# Universal Quantum State Merging

Igor Bjelaković, Holger Boche, Gisbert Janßen
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany
Email:{igor.bjelakovic, boche, gisbert.janssen}@tum.de

***Abstract*—We consider quantum state merging under uncertainty of the state held by the merging parties. More precisely we determine the optimal entanglement rate of a merging process when the state is unknown up to membership in a certain set of states. We find that merging is possible at the lowest rate allowed by the individual states.**

## I. Introduction

Like its classical archetype, quantum Shannon theory seeks to quantify information operationally by the amount of certain communication resources needed to store or transmit it. Success in this endeavour is in most cases strongly connected to understanding the meaning of and the interplay between different communication resources.

One of the interesting questions arising in this context is that of partial information. Let the output of a bipartite memoryless quantum source be distributed over two distant communication partners $A$ and $B$. How much communication is needed per copy to provide $B$ full knowledge of the source?

The answer was provided by Horodecki, Oppenheim and Winter imposing their quantum state merging task [1], [2], treating this communication issue under conversion of shared maximal entanglement and free classical communication (entanglement assisted LOCC).

The optimal ratio between input and output entanglement per copy of the state was identified as the conditional von Neumann entropy $S(A|B)$ of $\rho_{AB}$ given B. In this way, the conditional von Neumann entropy gets an operational meaning even for its negative values as the amount of quantum resources needed to perform the state merging task. Because of its generality, many communication tasks (especially multi-user problems) can be treated by modifying the quantum state merging protocol [2]. Here one must mention distributed compression, quantum source coding with side information at the decoder and entanglement generation over quantum multiple access channels.

However these results where established assuming idealized conditions. The authors of [1], [2] assumed the source to be memoryless and perfectly known. Both of these conditions will hardly be fulfilled in real-life communication settings.

In this paper we relax the second condition and determine the optimal average cost of entanglement under uncertainty of the state to merge. This means that the statistics of the systems emitted by the source are not perfectly known to the merging partners. Rather they only know that the state belongs to a certain set of states, so that they have to use a protocol which works well for every member of this set.

A version of the quantum state merging protocol that is robust in this sense is strongly desired because there is some hope that robust versions of protocols solving the above mentioned communication tasks can be derived from this result!

Our main technical result is a generalization of the original one-shot bound given in [2] which respects this kind of ignorance. Towards our goal we use techniques already known from earlier results dealing with universal coding of compound quantum channels (see [3], [4]).

This paper is organized as follows. In Sect. II we fix some notation which is used throughout the rest of the paper. Definitions and the main result of this paper are stated in Sect. III. Before we prove our result we establish a one shot bound in Sect. IV. After that we are able to prove the merging theorem in Sect. V. Due to limited space, most of the arguments we give are only sketches. For more detailed proofs we refer to [5].

## II. Notation and Conventions

All the Hilbert spaces which appear in this work are assumed to be finite dimensional and complex. For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, $\mathcal{B}(\mathcal{H})$ denotes the set of linear maps on $\mathcal{H}$ and $\mathcal{C}(\mathcal{H}, \mathcal{K})$ the set of quantum channels (i.e. completely positive and trace preserving maps) from $\mathcal{B}(\mathcal{H})$ to $\mathcal{B}(\mathcal{K})$. Because we mainly deal with systems containing several relevant subsystems, we will freely make use of the following convention: A Hilbert space $\mathcal{H}_{XYZ}$ is always thought to be the space of a composite system consisting of systems with Hilbert spaces $\mathcal{H}_X$, $\mathcal{H}_Y$ and $\mathcal{H}_Z$. We use a similar notation for states of composite systems. A state denoted $\rho_{XY}$ for instance is a bipartite state with marginals $\rho_X$ and $\rho_Y$ and so on.

We use the fidelity in its squared version, i.e.

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$$

for some quantum states $\rho$ and $\sigma$ on a Hilbert space $\mathcal{H}$. For the properties of this fidelity measure we refer to [6]. The von Neumann entropy of a state $\rho$ is given by

$$S(\rho) := -\mathrm{tr}(\rho \log \rho)$$

where $\log(\cdot)$ (as everywhere in this work) denotes the base two logarithm. We further denote the hermitean conjugate of an operator $a$ by $a^*$ and the complex conjugate of a complex number $z$ by $\overline{z}$.

## III. Definitions and Main Result

Let $\mathcal{X} \subseteq \mathcal{S}(\mathcal{H}_{AB})$ be a collection of bipartite states with subsystems distributed to (possibly) distant communication partners A and B. An $(l, k_l)$-merging for $\mathcal{X}$ is an LOCC-Channel

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

with local operations on the $A$- and the $B$-subscripted spaces, where $\mathcal{K}^i_A \simeq \mathcal{K}^i_B$ for $i = 1, 2$ and $k_l := \dim \mathcal{K}^0_A / \dim \mathcal{K}^1_A$. A real number $R$ is called an achievable *entanglement rate* for $\mathcal{X}$, if there exists a sequence of $(l, k_l)$-mergings with

1) $\limsup_{l\to\infty} \frac{1}{l} \log(k_l) \leq R$
2) $\inf_{\mathcal{X}_p} F(\mathcal{M}_l \otimes id_{\mathcal{H}_E}(\phi^l_0 \otimes \psi^{\otimes l}_{ABE}), \phi^l_1 \otimes \psi^{\otimes l}_{B'BE}) \to 1$ for $l \to \infty$.

where $\phi^l_0 \in \mathcal{S}(\mathcal{K}^0_{AB})$ and $\phi^l_1 \in \mathcal{S}(\mathcal{K}^1_{AB})$ are maximally entangled states on their spaces. The infimum in the second condition is evaluated over a set $\mathcal{X}_p$ which contains a purification $\psi_{ABE}$ on a space $\mathcal{H}_{ABE}$ for each $\rho_{AB}$ in $\mathcal{X}$. $\psi_{B'BE}$ is the state $\psi_{ABE}$ where the A-part is located on a Hilbert space $\mathcal{H}_{B'}$ under B's control. The fidelity measure in 2) is independent of the chosen purifications (which will be shown in the next section). We use the abbreviation

$$F_m(\rho, \mathcal{M}) := F(\mathcal{M} \otimes id_{\mathcal{H}_E}(\phi_0 \otimes \psi_{ABE}), \phi_1 \otimes \psi_{B'BE})$$

where the maximally entangled input and output states $\phi_0$ and $\phi_1$ are thought to be determined by $\mathcal{M}$. We further use a notation for the conditional von Neumann entropy indicating its state dependency. We write

$$S(A|B; \rho) := S(\rho) - S(\mathrm{tr}_A \rho)$$

for the conditional von Neumann entropy given $B$ of the state $\rho$ on $\mathcal{H}_{AB}$. The optimal entanglement rate $C_m(\mathcal{X})$, i.e.

$$C_m(\mathcal{X}) := \inf\{R : R \text{ is an achievable rate for } \mathcal{X}\}$$

is called *merging cost* of $\mathcal{X}$.
Our result is the following theorem which quantifies the merging cost of a set $\mathcal{X}$ of bipartite states.

*Theorem 1:* Let $\mathcal{X}$ be a collection of states on a bipartite Hilbert space. Then

$$C_m(\mathcal{X}) = \sup_{\rho\in\mathcal{X}} S(A|B; \rho). \qquad (1)$$

In light of the original result on perfectly known states this means: If an entanglement rate R is achievable for every state contained in a set $\mathcal{X}$, then this rate is achievable with merging schemes universal in the sense that they merge every state in the set faithfully.
We will only prove the achievability part of the above theorem (i.e. the RHS of eq. (1) is an upper bound for the merging cost). The converse part is a immediate consequence of the converse in the case of a single state given in [2].

## IV. One Shot Results

Surprisingly the merging protocol used in the original work is suitable for our purposes. In this section we derive a one-shot bound for the worst-case merging fidelity over a given set of bipartite states. This is done by generalizing the so-called decoupling bound to the case of a finite set of states to be merged. Such an approach was used earlier to determine the quantum capacity of compound quantum channels [3], [4] and the techniques used here are very similar.

### A. Properties of the Fidelity Measure

First we provide some facts concerning the merging fidelity measure.

*Lemma 2:* The following statements hold for the merging fidelity.

1) For a given merging operation, the merging fidelity does not depend on the purification of the state to merge.
2) The merging fidelity is convex as a function of the bipartite input state.

*Proof:* Let $\mathcal{M}$ a merging operation for the state $\rho$ (with corresponding underlying spaces assumed to be given). We show that the merging fidelity admits a representation

$$F(\mathcal{M} \otimes id_{\mathcal{H}_E}(\phi_0 \otimes \psi), \phi_1 \otimes \psi') = \sum_{z=1}^{Z} |\mathrm{tr}(w_z \rho)|^2 \qquad (2)$$

with some integer $Z$, where the operators $w_1, ..., w_Z$ depend only on $\mathcal{M}$ and the maximally entangled input and output states $\phi_0$, $\phi_1$. We remark here that the proof works for every channel $\mathcal{M}$. The function on the RHS of (2) does not depend on the chosen purification and clearly is a convex function of the state. Let

$$\mathcal{M}(\cdot) := \sum_{z=1}^{Z} m_z(\cdot) m^*_z \qquad (3)$$

be a Kraus decomposition of $\mathcal{M}$ with operators $m_z \in \mathcal{B}(\mathcal{K}^0_{AB} \otimes \mathcal{H}_{AB}, \mathcal{K}^1_{AB} \otimes \mathcal{H}_{B'B})$ for $z \in \{1, ..., Z\}$ and

$$|\psi\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}\, |e_i\rangle \otimes |f_i\rangle \qquad (4)$$

be the Schmidt decomposition of $\psi_{ABE}$ (we will omit the subscripts for brevity) with $\{e_i\}^r_{i=1}$ and $\{f_i\}^r_{i=1}$ orthonormal systems in $\mathcal{H}_A$ resp. $\mathcal{H}_B$. Because $\phi_0 \otimes \psi$ is a pure state, the fidelity on the LHS of (2) equals

$$\langle \phi_1 \otimes \psi, (\mathcal{M} \otimes id_{\mathcal{H}_E}(\phi_0 \otimes \psi))\phi_1 \otimes \psi\rangle. \qquad (5)$$

Decomposing this scalar product according to the Schmidt decomposition from eq. (4), elementary manipulations show that (5) equals

$$\sum_{i,j=1}^{r} \lambda_i \lambda_j \langle \phi_1 \otimes e_i, \mathcal{M}(\phi_0 \otimes |e_i\rangle\langle e_j|)\phi_1 \otimes e_j\rangle. \qquad (6)$$

With the help of the Kraus decomposition of $\mathcal{M}$ from (3) for every $i,j \in \{1,...,r\}$ we calculate

$$\begin{aligned}
&\langle \phi_1 \otimes e_i, \mathcal{M}(\phi_0 \otimes |e_i\rangle\langle e_j|)\phi_1 \otimes e_j\rangle \\
&= \sum_{z=1}^{Z} \langle \phi_1 \otimes e_i, m_z(\phi_0 \otimes |e_i\rangle\langle e_j|)m_z^*\phi_1 \otimes e_j\rangle \\
&= \sum_{z=1}^{Z} \langle r_z e_i, \phi_0 \otimes e_i\rangle \langle \phi_0 \otimes e_j, r_z e_j\rangle \qquad (7)
\end{aligned}$$

where $r_z$ for $z \in \{1,...,Z\}$ is the linear map defined by

$$r_z|v\rangle = m_z^*(|\phi_1\rangle \otimes |v\rangle).$$

Inserting the RHS of (7) to (5) and defining for every $z$ another linear map $w_z$ by

$$w_z|v\rangle := r_z^*(|\phi_0\rangle \otimes |v\rangle), \qquad (8)$$

we arrive at

$$\begin{aligned}
&F(\mathcal{M} \otimes id_{\mathcal{H}_E}(\phi_0 \otimes \psi), \phi_1 \otimes \psi) \\
&= \sum_{z=1}^{Z}\sum_{i,j=1}^{r} \lambda_i\lambda_j \overline{\langle w_z e_i, e_i\rangle}\langle w_z e_j, e_j\rangle \qquad (9)\\
&= \sum_{z=1}^{Z} |\mathrm{tr}(w_z\rho)|^2. \qquad (10)
\end{aligned}$$

■

### B. One-shot bound

For our purposes we consider merging LOCCs already used in [2]. Let $\rho_{AB}$ be a state on a bipartite Hilbert space $\mathcal{H}_{AB}$ (in the following we denote the dimension of $\mathcal{H}_A$ by $d_A$). For an integer $0 \leq L \leq d_A$ an *L-merging* is a channel

$$\mathcal{M} : \mathcal{B}(\mathcal{H}_{AB}) \to \mathcal{B}(\mathcal{K}_{AB}) \otimes \mathcal{B}(\mathcal{H}_{B'B})$$

of the form

$$\mathcal{M}(\rho) = \sum_{k=0}^{D} a_k \otimes u_k(\rho)a_k^* \otimes u_k^*, \quad (\rho \in \mathcal{S}(\mathcal{H}_{AB})) \qquad (11)$$

where $D := \lfloor \frac{d_A}{L} \rfloor$ and $\mathcal{K}_A$ and $\mathcal{K}_B$ Hilbert spaces $\dim \mathcal{K}_A = \dim \mathcal{K}_B = L$ and

- $\{a_k\}_{k=0}^D \subset \mathcal{B}(\mathcal{H}_A, \mathcal{K}_A)$ is a set of rank-$L$-partial isometries (except $a_0$ which has rank $d_A - L \cdot D < L$) with pairwise orthogonal initial subspaces
- $\{u_k\}_{k=0}^D \subset \mathcal{B}(\mathcal{H}_B, \mathcal{K}_B \otimes \mathcal{H}_{B'B})$ is a family of isometries.

For a purification $\psi_{ABE}$ of $\rho_{AB}$ on $\mathcal{H}_{ABE}$ and $k \in \{0,...D\}$ we define

$$p_k := \mathrm{tr}(a_k\rho_A a_k^*), \qquad \rho_{AE}^k := \mathrm{tr}_B(\mathcal{A}_k \otimes id_{\mathcal{H}_E}(\psi_{ABE})),$$

$\mathcal{A}_k(\cdot) := a_k(\cdot)a_k^*$ for all $k$. The following lemma, which is a restatement of Proposition 3 from [2], provides a lower bound on the merging fidelity.

*Lemma 3 (cf. [2]):* Let $\rho_{AB}$ be a bipartite state on $\mathcal{H}_{AB}$ and $\{a_k\}_{k=0}^D \subset \mathcal{B}(\mathcal{H}_A, \mathcal{K}_A)$ be a set of partial isometries as defined above (with parameter $L$). There exists a family $\{u_k\}_{k=0}^D$ of isometries completing $\{a_k\}_{k=0}^D$ to an *L-merging* (in the form given in (11)) such that

$$F(\mathcal{M} \otimes id_{\mathcal{H}_E}(\psi_{ABE}), \phi_L \otimes \psi_{B'BE}) \geq 1 - \tilde{Q}$$

where $\tilde{Q}$ is defined by

$$\tilde{Q} := 2\left(p_0 + \sum_{k=1}^{D} \|\rho_{AE}^k - \frac{L}{d_A}\pi_L \otimes \rho_E\|_1\right). \qquad (12)$$

The state $\phi_L$ here is the maximally entangled one on $\mathcal{K}_{AB}$, $\pi_L$ the maximally mixed state on $\mathcal{K}_A$ (i.e. $\pi_L := \frac{\mathbb{1}}{L}$) .

*Proof:* The proof is the same as in Proposition 3. Additionally we use that

$$\|\rho_{AE}^k - p_k\pi_L \otimes \rho_E\|_1 \leq 2 \cdot \|\rho_{AE}^k - \frac{L}{d_A}\pi_L \otimes \rho_E\|_1$$

for all $k$, which can be verified using the triangle inequality plus the fact that the trace distance for states does not exceed 2. ■

The above stated lemma will now be used to find an appropriate lower bound on the merging fidelity which holds for a given finite set of states $\mathcal{X} := \{\rho_{AB,i}\}_{i=1}^N$. The idea which leads to this bound can be described as follows. The convexity property of the merging fidelity (see Lemma 2) guarantees that a good bound on the merging fidelity of the arithmetic average state

$$\overline{\rho}_{AB} := \frac{1}{N}\sum_{i=1}^{N} \rho_{AB,i} \qquad (13)$$

gives us a fair bound on the worst-case merging fidelity for $\mathcal{X}$. Now let $\psi_{ABE,i}$ be any purification of $\rho_{AB,i}$ on a space $\mathcal{H}_{ABE}$ for every $i \in \{1,...,N\}$. Then

$$|\overline{\psi}_{ABR}\rangle\langle\overline{\psi}_{ABR}| := \frac{1}{N}\sum_{i,j=1}^{N} |\psi_{ABE,i}\rangle\langle\psi_{ABE,j}| \otimes |e_i\rangle\langle e_j| \qquad (14)$$

is a purification of $\overline{\rho}_{AB}$ on $\mathcal{H}_{ABR}$ with with $\{e_i\}_{i=1}^N$ being an orthonormal basis of $\mathbb{C}^N$ and $\mathcal{H}_R := \mathcal{H}_E \otimes \mathbb{C}^N$.

*Lemma 4:* Let $\{\rho_{AB,i}\}_{i=1}^N$ be a collection of states on $\mathcal{H}_{AB}$. Then for the corresponding averaged state $\overline{\rho}_{AB}$ and purifications $\psi_{ABE,1},...,\psi_{ABE,N}$, Lemma 3 holds with $\tilde{Q}$ replaced by

$$Q := 2\left(p_0 + \frac{1}{N}\sum_{k=1}^{D}\sum_{i,j=1}^{N} \sqrt{L_{ij} \cdot T_{i,j}^{(k)}}\right) \qquad (15)$$

where $L_{ij} := L \cdot \min_{k \in \{i,j\}}\{\mathrm{rank}(\rho_{E,k})\}$ and

$$T_{i,j}^{(k)} := \|\rho_{AE,ij}^k - \frac{L}{d_A}\pi_L \otimes \rho_{E,ij}\|_2^2. \qquad (16)$$

We further used the definitions

$$\psi_{ABE,ij} := |\psi_{ABE,i}\rangle\langle\psi_{ABE,j}|, \ \rho_{E,ij} := \mathrm{tr}_{AB}(\psi_{ABE,ij}),$$
$$\rho_{AE,ij}^k := \mathrm{tr}_B((a_k \otimes id_{\mathcal{H}_E})\psi_{ABE,ij}(a_k^* \otimes id_{\mathcal{H}_E}))$$

for $i,j \in \{1,...,N\}, k \in \{1,...,D\}$.

*Proof:* We bound the trace distance terms on the RHS of (12) for $\overline{\rho}_{AB}$ with its purification introduced in eq. (14). Explicitly we have

$$\begin{aligned}&\|\overline{\rho}^k_{AR} - \frac{L}{d_A}\pi_L \otimes \overline{\rho}_R\|_1\\ \le& \frac{1}{N}\sum_{i,j=1}^N \sqrt{L_{ij}}\|\rho^k_{AE,ij} - \frac{L}{d_A}\pi_L \otimes \rho_{E,ij}\|_2.\end{aligned}$$

The above inequality results from inserting (14), the linearity of the involved maps along with multiplicativity of the trace norm and the triangle inequality. Furthermore we used the well-known relation $\|X\|_1 \le \sqrt{r}\|X\|_2$ which holds for any operator $X$ of rank $r$. ■

The rest of this section is devoted to proving that there exists a merging protocol with fidelity bounded from below in an appropriate way. To this end we show that random selection of $L$-mergings from a certain set results in a good mean merging fidelity.

Let $L \in \{1, ..., d_A\}$ be given. We construct a set of $L$-mergings parametrized by the elements of $\mathfrak{U}(\mathcal{H}_A)$, the group of unitary operators on $\mathcal{H}_A$. Let $\{a_k\}_{k=0}^D$ be a set of Kraus operators suitable for forming an $L$-merging and $U$ a random variable with values in $\mathfrak{U}(\mathcal{H}_A)$ which is distributed according to the Haar measure. Then $\{a_k(U)\}_{k=0}^D$, defined by $a_k(u) := a_k u$ for every $k \in \{0, ..., D\}, u \in \mathfrak{U}(\mathcal{H}_A)$ is a random set of partial isometries suitable for forming an $L$-merging. In this way for every $u \in \mathcal{U}(\mathcal{H}_A)$ we get an $L$-merging $\mathcal{M}_u$ if we combine $\{a_k(u)\}_{k=0}^D$ with a family of isometries $\{u_k(u)\}_{k=0}^D$ which fulfills the bound in Lemma 3. The expected merging fidelity under random selection of these LOCCs bounded in the following lemma.

*Lemma 5:* For a family $\{\rho_{AB,i}\}_{i=1}^N$ and $\psi_{ABE,i}$ a purification of $\rho_{AB,i}$ on $\mathcal{H}_{ABE}$ for each $i$,

$$\begin{aligned}&\mathbb{E}\{F(\overline{\rho}_{AB}, \mathcal{M}_U)\}\\ &\quad\ge 1 - 2\left(\frac{L}{d_A} + 2\cdot\sum_{i=1}^N \sqrt{L\cdot \mathrm{rank}(\rho_{E,i})\|\rho_{B,i}\|_2^2}\right)\end{aligned}$$

where $\mathbb{E}$ denotes the expectation according to the Haar measure on $\mathcal{U}(\mathcal{H}_A)$.

To prove our claim we need the help of the following two lemmas.

*Lemma 6 ([3]):* Let $L$ and $D$ be $N \times N$-matrices with nonnegative entries such that

$$L_{jl} \le L_{jj},\ L_{jl} \le L_{ll} \text{ and } D_{ij} \le \max\{D_{ii}, D_{jj}\}$$

for all $i, j \in \{1, ..., N\}$. Then

$$\sum_{i,j=1}^N \frac{1}{N}\sqrt{L_{ij}D_{ij}} \le 2\sum_{i=1}^N \sqrt{L_{ii}D_{ii}}$$

*Lemma 7:* Let $\tau$ and $\xi$ be elements of a bipartite Hilbert space $\mathcal{H} \otimes \mathcal{H}'$. Then

$$\|\mathrm{tr}_{\mathcal{H}'}(|\tau\rangle\langle\xi|)\|_2^2 \le \max_{\chi\in\{\tau,\xi\}} \|\mathrm{tr}_{\mathcal{H}'}(|\chi\rangle\langle\chi|)\|_2^2$$

*Proof:* The proof is based on elementary arguments and is carried out in [5]. ■

*Proof of Lemma 5:* Using Lemma 4 we get

$$F_m(\overline{\rho}_{AB}, \mathcal{M}_U) \ge 1 - Q_U$$

for the random $L$-merging $\mathcal{M}_U$ and random error

$$Q_U := 2\left(p_0(U) + \frac{1}{N}\sum_{k=1}^D\sum_{i,j=1}^N \sqrt{L_{ij}\cdot T^{(k)}_{i,j}(U)}\right).$$

Here $p_0(U) := \mathrm{tr}(a_0(U)\rho_A a_0(U))$,

$$T^{(k)}_{i,j}(U) := \|\rho^k_{AE,ij}(U) - \frac{L}{d_A}\pi_L \otimes \rho_{E,ij}\|_2^2 \quad \text{and}$$

$$\begin{aligned}&\rho^k_{AE,ij}(U) :=\\ &\qquad (a_k(U)\otimes id_{\mathcal{H}_E})\mathrm{tr}_B(\psi_{ABE,ij})(a_k(U)\otimes id_{\mathcal{H}_E})^*.\end{aligned}$$

With the help of Jensen's inequality

$$\begin{aligned}&\mathbb{E}_U\{Q_U\}\\ &\le 2\left(\mathbb{E}_U\{p_0(U)\} + \frac{1}{N}\sum_{k=1}^D\sum_{i,j=1}^N \sqrt{L_{ij}\cdot \mathbb{E}\{T^{(k)}_{i,j}(U)\}}\right).\end{aligned}$$

It remains to bound the expectations of $T^k_{i,j}(U)$ and $p_0(U)$. This was already done in [2], we have

$$\mathbb{E}\{T^k_{i,j}(U)\} \le \frac{L^2}{d_A^2}\|\mathrm{tr}_B(|\psi_{ABE,i}\rangle\langle\psi_{ABE,j}|)\|_2^2$$

and $\mathbb{E}\{p_0(U)\} \le \frac{L}{d_A}$. Therefore, abbreviating $D_{ij} := \|\mathrm{tr}_B(|\psi_{ABE,i}\rangle\langle\psi_{ABE,j}|)\|_2^2$,

$$\mathbb{E}_U\{Q_U\} \le 2\left(\frac{L}{d_A} + \frac{1}{N}\sum_{k=1}^D\sum_{i,j=1}^N \sqrt{L_{ij}\cdot\frac{L^2}{d_A^2}D_{ij}}\right) \quad (17)$$

$$\le 2\left(\frac{L}{d_A} + \frac{1}{N}\sum_{i,j=1}^N \sqrt{L_{ij}D_{ij}}\right). \quad (18)$$

The second inequality follows from the fact that the summands on the RHS of (17) are independent of $k$ and $D\frac{L}{d_A} \le 1$ by the definition of $D$. By the definition of $L_{ij}$ clearly $L_{ij} = \min\{L_{ii}, L_{jj}\}$ for all $i, j$ and so the first assumption of Lemma 6 is fulfilled. The second assumption (i.e. $D_{ij} \le \max\{D_{ii}, D_{jj}\}$) is a direct consequence of Lemma 7. Using Lemma 6, we obtain

$$\mathbb{E}_U\{Q_U\} \le 2\left(\frac{L}{d_A} + 2\sum_{i=1}^N \sqrt{L\cdot\mathrm{rank}(\rho_{E,i})\|\rho_{B,i}\|_2^2}\right).$$

Note that we replaced $\|\rho_{AE,i}\|_2$ by $\|\rho_{B,i}\|_2$ for every $i$, which is admissible because $\rho_{B,i}$ and $\rho_{AE,i}$ have the same eigenvalues. ■

*Remark 8:* Lemma 5 provides our desired bound on the worst-case merging fidelity of the set. Explicitly, if $F_m(\overline{\rho}_{AB}, \mathcal{M}) \ge 1-\epsilon$, the convexity property shown in Lemma 2 guarantees

$$\min_{i\in\{1,...,N\}} F_m(\rho_{AB,i}, \mathcal{M}) \ge 1 - N\epsilon$$

## V. Proof of Main result

In this section we prove the optimal merging rate theorem using our one-shot result from Lemma 5.

### A. Typical subspaces

Here we state some properties of the so-called frequency typical projections which will be needed in the achievability proof. The concept of typicality is standard in classical and quantum information theory. Therefore we state just the needed properties which can be found (along with basic definitions) in [3].

*Lemma 9:* There exists a real number $c > 0$ such that for every Hilbert space $\mathcal{H}$ of dimension $d$ the following holds: For any state $\rho$ on $\mathcal{H}$, $\delta \in (0, \frac{1}{2})$ and $l \in \mathbb{N}$ there is a projection $q_{\delta,l} \in \mathcal{B}(\mathcal{H}^{\otimes l})$ (its so-called *frequency typical projection)* with

1) $\mathrm{tr}(q_{\delta,l}\rho^{\otimes l}) \geq 1 - 2^{-l(c\delta^2 - h(l))}$
2) $q_{\delta,l}\rho^{\otimes l} q_{\delta,l} \leq 2^{-l(S(\rho)-\varphi(\delta))} q_{\delta,l}$
3) $2^{l(S(\rho)-\varphi(\delta)-h(l))} \leq \mathrm{rank}(q_{\delta,l}) \leq 2^{l(S(\rho)+\varphi(\delta)+h(l))}$

where the functions $\varphi(\delta) \to 0$ for $\delta \to 0$ and $h(l) \to \infty$ for $l \to \infty$. Explicitly they are given by

$$h(l) = \frac{d}{l}\log(d+1); \quad \varphi(\delta) = -\delta\log(\frac{\delta}{d})$$

for all $l \in \mathbb{N}$ and $\delta \in (0, \frac{1}{2})$.

### B. Achievability

Now we use our results from the previous sections for the achievability proof. We first consider a finite set $\mathcal{X} := \{\rho_{AB,i}\}_{i=1}^N \subset \mathcal{S}(\mathcal{H}_{AB})$ with purifications $\psi_{ABE,1}, ..., \psi_{ABE,N}$ on $\mathcal{H}_{ABE}$. For these states we introduce some sort of "typical reductions". We define

$$|\tilde{\psi}^{l,\delta}_{ABE,i}\rangle := \frac{1}{w_{i,\delta,l}} \tilde{q}_{i,\delta,l} \, |\psi_{ABE,i}\rangle^{\otimes l},$$

where $w_{i,\delta,l} := \sqrt{\mathrm{tr}(\tilde{q}_{i,\delta,l}\psi^{\otimes l}_{ABE,i})}$ for all $i \in \{1, ..., N\}, l \in \mathbb{N}$ and $\delta \in (0, \frac{1}{2})$. Here $\tilde{q}_{i,\delta,l}$ is given by the typical projectors $q_{A,i}$, $q_{B,i}$ and $q_{E,i}$ of the corresponding marginals of $\psi_{ABE,i}$

$$\tilde{q}_{i,\delta,l} := q_{A,i} \otimes q_{B,i} \otimes q_{E,i}$$

(with subscripts $\delta, l$ omitted for the sake of brevity).

*Theorem 10:* For a finite collection $\mathcal{X} := \{\rho_{AB,i}\}_{i=1}^N$ of states on $\mathcal{H}_{AB}$ it holds

$$C_m(\mathcal{X}) \leq \max_{i\in\{1,\ldots,N\}} S(A|B;\rho_{AB,i}).$$

*Proof:* The proof is similar to the corresponding one in [2], but uses the one-shot bound of Lemma 5. We show for all $\epsilon > 0$, that the number $\max_{i\in\{1,\ldots,N\}} S(A|B;\rho_{AB,i}) + \epsilon$ is an achievable rate for a merging of $\mathcal{X}$. First assume, that $\max_{i\in\{1,\ldots,N\}} S(A|B;\rho_{AB,i}) \leq 0$. Let $\delta \in (0, \frac{1}{2})$ such that $\frac{\epsilon}{5} < \varphi(\delta)$. Choose

$$L_l = \lfloor 2^{-l(\max_{i\in\{1,..,N\}} S(A|B;\rho_{AB,i})+\epsilon)} \rfloor. \tag{19}$$

If we now consider a merging LOCC $\mathcal{M}_l$ according to Section IV-B with subspace parameter $L_l$, we can bound the merging fidelity for the typical reductions of the states in $\mathcal{X}$ from below. To bound the average merging fidelity in Lemma 5 in the case of the typical reduced states we need the bounds

$$\frac{L_l}{\dim(\mathcal{H}_A^{\otimes l})} \leq 2^{-l(6\varphi(\delta)+h(k))},$$

$$\sqrt{L \cdot \mathrm{rank}(\tilde{\rho}_{E,i,\delta})\|\tilde{\rho}_{B,i,\delta}\|_2^2} \leq N \cdot \frac{2^{-\frac{k}{2}(\varphi(\delta)-2h(k))}}{1 - 4\cdot 2^{-l(c\delta^2-h(k))}}$$

which are obtained mainly by using the properties of the typical projections (see Lemma 9). These bounds, Lemma 5 and Remark 8 show that

$$\min_{1\leq i\leq N} F(\mathcal{M}_l \otimes id_{\mathcal{H}_E^{\otimes n}}(\tilde{\psi}^{l,\delta}_{ABE,i}), \phi_{L_l} \otimes \tilde{\psi}^{l,\delta}_{B'BE,i}) \geq 1 - f(l)$$

where $f$ is in $o(2^{-cl})$ with a positive constant $c$ depending on $\delta$ and $N$. The desired bound for the merging fidelity of the original set $\mathcal{X}$ basically follows from Winter's gentle measurement Lemma (cf. [7], Lemma 9). Explicitly, it holds

$$\min_{1\leq i\leq N} F(\rho^{\otimes l}_{AB,i}, \mathcal{M}_l) \geq 1 - 2\sqrt{f(l)} - 2\sqrt{8 \cdot w_{i,\delta,l}}.$$

It remains to verify the claim given that $\max_{i\in\{1,\ldots,N\}} S(A|B;\rho_{AB,i}) > 0$. This is easily done using the above argument and providing additional shared entanglement. Instead of the set $\{\rho_{AB,i}\}_{i=1}^N$ we consider the set $\{\phi \otimes \rho_{AB,i}\}_{i=1}^N$ where $\phi$ is a maximally entangled state of Schmidt-rank $2^{\lceil \max_{i\in\{1,\ldots,N\}} S(A|B;\rho_{AB,i})\rceil}$. The maximum conditional von Neumann entropy of this set clearly is negative and the above argument for the negative case can be used to show that the error is decreasing exponentially. ■

An extension of these results to arbitrary sets of states can be done by methods of discrete approximation (see [5] for a detailed proof). The set $\mathcal{X}$ is approximated by a sequence of nets (which are clearly finite). The cardinality of the nets can be chosen to increase polynomially in $l$. Since the error decreases exponentially, the claim holds as well.


## Acknowledgments

The authors gratefully acknowledge the support of the TUM Graduate School / Faculty Graduate Center FGC-EI at Technische Universität München, Germany. The work of I.B. and H.B. is supported by the DFG via grant BO 1734/20-1 and by the BMBF via grant 01BQ1050.


## References


[1] M. Horodecki, J. Oppenheim and A. Winter, "Partial quantum information", *Nature*, vol. 436, pp. 673–676, 2005.

[2] M. Horodecki, J. Oppenheim and A. Winter, "Quantum state merging and negative information", *Comm. Math. Phys.*, vol. 269, no. 1, pp. 107–136, 2007, arXiv:quant-ph/0512247.

[3] I. Bjelaković, H. Boche and J. Nötzel, "Quantum capacity of a class of compound channels", *Phys. Rev. A*, vol. 78, p. 042331, 2008.

[4] I. Bjelaković, H. Boche and J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Comm. Math. Phys.*, vol. 292, pp. 55–97, 2009. arXiv:0811.4588 [quant-ph].

[5] G. Janßen, "Universelles quanten- state merging", Diploma thesis, TU Berlin, 2010, available at: http://www.lti.ei.tum.de/fileadmin/w00bgd/www/pdf/DA.pdf

[6] R. Jozsa, "Fidelity for mixed quantum states", *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[7] A. Winter, "Coding theorem and strong converse for quantum channels", *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999.