoted $\mathbf{S}^l$ and $s^l := (s_1, ..., s_l)$ is the notation for elements of $\mathbf{S}^l$. For a natural number n, the shortcut $[n]$ is used to abbreviate the set $\{1, ..., n\}$. For a set A we denote the convex hull of A by $\mathrm{conv}(A)$ and its boundary by ∂A. By $\mathfrak{S}_l$, we denote the group of permutations on l elements, in this way $\sigma(s^l) = (s_{\sigma(1)}, ..., s_{\sigma(l)})$ for each $s^l = (s_1, ..., s_l) \in \mathbf{S}^l$ and permutation $\sigma \in \mathfrak{S}_l$. For any two nonempty sets $\mathcal{X}$, $\mathcal{X}'$ of states on a Hilbert space $\mathcal{H}$, the Hausdorff distance between $\mathcal{X}$ and $\mathcal{X}'$ (induced by the trace norm $\|\cdot\|_1$) is defined by

$$d_H(\mathcal{X}, \mathcal{X}')$$
$$:= \max\left\{\sup_{\sigma\in\mathcal{X}} \inf_{\sigma'\in\mathcal{X}'} \|\sigma - \sigma'\|_1, \sup_{\sigma'\in\mathcal{X}'} \inf_{\sigma\in\mathcal{X}} \|\sigma - \sigma'\|_1\right\}.$$

III. BASIC DEFINITIONS

Let $\mathcal{X} = \{\rho_s\}_{s\in\mathbf{S}}$ be a set of states on a Hilbert space $\mathcal{H}$. The *(memoryless) compound source generated by* $\mathcal{X}$ is given by the family $\{\{\rho_s^{\otimes l}\}_{s\in\mathbf{S}}\}_{l\in\mathbb{N}}$ of states. The *arbitrarily varying source (AVQS) generated by* $\mathcal{X}$ is given by the family $\{\{\rho_{s^l}\}_{s^l\in\mathbf{S}^l}\}_{l\in\mathbb{N}}$, with shortcut definitions

$$\rho_{s^l} := \rho_{s_1} \otimes ... \otimes \rho_{s_l} \qquad (s^l = (s_1, ..., s_l) \in \mathbf{S}^l).$$

We identify compound and AVQ sources with their generating sets and write *the compound source* $\mathcal{X}$ and *the AVQS* $\mathcal{X}$.

A quantum channel $\mathcal{M}$ is called an (l, k_l, D_l)-$A \to B$ *merging for states on* $\mathcal{H}_{AB}$ [11] if it is an $A \to B$ one-way LOCC

$$\mathcal{M} : \mathcal{L}(\mathcal{K}_{0,AB}^l \otimes \mathcal{H}_{AB}^{\otimes l}) \to \mathcal{L}(\mathcal{K}_{1,AB}^l \otimes \mathcal{H}_{B'B}^{\otimes l}),$$

with D_l summands as in defined in (1), where $\mathcal{H}_{B'} \simeq \mathcal{H}_A$ is a Hilbert space under control of B, and $\mathcal{K}_{AB,0}^l, \mathcal{K}_{AB,1}^l$ are bipartite Hilbert spaces of systems shared by A and B. These spaces are reserved to carry input and output maximally entangled states ϕ_0^l and ϕ_1^l, which we assume to have maximal Schmidt rank, such that

$$k_l := \frac{\dim\mathcal{K}_{A,0}^l}{\dim\mathcal{K}_{A,1}^l} = \frac{\dim\mathcal{K}_{B,0}^l}{\dim\mathcal{K}_{B,1}^l} = \frac{\mathrm{sr}(\phi_0^l)}{\mathrm{sr}(\phi_1^l)}.$$

holds. Given a state ρ on $\mathcal{H}_{AB}^{\otimes l}$, and an (l, k_l, D_l) $A \to B$ merging $\mathcal{M}_l$, the measure of fidelity of the protocol applied to ρ is defined

$$F_m(\rho, \mathcal{M}_l) := F\left(\mathcal{M}_l \otimes \mathrm{id}_{\mathcal{H}_E^l}(\phi_0^l \otimes \psi), \phi_1^l \otimes \psi'\right). \quad (2)$$

In (2), ψ is any purification of ρ on $\mathcal{H}_{AB}^{\otimes l} \otimes \mathcal{H}_E^l$ with an additional Hilbert space $\mathcal{H}_E^l$, and ψ' is a version of the state ψ on $\mathcal{H}_{B'B}^{\otimes l} \otimes \mathcal{H}_E^l$. It was shown in [7], that the r.h.s. of the equality (2) is independent of the choice of purification.

Definition 1. *A real number* R_q *is called an* achievable entanglement cost *for* $A \to B$ *merging of the AVQS* $\mathcal{X} \subset \mathcal{S}(\mathcal{H}_{AB})$ *with classical communication rate* R_c, *if there exists a sequence* $\{\mathcal{M}_l\}_{l\in\mathbb{N}}$ *of* (l, k_l, D_l)-$A \to B$-*mergings, which fulfills the conditions*

1) $\lim_{l\to\infty} \inf_{s^l\in\mathbf{S}^l} F_m(\rho_{s^l}, \mathcal{M}_l) = 1$
2) $\limsup_{l\to\infty} \frac{1}{l}\log k_l \leq R_q$
3) $\limsup_{l\to\infty} \frac{1}{l}\log D_l \leq R_c.$

The corresponding definition regarding achievable entanglement costs for the compound source $\mathcal{X}$ can be easily guessed, where the first condition in the above definition has to be replaced by

1') $\lim_{l\to\infty} \inf_{s\in\mathbf{S}} F_m(\rho_s^{\otimes l}, \mathcal{M}_l) = 1.$

Definition 2. *The* $A \to B$-*one-way merging cost* $C_{m,\to}^{AV}(\mathcal{X})$ *of the AVQS* $\mathcal{X}$ *is defined by*

$$C_{m,\to}^{AV}(\mathcal{X}) := \inf\left\{R_q : \begin{array}{l} R_q \text{ is achievable entanglement} \\ \text{cost for } A \to B \text{ merging of the} \\ \text{AVQS } \mathcal{X} \text{ with some classical} \\ \text{communication rate } R_c \in \mathbb{R} \end{array}\right\}$$

The $A \to B$ *merging cost for merging of the compound source* $\mathcal{X}$ is defined analogously and denoted $C_{m,\to}(\mathcal{X})$ [7], [8]. Concerning entanglement distillation, we are interested in the entanglement gain of one-way LOCC distillation procedures.

Definition 3. *A non-negative number R is an* achievable $A \to B$ *entanglement distillation rate for the AVQS $\mathcal{X}$ with classical communication rate R_c, if there exists a sequence $\{\mathcal{D}_l\}_{l\in\mathbb{N}}$ of $A \to B$ LOCC channels, each with a representation as given in (1) with D_l summands, such that the conditions*

1) $\lim\limits_{l\to\infty}\inf_{s^l\in\mathbf{S}^l}F(\mathcal{D}_l(\rho_{s^l}),\phi_l)=1$
2) $\liminf\limits_{l\to\infty}\frac{1}{l}\log\operatorname{sr}(\phi_l)\geq R$
3) $\limsup\limits_{l\to\infty}\frac{1}{l}\log D_l\leq R_c$

hold, where ϕ_l is a maximally entangled state shared by A and B for each $l\in\mathbb{N}$.

Definition 4. *The $A\to B$ entanglement distillation capacity for the AVQS $\mathcal{X}$ is defined*

$$D_\to^{AV}(\mathcal{X}):=\sup\left\{R:\begin{array}{c}R\text{ is achievable }A\to B\text{ }dis-\\\text{tillation rate for the AVQS }\mathcal{X}\\\text{with some classical rate }R_c\end{array}\right\}.$$

For entanglement distillation again, the definitions in case of a compound quantum source can be easily guessed, and we denote the *one-way entanglement distillation capacity for the compound source $\mathcal{X}$* by $D_\to(\mathcal{X})$. We do not determine optimal classical communication rates for entanglement distillation here. These are unknown in general even in the case where the source is i.i.d. with perfectly known state [10].

IV. QUANTUM STATE MERGING FOR COMPOUND SOURCES

In this section, we show existence of $A\to B$ LOCC protocols, which are asymptotically optimal regarding their entanglement as well as classical side communication requirements, due to the converse results given in [7]. Optimality is known from the corresponding converse statement given in [7], Section V, where it was shown, that successful one-way merging of a compound source $\mathcal{X}$ is not possible with asymptotic classical cost smaller than $\sup_{\rho\in\mathcal{X}}I(A;E,\rho)$.

Theorem 5. *Let $\mathcal{X}\subset\mathcal{S}(\mathcal{H}_{AB})$ be a set of bipartite states. For each $\delta>0$, $R_q=\sup_{\rho\in\mathcal{X}}S(A|B,\rho)+\delta$ is an achievable entanglement cost for $A\to B$ merging of the compound source $\mathcal{X}$ with classical communication rate*

$$R_c=\sup_{\rho\in\mathcal{X}}I(A;E,\rho)+\delta,\qquad(3)$$

where $I(A;E,\rho)=S(\rho_A)+S(A|B,\rho)$ is the quantum mutual information between the A and E systems of a purification of ρ on a larger system with parties A,B,E.

Our proof of Theorem 5 has two main ingredients. We use slight generalizations of the results from [7], Theorems 4 and 6 (see [8]) where achievability of the entanglement cost $\sup_{\rho\in\mathcal{X}}S(A|B,\rho)$ was shown. However, the protocols used there, have classical $A\to B$ communication requirements of at least $\sup_{\rho\in\mathcal{X}}S(\rho_A)+\sup_{\rho\in\mathcal{X}}S(A|B,\rho)$ which is, in general, strictly greater than the rate given in (3). We show, that R_q is achievable with classical communication of rate R_c from (3) by combining the protocols from [7] with a suitably fine-grained entropy estimating instrument on the A-system.

Proof of Theorem 5: Let $\delta>0$, $l\in\mathbb{N}$, $d:=\dim\mathcal{H}_A$ and assume $\tilde{s}:=\sup_{\rho\in\mathcal{X}}S(A|B,\rho)-\frac{\delta}{2}<0$ (the remaining case $\tilde{s}\geq0$ follows by simple modifications). Consider the sequence $s_0:=0<s_1<...<s_N:=\log d$ with $s_i:=s_{i-1}+\eta$, $1\leq i<N$, and the intervals $I_0:=[s_0,s_1],I_i:=(s_{i-1},s_i)$,

$1<i<N$. These generate a decomposition $\mathcal{X}_1,...,\mathcal{X}_N$ of $\mathcal{X}$ into pairwise disjoint subsets (some may be empty), defined

$$\mathcal{X}_i:=\{\rho\in\mathcal{X}:\ S(\rho_A)\in I_i\}\qquad(i\in[N]).$$

We further define sets $\tilde{\mathcal{X}}_i:=\bigcup_{j\in n(i)}\mathcal{X}_j$, where $n(i):=\{j\in[N]:|j-i|\leq1\}$. We construct an entropy estimating instrument $\{\mathcal{P}^{(i)}\}_{i\in[N]}\subset\mathcal{C}^\downarrow(\mathcal{H}_A^{\otimes l},\mathcal{H}_A^{\otimes l})$ by defining

$$\mathcal{P}^{(i)}:=p_i(\cdot)p_i,\text{ with }p_i:=\sum_{\lambda:H(\overline\lambda)\in I_i}P_{\lambda,l}\quad(i\in[N]),$$

where $P_{\lambda,l}$ is the projection supported on the invariant subspace of $\mathcal{H}_A^{\otimes l}$ belonging to the representation of $\mathfrak{S}_l$ labeled by Young frame λ, and $H(\overline\lambda)$ is the Shannon entropy of the probability distribution given by the normalized box-lengths λ [9]. It can be shown (using the bounds from Theorem 1 in [9], which first appeared in [12]), that our definitions imply for sufficiently large blocklength l,

$$\sum_{j\in[N]\setminus n(i)}\operatorname{tr}(\mathcal{P}^{(j)}\otimes id_{\mathcal{H}_B^{\otimes l}}(\rho^{\otimes l}))\leq2^{-lc_2}\qquad(4)$$

for each $i\in[N]$ and $\rho\in\mathcal{X}_i$ with a positive constant $c_2=c_2(\eta)$. Moreover it is known from [7], Theorem 6 (with some simple modifications, see [8]), that for each i with $\tilde{\mathcal{X}}_i\neq\emptyset$ and large enough blocklength, there is a $(l,k_l,\tilde{D}_l^{(i)})-A\to B$ merging $\tilde{\mathcal{M}}^{(i)}$ with

$$\inf_{\rho\in\tilde{\mathcal{X}}_i}F_m(\rho^{\otimes l},\tilde{\mathcal{M}}_l^{(i)})\geq1-2^{-lc_3}\qquad(5)$$

with a positive constant $c_3>0$, $k_l\geq2^{-l\tilde{s}}$ and, for each i,

$$\frac{1}{l}\log\tilde{D}_l^{(i)}\leq\sup_{\rho\in\tilde{\mathcal{X}}_i}S(\rho_A)+\sup_{\rho\in\tilde{\mathcal{X}}_i}S(A|B,\rho)+\frac{\delta}{2}\qquad(6)$$

$$\leq\sup_{\rho\in\tilde{\mathcal{X}}_i}I(A;E,\rho)+\frac{\delta}{2}+3\eta.\qquad(7)$$

Define

$$\mathcal{M}_l:=\sum_{i\in[N]}\tilde{\mathcal{M}}_l^{(i)}\circ(\mathcal{P}^{(i)}\otimes id_{\mathcal{H}_B^{\otimes l}}),$$

and observe, that $\mathcal{M}_l$ is an (l,k_l,D_l) $A\to B$ merging with

$$\frac{1}{l}\log D_l=\frac{1}{l}\log\left(\sum_{i=1}^N D_i\right)\leq\sup_{\rho\in\mathcal{X}}I(A;E,\rho)+\frac{\delta}{2}+3\eta.$$

Eqns (4), (5) and properties of the merging fidelity imply

$$\inf_{\rho\in\mathcal{X}}F_m(\rho^{\otimes l},\mathcal{M}_l)\geq1-2^{-lc_4}\qquad(8)$$

with a positive constant c_4 for large enough blocklength. Since η and δ are free to choose, we are done. $\blacksquare$

V. ONE-WAY ENTANGLEMENT DISTILLATION FOR AVQS

The following theorem determines the capacity for $A \to B$ one way entanglement distillation in presence of an AVQS generated by a set $\mathcal{X}$ of density matrices. As in several coding theorems for classical AV channels and sources, the capacity of the AV source $\mathcal{X}$ equals the capacity of the compound source $\overline{\text{conv}(\mathcal{X})}$. Notice, that it makes no difference to consider $\text{conv}(\mathcal{X})$ instead of its closure since these sets have Hausdorff distance zero and the capacity function is continuous (see [8]).

Theorem 6. *Let* $\mathcal{X} \subset \mathcal{S}(\mathcal{H}_{AB})$ *be a set of bipartite states. It holds*

$$D_{\to}^{AV}(\mathcal{X}) = D_{\to}(\text{conv}(\mathcal{X}))$$
$$= \lim_{k \to \infty} \frac{1}{k} \max_{\mathcal{T}} \inf_{\tau \in \text{conv}(\mathcal{X})} D^{(1)}(\tau^{\otimes k}, \mathcal{T}),$$

where the maximization is over all instruments with domain $\mathcal{L}(\mathcal{H}_X)$, *and for each state* σ *on a bipartite space* $\mathcal{H}_{XY}$ *and instrument* $\mathcal{E} = \{\mathcal{E}_j\}_{j=1}^J$, *we use the definition*

$$D^{(1)}(\sigma, \mathcal{E}) := \sum_{\substack{\lambda_j(\sigma): \\ \lambda_j \neq 0}} \lambda_j(\sigma) \, I_c(X \rangle Y, \hat{\sigma}_j)$$

with $\lambda_j(\sigma) := \text{tr}(\mathcal{E}_j \otimes \text{id}_{\mathcal{H}_Y}(\sigma))$ *and* $\hat{\sigma}_j := \lambda_j(\sigma)^{-1} \mathcal{E}_j \otimes \text{id}_{\mathcal{H}_Y}(\sigma)$.

In the proof of Theorem 6 below, we invoke the robustification technique [2], to generate good entanglement distillation schemes for the AVQS $\mathcal{X}$ from good protocols for the compound source $\overline{\text{conv}\mathcal{X}}$.

Lemma 7 (Robustification technique, cf. [2] and Theorem 6 in [3]). *Let* $\mathbf{S}$ *be a set with* $|\mathbf{S}| < \infty$ *and* $l \in \mathbb{N}$. *If a function* $f : \mathbf{S}^l \to [0, 1]$ *satisfies*

$$\sum_{s^l \in \mathbf{S}^l} f(s^l) q(s_1) \cdot \ldots \cdot q(s_l) \geq 1 - \gamma \qquad (9)$$

for each type q *of sequences in* $\mathbf{S}^l$ *for some* $\gamma \in [0, 1]$, *then*

$$\frac{1}{l!} \sum_{\sigma \in \mathfrak{S}_l} f(\sigma(s^l)) \geq 1 - (l+1)^{|\mathbf{S}|} \cdot \gamma \qquad \forall s^l \in \mathbf{S}^l. \qquad (10)$$

Proof of Theorem 6: To show achievability, we first prove the assertion of the theorem for the case of a finite set $\mathcal{X} := \{\rho_s\}_{s \in \mathbf{S}}$. We show, that each achievable $A \to B$ entanglement distillation rate for the compound source $\text{conv}(\mathcal{X})$ is also achievable for the AVQS $\mathcal{X}$ and use the fact, that

$$\text{conv}(\mathcal{X}) = \left\{ \rho_p : \rho_p = \sum_{s \in \mathbf{S}} p(s) \rho_s, \ p \in \mathfrak{P}(\mathcal{X}) \right\}$$

holds. Assuming, that R is an achievable rate for the compound source $\text{conv}(\mathcal{X})$, we know, that for each $\delta > 0$ and large enough blocklength l, there is an $A \to B$ LOCC channel $\mathcal{D}_l$, such that for each $p \in \mathfrak{P}(\mathbf{S})$ the fidelity is bounded $F(\mathcal{D}_l(\rho_p^{\otimes l}), \phi_l) \geq 1 - 2^{-lc_5}$ with a constant $c_5 > 0$ (in the proof of Theorem 8 in [7], it was shown, that each achievable

rate can be achieved by protocols with exponentially decreasing error). With $f(s^l) := \rho_{s^l}$, and linearity of the fidelity in the first input, we yield

$$\sum_{s^l} p^l(s^l) \, f(s^l) \geq 1 - 2^{-lc_5} \quad \text{for all} \ p \in \mathfrak{P}(\mathbf{S}). \qquad (11)$$

Eq. (11) implies, that the function f satisfies the conditions of Lemma 7. Let $\mathcal{U}_\sigma$ be the (local) unitary channel, which permutes the tensor factors in $\mathcal{H}_{AB}^{\otimes l}$ according to the permutation σ, i.e. $\rho_{\sigma(s^l)} = \mathcal{U}_\sigma(\rho_{s^l})$, and $f(\sigma(s^l)) = F(\mathcal{D}_l \circ \mathcal{U}_\sigma(\rho_{s^l}), \phi_l)$. Lemma 7 and (11) imply, that

$$1 - (l+1)^{|\mathbf{S}|} \cdot 2^{-lc_5} \leq \frac{1}{l!} \sum_{\sigma \in l} f(\sigma(s^l)) = F(\hat{\mathcal{D}}_l(\rho_{s^l}), \phi_l)$$

holds for each s^l, where we defined an $A \to B$ one-way LOCC channel $\hat{\mathcal{D}}_l$ by $\hat{\mathcal{D}}_l := (l!)^{-1} \sum_{\sigma \in \mathfrak{S}_l} \mathcal{D}_l \circ \mathcal{U}_\sigma$. From the above inequality and the polynomial growth of the function $(l+1)^{|\mathbf{S}|}$ for $l \to \infty$, we infer, that R is an achievable rate for one-way entanglement distillation for the AVQS $\mathcal{X}$ with fidelity going to one exponentially fast. By Theorem 8 in [7] (generalized to the case of infinite compound sources in [8]), we can choose any rate $R \geq 0$ with $R \leq D_{\to}(\text{conv}(\mathcal{X}))$.

However, the protocols $\{\hat{\mathcal{D}}_l\}_{l=1}^\infty$ we introduced, are not reasonable regarding the classical side communication cost, since A has to communicate the messages required within application of $\tilde{\mathcal{D}}_l$ *and* the choice of permutation σ (out of $l!$ possibilities), i.e. the classical communication requirements are not rate-bounded for $l \to \infty$. However, we can invoke the derandomization technique from ([1]) to derive protocols with rate-bounded classical communication (see [8] for details).

To prove the general case of a not necessary finite or countable set $\mathcal{X}$, we apply a polytope approximation technique similar to the one used in [4]. For simplicity, we assume $\overline{\text{conv}(\mathcal{X})} \cap \partial \mathcal{S}(\mathcal{H}) = \emptyset$ (this condition can be removed by slight depolarization of the states in the set $\mathcal{X}$). Then, for any small enough number $\eta > 0$, we find a polytope P_η, i.e. the convex hull of a finite set $\{\tau_e\}_{e \in E}$ of extreme points, such that $\overline{\text{conv}(\mathcal{X})} \subset P_\eta \subset \mathcal{S}(\mathcal{H}_{AB}) \setminus \partial \mathcal{S}(\mathcal{H}_{AB})$, and

$$d_H(\text{conv}(\mathcal{X}), P_\eta) < \eta. \qquad (12)$$

Applying the argument for finite sets given above to P_η, we find, for each sufficiently large l, a distillation protocol $\hat{\mathcal{D}}_l$, such that

$$\min_{e^l \in E^l} F(\hat{\mathcal{D}}(\tau_{e^l}), \phi_l) \geq 1 - 2^{-lc_5} \qquad (13)$$

holds with a maximally entangled state ϕ_l, such that

$$\frac{1}{l} \log \text{sr}(\phi_l) \geq \frac{1}{k} \max_{\mathcal{T}} \inf_{\tau \in P_\eta} D(\tau^{\otimes k}, \mathcal{T}) - \frac{\delta}{2}. \qquad (14)$$

Since ρ_s can be written as a convex combination of extremal points of P_η, (13) implies

$$\inf_{s^l \in \mathbf{S}^l} F(\hat{\mathcal{D}}(\rho_{s^l}), \phi_l) \geq 1 - 2^{-lc_5}. \qquad (15)$$

By continuity properties of the function $D^{(1)}$ (see [8] for details), and (12) together with a (sufficiently small) choice of the parameter η, it holds

$$\max_{\mathcal{T}} \inf_{\tau \in P_\eta} D^{(1)}(\tau^{\otimes k}, \mathcal{T}) \geq \max_{\mathcal{T}} \inf_{\rho \in \mathrm{conv}(\mathcal{X})} D^{(1)}(\rho^{\otimes k}, \mathcal{T}) - \frac{k\delta}{2}$$

which, together with (15) and (14) gives achievability. The converse is obvious, since each entanglement distillation protocol $\mathcal{D}_l$ which is ϵ-good for the AVQS $\mathcal{X}$ is also ϵ-good for entanglement generation of $\overline{\mathrm{conv}(\mathcal{X})}$, so that the converse for the compound distillation theorem ([7], Theorem 8) applies. ∎

VI. QUANTUM STATE MERGING FOR AVQS

Regarding the task of one-way quantum state merging, the close connection between the merging cost of an AVQS $\mathcal{X}$ and the merging cost of the compound source generated by $\mathrm{conv}(\mathcal{X})$ breaks down. We demonstrate this by example.

Example 8. *There exists a set $\mathcal{X}$, such that*

$$C_{m,\rightarrow}^{AV}(\mathcal{X}) < C_{m,\rightarrow}(\mathrm{conv}(\mathcal{X})).$$

Consider the set $\hat{\mathcal{X}} := \{\rho_s\}_{s=1}^N \subset \mathcal{S}(\mathcal{H}_{AB})$, $N < \infty$, with

$$\rho_s := (U_s \otimes \mathbb{1}_{\mathcal{H}_B}) \rho_1 (U_s^* \otimes \mathbb{1}_{\mathcal{H}_B}) \qquad (s \in [N]) \qquad (16)$$

with $\rho_1 \in \mathcal{S}(\mathcal{H}_{AB})$ such that $S(A|B, \rho_1) < 0$, and unitary matrices $U_1 := \mathbb{1}_{\mathcal{H}_A}, U_2, ..., U_N$, such that the supports of the A marginals of the states in $\hat{\mathcal{X}}$ are pairwise orthogonal. We assume $\dim \mathcal{H}_A \geq N \cdot \mathrm{supp}(\rho_{A,1})$. These definitions also imply for each $s, s' \in [N], s \neq s'$

$$\rho_{B,s} = \rho_{B,1}, \text{ and } \mathrm{supp}(\rho_s) \perp \mathrm{supp}(\rho_{s'}). \qquad (17)$$

In the following, we show, that for each set constructed in the above manner, it holds the relation $C_{m,\rightarrow}^{AV}(\hat{\mathcal{X}}) \leq C_{m,\rightarrow}(\hat{\mathcal{X}}) - \log N$ for the one-way merging cost. Moreover, each achievable entanglement cost can be achieved with classical communication rate R_c such that $R_c \leq \sup_{\rho \in \mathrm{conv}(\hat{\mathcal{X}})} I(A; E, \rho) - \log N$ holds. From the orthogonality conditions (16) follows, that there is an instrument $\{\tilde{\mathcal{V}}_s\}_{s=1}^N$ on A's system, such that

$$\mathcal{V}_{s'}(\rho_s) := \tilde{\mathcal{V}}_{s'} \otimes \mathrm{id}_{\mathcal{H}_B}(\rho_s) = \delta_{ss'} \rho_1 \qquad (18)$$

holds for each $s \in [N]$. Since $C_{m,\rightarrow}(\rho_1) = S(A|B, \rho_1)$ [11], we find for each $\delta > 0$ and large enough blocklength l, an $(l, k_l, \tilde{D}_l)$ merging for ρ_1, with

$$k_l \leq 2^{l(S(A|B,\rho_1)+\delta)}, \quad \tilde{D}_l \leq 2^{l(I(A;E,\rho_1)+\delta)} \qquad (19)$$

$$\text{and} \quad F_m(\rho_1^{\otimes l}, \tilde{\mathcal{M}}_l) \geq 1 - 2^{-l\tilde{c}} \qquad (20)$$

with a constant $\tilde{c} > 0$. Define $\mathcal{M}_l := \sum_{s=1}^N \mathcal{U}_{s^l} \circ \tilde{\mathcal{M}}_l \circ \mathcal{V}_{s^l}$, with $\mathcal{U}_{s^l}(\cdot) := U_{s^l} \otimes \mathbb{1}_{\mathcal{H}_B^{\otimes l}}(\cdot) U_{s^l}^* \otimes \mathbb{1}_{\mathcal{H}_B^{\otimes l}}$. It holds

$$F_m(\rho_{s^l}, \mathcal{M}_l)$$
$$= \sum_{s'^l \in [N]^l} F(\mathcal{U}_{s'^l} \circ \tilde{\mathcal{M}}_l \circ \mathcal{V}_{s'^l} \otimes \mathrm{id}_{\mathcal{H}_E^{\otimes l}}(\psi_{s^l}), \phi_l \otimes \psi'_{s^l})$$
$$= \sum_{s'^l \in [N]^l} F(\tilde{\mathcal{M}}_l \otimes \mathrm{id}_{\mathcal{H}_E^{\otimes l}}(\mathcal{V}_{s'^l}(\psi_{s^l})), \phi_l \otimes \mathcal{U}_{s'^l}^*(\psi'_{s^l}))$$
$$= F_m(\rho_1^{\otimes l}, \tilde{\mathcal{M}}_l) \geq 1 - 2^{l\tilde{c}}.$$

for each $s^l \in [N]^l$. The first equality above is by linearity of the merging fidelity in the merging operation, the second one is by invariance of the fidelity under unitary evolutions, the third equality is by (18). The last inequality is (20). $\mathcal{M}_l$ is an (l, k_l, D_l)-$A \rightarrow B$-merging with $D_l = N^l \cdot \tilde{D}_l$, i.e.

$$\frac{1}{l} \log D_l \leq I(A; E, \rho_1) + \log N. \qquad (21)$$

By properties of the set $\tilde{\mathcal{X}}$, i.e. (16) and (17), and the equality $S(\rho_p) = \sum_{s=1}^N p(s) S(\rho_s) + H(p)$ which holds for each $\rho_p := \sum_{s=1}^N p(s) \rho_s$, $p \in \mathfrak{P}([N])$, due to orthogonality of the supports of the states, we infer by calculation of the entropies and maximization over p

$$\max_{p \in \mathfrak{P}([N])} S(A|B, \rho_p) = S(A|B, \rho_1) + \log N, \text{ and} \qquad (22)$$

$$\max_{p \in \mathfrak{P}([N])} I(A; E, \rho_p) = I(A; E, \rho_1) + 2 \log N. \qquad (23)$$

Eqns. (22) and (23) together with (19) and (21), show, that

$$R_q = \max_{p \in \mathfrak{P}([N])} S(A|B, \rho_p) - \log N$$

is achievable with asymptotic classical side communication at rate

$$R_c = \max_{p \in \mathfrak{P}([N])} I(A; E, \rho_p) - \log N.$$

REFERENCES

[1] R. Ahlswede. Elimination of Correlation in Random Codes for Arbitrarily Varying Channels. *Z. Wahr. Verw. Geb.* 44, 159–175 (1978).
[2] R. Ahlswede. Coloring Hypergraphs: A new Approach to Multi-user Source Coding II. *J. Comb., Info. & Sys. Sci.* 5, 220–268 (1980).
[3] R. Ahlswede. Arbitrarily Varying Channels with State Sequence Known to the Sender. *IEEE Trans. Inf. Th.* 32, 621–629 (1986).
[4] R. Ahlswede, I. Bjelaković, H. Boche, J. Nötzel. Quantum Capacity under adversarial quantum noise: arbitrarily varying quantum channels. *Comm. Math. Phys.* vol. 317, 103–156 (2013).
[5] R. Ahlswede, V. Blinovsky. Classical Capacity of Classical-Quantum Arbitrarily Varying Channels. *IEEE Trans. Inf. Th.* 53, 526–533 (2007).
[6] M. Berta. Single-shot Quantum State Merging. Diploma Thesis, ETH Zürich (2008) Available at http://arxiv.org/abs/0912.4495
[7] I. Bjelaković, H. Boche, G. Janßen. Universal quantum state merging. *J. Math. Phys.* 54, 032204 (2013).
[8] H. Boche, G. Janßen. Resource cost results for one-way entanglement distillation and state merging of compound and arbitrarily varying quantum sources (2014). Available at http://arxiv.org/abs/1401.6063
[9] M. Christandl, G. Mitchinson. The Spectra of Quantum States and the Kronecker Coefficients of the Symmetric Group *Comm. Math. Phys.* vol. 261, 789–797 (2006).
[10] I. Devetak, A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc.* A2005 461, 207–235 (2005).
[11] M. Horodecki, J. Oppenheim, A. Winter. Quantum State Merging and Negative Information. *Comm. Math. Phys.* 269, 107–136 (2007).
[12] M. Keyl, R.F. Werner. Estimating the spectrum of a density operator. *Phys. Rev. A* 64, 052311 (2001).