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 \( \rho_{AB} \) 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 [3], [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 \( \mathcal{C}^t(\mathcal{H}, \mathcal{K}) \) 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. \( \sigma_{XZ} := \text{tr}_{H_Y}(\sigma) \) for \( \sigma \in S(H_{XYZ}) \) and so on. For a bipartite pure state \( |\psi\rangle \langle \psi| \) on a Hilbert space \( H_{XY} \), we denote its Schmidt rank (i.e. number of non-zero coefficients in the Schmidt representation of \( \psi \)) by \( \text{sr}(\psi) \). We use the definition \( F(a,b) := \| \sqrt{ab} \|_1^2 \) 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.e. \( I(X|Y,\rho) \) for the quantum mutual information (coherent information, 2) for the quantum mutual information (coherent information, conditional entropy) of a bipartite state \( \rho \) shared by parties \( X \) and \( Y \). The protocols we consider are built from one-way LOCC maps, such that \( \sup \) for the compound source \( H \) is given by the family \( \mathcal{K}_{A,B} \) of channels in the sense, that it can hold for each \( k \). 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 \( A \rightarrow B \) merging of the AVQS \( X \subset S(H_{AB}) \) with classical communication rate \( R_c \), if there exists a sequence \( \{M_l\}_{l \in \mathbb{N}} \) of \((l,k_1,D_l)\)-\( A \rightarrow B \)-merging maps, which fulfills the conditions

1) \( \lim_{l \rightarrow \infty} \inf_{\rho,\phi} \sup_{M \in M_l} F_m(\rho,\phi,M_l) = 1 \)

2) \( \lim_{l \rightarrow \infty} \sup_{\rho,\phi} \frac{1}{l} \log \| D_l \| \leq R_q \)

3) \( \lim_{l \rightarrow \infty} \sup_{\rho,\phi} \frac{1}{l} \log \| D_l \| \leq R_c \).

The corresponding definition regarding achievable entanglement costs for the compound source \( X' \) can be easily guessed, where the first condition in the above definition has to be replaced by

1') \( \lim_{l \rightarrow \infty} \inf_{\rho,\phi} \sup_{M \in M_l} F_m(\rho,\phi,M_l) = 1 \).

**Definition 2.** The \( A \rightarrow B \)-one-way merging cost \( C_{m,\rightarrow}(X') \) of the AVQS \( X' \) is defined by

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

The \( A \rightarrow B \) merging cost for merging of the compound source \( X \) is defined analogously and denoted \( C_{m,\rightarrow}(X) \). 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 \( A \rightarrow B \) entanglement distillation rate for the AVQS \( X \) with classical communication rate \( R_c \), if there exists a sequence \( \{D_l\}_{l \in \mathbb{N}} \) of \( A \rightarrow B \) LOCC channels, each with a representation as given in (1) with \( D_l \) summands, such that the conditions...
1) \( \lim_{l \to \infty} \inf_{\rho \in \mathcal{S}} F(D_l(\rho), \phi_l) = 1 \)
2) \( \lim_{l \to \infty} \frac{1}{l} \log s(\phi_l) \geq R \)
3) \( \lim_{l \to \infty} \frac{1}{l} \log D_l \leq R_c \)

hold, where \( \phi_l \) 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

\[
D_{AV}^\delta(\mathcal{X}) := \sup \left\{ R : \text{R is achievable } A \to B \text{ distillation rate for the AVQS } \mathcal{X} \text{ with some classical rate } R_c \right\}.
\]

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 \( D_{AV}(\mathcal{X}) \). 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 \( \rho \).

**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 \( \mathcal{X} \subseteq \mathcal{S}(\mathcal{H}_{AB}) \) 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

\[
R_c = \sup_{\rho \in \mathcal{X}} I(A; E; \rho) + \delta,
\]

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 \( \rho \) 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 \( \sup_{\rho \in \mathcal{X}} S(A|B, \rho) = \sup_{\rho \in \mathcal{X}} S(\rho_A) + S(A|B, \rho) \) 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 \( \bar{s} := \sup_{\rho \in \mathcal{X}} S(A|B, \rho) \geq \frac{\delta}{2} \). The remaining case \( \bar{s} \geq 0 \) follows by simple modifications). Consider the sequence \( s_0 = 0 < s_1 < \ldots < s_N := \log d \) 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 \( \mathcal{X}_1, \ldots, \mathcal{X}_N \) of \( \mathcal{X} \) into pairwise disjoint subsets (some may be empty), defined

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

We further define sets \( \tilde{X}_i := \bigcup_{j \in \{i\}} \mathcal{X}_j \), where \( n(i) := \{ j \in [N] : |j - i| \leq 1 \} \). We construct an entropy estimating instrument \( \{ \mathcal{P}^{(i)} \}_{i \in [N]} \subset C^1(\mathcal{H}^\mathbb{R}_A, \mathcal{H}^\mathbb{R}_A) \) by defining

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

where \( P_{\lambda,l} \) is the projection supported on the invariant subspace of \( \mathcal{H}^\mathbb{R}_A \) belonging to the representation of \( \mathcal{S}_l \) labeled by Young frame \( \lambda \) and \( H(X) \) is the Shannon entropy of the probability distribution given by the normalized box-lengths \( \delta \). 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 \( l \),

\[
\sum_{j \in [N]} n(i) \log(\mathcal{P}^{(j)} \otimes id_{\mathcal{H}^\mathbb{R}_B})(\rho^{\mathbb{R}_B}) \leq 2^{-lc_2}
\]

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 \( X_i \neq \emptyset \) and large enough blocklength, there is a \((i, k_i, \tilde{D}^{(i)}) - A \to B \) merging \( \mathcal{M}^{(i)} \) with

\[
inf_{\rho \in \mathcal{X}_i} F_m(\rho^{\mathbb{R}_B}, \mathcal{M}^{(i)}) \geq 1 - 2^{-lc_3}
\]

with a positive constant \( c_3 > 0, k_i \geq 2^{-l^2} \) and, for each \( i \),

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

\[
\leq \inf_{\rho \in \mathcal{X}_i} I(A; E; \rho) + \frac{\delta}{2} + 3\eta.
\]

**Definition**

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

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

\[
\inf_{\rho \in \mathcal{X}} F_m(\rho^{\mathbb{R}_B}, \mathcal{M}_l) \geq 1 - 2^{-lc_4}
\]

with a positive constant \( c_4 \) for large enough blocklength. Since \( \eta \) and \( \delta \) are free to choose, we are done.
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 \( \text{conv}(\mathcal{X}) \). 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

\[
D_{AV}^+ (\mathcal{X}) = D_{\to} (\text{conv}(\mathcal{X}))
\]

\[
= \lim_{k \to \infty} \frac{1}{k} \max \inf \ D^{(1)} (\tau^k, T),
\]

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

\[
D^{(1)} (\sigma, \mathcal{E}) := \sum_{\lambda_j} \lambda_j (\sigma) \ I_c (X | Y, \hat{\sigma}_j)
\]

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

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 \( \text{conv}(\mathcal{X}) \).

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

\[
\sum_{s^l \in \mathcal{S}^l} f(s^l) q(s_1) \ldots q(s_l) \geq 1 - \gamma \quad (9)
\]

for each type \( q \) of sequences in \( \mathcal{S}^l \) for some \( \gamma \in [0,1] \), then

\[
\frac{1}{l!} \sum_{\sigma \in \mathcal{E}^l} f(\sigma(s^l)) \geq 1 - (l + 1)|\mathcal{S}| \cdot \gamma \quad \forall s^l \in \mathcal{S}^l. \quad (10)
\]

**Proof of Theorem 6** To show achievability, we first prove the assertion of the theorem for the case of a finite set \( \mathcal{X} := \{ \rho_s \}_{s \in \mathcal{S}} \). 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

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

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 \( p \in \mathcal{P}(\mathcal{X}) \) the fidelity is bounded

\[
F(\mathcal{D}_l (\rho_p^l), \phi_l) \geq 1 - 2^{-l c_5} \quad \text{with a constant } c_5 > 0 \quad \text{(in the proof of Theorem 8 in [7], it was shown, that each achievable rate can be achieved by protocols with exponentially decreasing error).}
\]

With \( f(s^l) := \rho_{s^l} \), and linearity of the fidelity in the first input, we yield

\[
\sum_{s^l} p_l (s^l) f(s^l) \geq 1 - 2^{-l c_5} \quad \text{for all } p \in \mathcal{P}(\mathcal{S}). \quad (11)
\]

Eq. (11) implies, that the function \( f \) satisfies the conditions of Lemma 7. Let \( \mathcal{U}_c \) be the (local) unitary channel, which permutes the tensor factors in \( \mathcal{H}_{AB}^\otimes l \) according to the permutation \( \sigma \), i.e. \( \rho_{s^l} (\sigma) = \mathcal{U}_c (\rho_{s^l}, \phi_l). \) From the above inequality and the polynomial growth of the function \( (l + 1)^{|\mathcal{S}|} \) 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 \( \{ \mathcal{D}_l \}_{l \in \mathbb{N}} \), introduced are not reasonable regarding the classical side communication cost, since \( A \) has to communicate the messages required within application of \( \mathcal{D}_l \) and the choice of permutation \( \sigma \) (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 (11) 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 \( \text{conv}(\mathcal{X}) \cap \partial \mathcal{S}(\mathcal{H}) = \emptyset \) (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 \( P_\eta \), i.e. the convex hull of a finite set \( \{ \tau_e \}_{e \in \mathcal{E}} \) of extreme points, such that \( \text{conv}(\mathcal{X}) \subset P_\eta \subset C(\mathcal{H}_{AB}) \) and

\[
d_H (\text{conv}(\mathcal{X}), P_\eta) < \eta. \quad (12)
\]

Applying the argument for finite sets given above to \( P_\eta \), we find, for each sufficiently large \( l \), a distillation protocol \( \mathcal{D}_l \), such that

\[
\min_{s^l \in \mathcal{E}^l} F(\mathcal{D}_l (\tau_e), \phi_l) \geq 1 - 2^{-l c_5} \quad \text{holds with a maximally entangled state } \phi_l, \quad \text{such that}
\]

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

Since \( \rho_s \) can be written as a convex combination of extremal points of \( P_\eta \), (13) implies

\[
\inf_{s^l \in \mathcal{S}^l} F(\mathcal{D}_l (\rho_{s^l}), \phi_l) \geq 1 - 2^{-l c_5}. \quad (15)
\]
By continuity properties of the function $D^{(1)}$ (see [8] for details), and (12) together with a (sufficiently small) choice of the parameter $\eta$, it holds
\[
\max_{\tau} \inf_{T} D^{(1)}(\tau \otimes \mathcal{T}, \mathcal{T}) \geq \max_{\tau} \inf_{\rho \in \text{conv}(X)} D^{(1)}(\rho \otimes k, \mathcal{T}) - \frac{k \delta}{2}
\]
which, together with (15) and (14) gives achievability. The converse is obvious, since each entanglement distillation protocol $\mathcal{D}_t$ which is $\epsilon$-good for the AVQS $\mathcal{X}$ is also $\epsilon$-good for entanglement generation of $\text{conv}(\mathcal{X})$, 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 $\text{conv}(\mathcal{X})$ breaks down. We demonstrate this by example.

Example 8. There exists a set $\mathcal{X}$, such that
\[
C_{m,\rightarrow}^{N}(\mathcal{X}) < C_{m,\rightarrow}(\text{conv}(\mathcal{X})).
\]
Consider the set $\tilde{\mathcal{X}} := \{ (\rho_{s})_{s=1}^{N} \subset \mathcal{S}(\mathcal{H}_{AB}) \}, N < \infty$, with
\[
\rho_{s} := (U_{s} \otimes \mathbb{1}_{\mathcal{H}_{B}}) \rho_{1} (U_{s}^{*} \otimes \mathbb{1}_{\mathcal{H}_{B}}) \quad (s \in [N])
\]
with $\rho_{1} \in \mathcal{S}(\mathcal{H}_{AB})$ such that $S(A|B, \rho_{1}) < 0$, and unitary matrices $U_{1} := \mathbb{1}_{\mathcal{H}_{A}}, U_{2}, \ldots, U_{N}$, such that the supports of the $A$ marginals of the states in $\tilde{\mathcal{X}}$ are pairwise orthogonal. We assume $\dim \mathcal{H}_{A} \geq N \cdot \text{supp}(\rho_{1,1})$. These definitions also imply for each $s, s' \in [N], s \neq s'$
\[
\rho_{bs,s} = \rho_{b,1,s}, \quad \text{and} \quad \text{supp}(\rho_{bs,s}) \perp \text{supp}(\rho_{bs,s'}). \quad (17)
\]
In the following, we show that for each set constructed in the above manner, it holds the relation $C_{m,\rightarrow}(\mathcal{X}) \leq C_{m,\rightarrow}(\text{conv}(\mathcal{X})) - \log N$ for the one-way merging cost. Moreover, each achievable entanglement cost can be achieved with classical communication rate $R_{c}$ such that $R_{c} \leq \sup_{\rho \in \text{conv}(\tilde{\mathcal{X}})} I(A; E, \rho) - \log N$ holds. From the orthogonality conditions (16) follows, that there is an instrument $\{ \hat{V}_{s} \}_{s=1}^{N}$ on $A$‘s system, such that
\[
\text{Var}(\rho_{s}) := \hat{V}_{s} \otimes \text{id}_{\mathcal{H}_{B}}(\rho_{s}) = \delta_{s,s'}(\rho_{1,1}) \quad (18)
\]
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 length $l$, an $(l, k, \hat{D}_{l})$ merging for $\rho_{1}$, with
\[
k_{l} \leq 2^{g(S(A|B, \rho_{1})+\delta)}, \quad \hat{D}_{l} \leq 2^{g(I(A; E, \rho_{1})+\delta)} \quad (19)
\]
and
\[
F_{m}(\rho_{1}^{\otimes l}, \mathcal{M}_{l}) \geq 1 - 2^{-l\epsilon} \quad (20)
\]
with a constant $\epsilon > 0$. Define $\mathcal{M}_{l} := \sum_{s=1}^{N} \tilde{U}_{s} \circ \hat{M}_{l} \circ V_{s}$, with $\tilde{U}_{s}(\cdot) := U_{s} \otimes \mathbb{1}_{\mathcal{H}_{B}}^{(s)} \otimes \mathbb{1}_{\mathcal{H}_{B}}^{(s')}$. It holds
\[
F_{m}(\rho_{s}^{\otimes l}, \mathcal{M}_{l}) = \sum_{s' \in [N]^{l}} F(\tilde{U}_{s'} \circ \hat{M}_{l} \circ V_{s'}, \mathcal{M}_{l} \otimes \text{id}_{\mathcal{H}_{E}}^{(s')}(\psi_{s'}), \phi_{l} \otimes \psi_{s'}) = \sum_{s' \in [N]^{l}} F(\hat{M}_{l} \otimes \text{id}_{\mathcal{H}_{E}}^{(s')}(\mathcal{V}_{s'}(\psi_{s'})), \phi_{l} \otimes \tilde{U}_{s'}^{(s')}(\psi_{s'})) = F_{m}(\rho_{1}^{\otimes l}, \mathcal{M}_{l}) \geq 1 - 2^{-l\epsilon}.
\]
for each $s' \in [N]^{l}$. 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 $(l, k_{l}, \hat{D}_{l})$-$A \rightarrow B$-merging with $D_{l} := N^{l}, \tilde{D}_{l}$, i.e.
\[
\frac{1}{l} \log \tilde{D}_{l} \leq I(A; E, \rho_{1}) + \log N. \quad (21)
\]
By properties of the set $\tilde{\mathcal{X}}$, i.e. (16) and (17), and the equality $S(\rho_{p}) = \sum_{l=1}^{N} p(s) S(\rho_{s}) + H(p)$ which holds for each $\rho_{p} := \sum_{l=1}^{N} p(s) \rho_{s}, p \in \mathcal{P}([N])$, due to orthogonality of the supports of the states, we infer by calculation of the entropies and maximization over $p$
\[
\max_{p \in \mathcal{P}([N])} S(A|B, \rho_{p}) = S(A|B, \rho_{1}) + \log N, \quad (22)
\]
\[
\max_{p \in \mathcal{P}([N])} I(A; E, \rho_{p}) = I(A; E, \rho_{1}) + 2 \log N. \quad (23)
\]
Eqs. (22) and (23) together with (19) and (21), show that $R_{q} = \max_{p \in \mathcal{P}([N])} S(A|B, \rho_{p}) - \log N$ is achievable with asymptotic classical side communication at rate
\[
R_{c} = \max_{p \in \mathcal{P}([N])} I(A; E, \rho_{p}) - \log N.
\]
ACKNOWLEDGMENTS

The authors are grateful to Igor Bjelaković for many stimulating discussions and valuable suggestions. The work of H.B. is supported by the DFG via grant BO 1734/20-1 and by the BMBF via grant 16BQ1050.

REFERENCES

[1] R. Ahlswede. Elimination of Correlation in Random Codes for Arbitrarily Varying Channels. Z. Wahrs. 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. Bjelakovic, 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. Bjelakovic, H. Boche, G. Janžen. Universal quantum state merging. J. Math. Phys. 54, 032204 (2013).
[8] H. Boche, G. Janžen. 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/1401.6065
[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).