Upper Bounds on the Distillable Randomness of Bipartite Quantum States

Lami, L.; Regula, B.; Wang, X.; Wilde, M.M.

DOI
10.1109/ITW55543.2023.10161613

Publication date
2023

Document Version
Other version

Published in
2023 IEEE Information Theory Workshop (ITW 2023)

Citation for published version (APA):
https://doi.org/10.1109/ITW55543.2023.10161613
Upper Bounds on the Distillable Randomness of Bipartite Quantum States

Ludovico Lami†‡, Bartosz Regula†‡, Xin Wang§, and Mark M. Wilde¶

* Institute for Theoretical Physics, Korteweg–de Vries Institute for Mathematics, and QuSoft, University of Amsterdam, the Netherlands. Email: ludovico.lami@gmail.com
† Institute for Theoretical Physics and IQST, University of Ulm, Albert-Einstein-Allee 11, D-89069 Ulm, Germany
‡Department of Physics, Graduate School of Science, The University of Tokyo, Bunkyo-ku, Tokyo 113-0033, Japan. Email: bartosz.regula@gmail.com
§Institute for Quantum Computing, Baidu Research, Beijing 100193, China. Email: wangxin felix@gmail.com
¶School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA. Email: wilde@cornell.edu

Abstract—The distillable randomness of a bipartite quantum state is an information-theoretic quantity equal to the largest net rate at which shared randomness can be distilled from the state by means of local operations and classical communication. This quantity has been widely used as a measure of classical correlations, and one version of it is equal to the regularized Holevo information of the ensemble that results from measuring one share of the state. However, due to the regularization, the distillable randomness is difficult to compute in general. To address this problem, we define measures of classical correlations and prove a number of their properties, most importantly that they serve as upper bounds on the distillable randomness of an arbitrary bipartite state. We then further bound these measures from above by some that are efficiently computable by means of semi-definite programming, we evaluate one of them for the example of an isotropic state, and we remark on the relation to quantities previously proposed in the literature.

Full version at https://markwilde.com/RD-bnds.pdf

I. INTRODUCTION

The distillable randomness of a bipartite quantum state is equal to the largest net rate at which uniformly random, perfectly correlated bits can be distilled from the state by means of local operations and one-way classical communication (1W-LOCC) [1]. That is, in this scenario, the net rate is the rate at which shared randomness is distilled minus the rate at which classical bits are communicated to accomplish the task. It is important to subtract the classical communication rate, as failure to do so would trivialize the task, allowing for an infinite number of random bits to be shared. This task fundamentally has its roots in classical information theory [2], [3]. Here we also extend the task to allow for general local operations and classical communication (LOCC).

The distillable randomness of a bipartite state is considered a fundamental measure of classical correlations contained in a state. There has been a large literature on this topic, starting with [4], [5] and reviewed in [6], due to the wide interest in understanding correlations present in quantum states. However, [1] is the one of the few papers to consider understanding these correlations in an information-theoretic manner (see also [7]–[13] for other perspectives and related works).

Ref. [1] provided a formal solution for the aforementioned information-theoretic task. However, like many such formal solutions in quantum Shannon theory, it does not provide a computationally efficient procedure for quantifying correlations because it is expressed as a multi-letter or regularized formula. Our goal here is to fill this void by providing upper bounds on the distillable randomness that are efficiently computable by semi-definite programming. We also justify how some of the newly proposed measures are themselves measures of classical correlations contained in a bipartite state.

Although our results here can be viewed as a static counterpart to the results in the dynamical setting from [14]–[17], their derivation requires some new insights, as we explain in detail below. Ref. [17] proved that generalizations of the dynamical measures from [14]–[16] give upper bounds on the rate at which classical messages be communicated from one party to another, whenever they have access to a bipartite channel as a communication resource. A special case of this setting is when a sender is communicating classical messages to a receiver, with the assistance of a classical feedback channel. In contrast, as described earlier, our static setting here involves two parties distilling shared randomness from a bipartite state, by means of 1W-LOCC or general LOCC.

We comment here on the novel contributions of our paper when compared to earlier works such as [14]–[17]. The main measures of classical correlations proposed here, denoted by γ, Cγ, and Τ in Section III, are inspired by the measures that have appeared earlier in [14]–[17], denoted there by β, Cβ, and Υ. However, the measures proposed here are symmetric with respect to a swap of the A and B systems. This property is critical for bounding the LOCC-assisted distillable randomness from above, as accomplished in Theorems 11 and 12. Furthermore, we prove here that these measures obey the classical communication bound in Proposition 7, also known as a “non-lockability” property in prior work on correlation measures [18], [19]. Finally, Lemma 9 and Proposition 10 are critical bounds that allow us to compare the actual state at the end of a randomness distillation protocol with an ideal state, and they ultimately lead to a strong converse upper bound.
for the distillable randomness. For the task of randomness
distillation, the target (ideal) state is a mixed state, which is
in distinction to most prior works on quantum resource theories,
in which the target state is necessarily pure \([20]–[22]\). So the
approach we have taken here goes beyond methods previously
applied in such contexts and could potentially be useful more
generally in research on quantum resource theories. We note
here that similar methods were employed in \([23]\), \([24]\), but
Lemma 9 and Proposition 10 provide a comparison between
the ideal mixed state of interest and a convex set of positive
semi-definite operators, rather than a comparison between an
ideal mixed state and just one other mixed state.

The rest of the paper is organized as follows. In Section II
we introduce some notation and key concepts. In Section III
we construct and study certain classical correlation measures,
while in Section IV we define the distillable randomness of
a bipartite state. Continuing, in Section V we prove that
the proposed measures are upper bounds on the distillable
randomness. For the task of randomness

\(C_{\gamma}(\sigma_{AB}) := \log_2 \gamma(\sigma_{AB}).\)

For a bipartite state \(\rho_{AB}\), we then define

\(\Gamma(\rho_{AB}) := \inf_{\sigma_{AB} \geq 0; \gamma(\sigma_{AB}) \leq 1} D(\rho_{AB} \| \sigma_{AB}),\)

which follows an approach for defining resource measures pro-
posed originally by \([27]–[29]\) in the context of entanglement
theory. Also, as a consequence of the scaling and zero-value
properties listed above, we conclude that

\(\Gamma(\rho_{AB}) \leq D(\rho_{AB} \| \rho_{AB}/(\gamma(\rho_{AB}))) = C_{\gamma}(\rho_{AB}).\)

Our goal is to show that \(\Gamma(\rho_{AB})\) is an upper bound on the
distillable randomness of a bipartite state \(\rho_{AB}\). We do so in
Section VI after proving various properties of \(\gamma\), \(C_{\gamma}\), and \(\Gamma\), in Section III–A.

A. Properties of Classical Correlation Measures

In this section, we establish a number of properties of the
quantities \(\gamma\), \(C_{\gamma}\), and \(\Gamma\), proposed in Section III. In particular,
we prove that these measures satisfy several properties
expected for a measure of classical correlations of a bipartite
state, including

1) symmetry under exchange of \(A\) and \(B\) (Proposition I).
2) data processing under local channels (Proposition II).
3) local isometric invariance (Corollary III).
4) non-negativity, faithfulness for product states (Proposition IV).
5) dimension bound (Proposition V).
6) scale invariance (Proposition VI).
7) classical communication bound (Proposition VII).
8) subadditivity (Proposition VIII), and
9) continuity near maximally classically correlated states
(Proposition IX).

Proposition I (Exchange Symmetry): Let \(\sigma_{AB}\) be a bipartite
positive semi-definite operator, and let \(\rho_{AB}\) be a state. Then

\(C_{\gamma}(A; B)_{\sigma} = C_{\gamma}(B; A)_{\sigma},\)  

\(\Gamma(A; B)_{\rho} = \Gamma(B; A)_{\rho}.\)

Proof. This follows by inspecting the definitions and using
the fact that, for a Hermitian operator \(W_{AB}\), the inequality
\(T_B(W_{AB}) \geq 0\) holds if and only if \(T_A(W_{AB}) \geq 0\) does. ■

Proposition 2 (Data-Processing under Local Channels): Let \(\sigma_{AB}\) be a bipartite positive semi-definite operator, and let \(\mathcal{N}_{A \rightarrow A'}\) and \(\mathcal{M}_{B \rightarrow B'}\) be quantum channels. Then

\(C_{\gamma}(A; B)_{\sigma} \geq C_{\gamma}(A'; B')_{\omega},\)  

\(\Gamma(A; B)_{\rho} \geq \Gamma(A'; B')_{\rho},\)

where \(\omega_{A'B'} := (\mathcal{N}_{A \rightarrow A'} \otimes \mathcal{M}_{B \rightarrow B'})(\rho_{AB}).\)

Proof. See Appendix A. ■

Corollary 3 (Local Isometric Invariance): Let \(\sigma_{AB}\) be a bipartite
positive semi-definite operator, \(\mathcal{U}_{A \rightarrow A'}\) an isometric
channel, and \(\mathcal{V}_{B \rightarrow B'}\) an isometric channel. Then

\(C_{\gamma}(A; B)_{\sigma} = C_{\gamma}(A'; B')_{\omega},\)
\[ \Gamma(A; B)_\sigma = \Gamma(A'; B')_\omega, \]  

(11)

where \( \omega_{A'B'} := (U_{A' \rightarrow A} \otimes V_{B' \rightarrow B})(\sigma_{AB}) \).

**Proof.** The inequality \( C_\gamma(A; B)_\sigma \geq C_\gamma(A'; B')_\omega \) follows by a direct application of Proposition 2. Let us define the channels

\[ \mathcal{L}_{A' \rightarrow A}(\cdot) := (U_{A' \rightarrow A})^\dagger(\cdot) + \text{Tr}[|U_{A' \rightarrow A}|^2](\cdot)\tau_A, \]

\[ \mathcal{M}_{B' \rightarrow B}(\cdot) := (V_{B' \rightarrow B})^\dagger(\cdot) + \text{Tr}[|V_{B' \rightarrow B}|^2](\cdot)\eta_B, \]

(12)

where \( \tau_A \) and \( \eta_B \) are arbitrary quantum states. Consider that \( \mathcal{L}_{A' \rightarrow A} \circ \mathcal{U}_{A' \rightarrow A} = \text{id}_A \) and \( \mathcal{M}_{B' \rightarrow B} \circ \mathcal{V}_{B' \rightarrow B} = \text{id}_B \). Then the opposite inequality also follows by applying Proposition 2.

Let \( \rho_{AB} \) be a bipartite state. Then \( C_\gamma(A; B)_\rho \) and \( \Gamma(A; B)_\rho \) are non-negative, i.e.,

\[ C_\gamma(A; B)_\rho \geq 0, \quad \Gamma(A; B)_\rho \geq 0, \]

(14)

and equal to zero if \( \rho_{AB} = \sigma_A \otimes \tau_B \) is a product state. Furthermore, \( C_\gamma \) is faithful, i.e., \( C_\gamma(\rho_{AB}) = 0 \) implies that \( \rho_{AB} \) is a product state, and \( \Gamma \) is faithful provided that the underlying divergence \( D \) is itself faithful (positive definite) and also lower semicontinuous in its second argument.

**Proof.** See Appendix B. 

**Proposition 5 (Dimension Bound):** Let \( \rho_{AB} \) be a bipartite state. Then

\[ \Gamma(A; B)_\rho \leq C_\gamma(A; B)_\rho \leq \log_2 \min\{d_A, d_B\}, \]

(15)

where \( d_A \) and \( d_B \) denote the dimensions of the local systems.

**Proof.** See Appendix D. 

**Proposition 6 (Scale Invariance):** Let \( \sigma_{AB} \) be a positive semi-definite, bipartite operator, and let \( c > 0 \). Then

\[ \gamma(c \sigma_{AB}) = c \gamma(\sigma_{AB}). \]

(16)

**Proof.** Let \( K_A, L_B, \) and \( V_{AB} \) be arbitrary choices for the optimization problem for \( \gamma(\sigma_{AB}) \). Then \( cK_A, L_B, \) and \( cV_{AB} \) are particular choices for which the objective function evaluates to \( \text{Tr}[cK_A \otimes L_B] = c \text{Tr}[K_A \otimes L_B] \) and such that the constraints for \( \sigma_{AB} \) hold. It follows then that \( \gamma(c \sigma_{AB}) \leq c \gamma(\sigma_{AB}) \). To see the opposite inequality, consider applying this again to find that \( \gamma(c^{-1} \sigma_{AB}) \leq c^{-1} \gamma(\sigma_{AB}) \), which is equivalent to \( c \gamma(\sigma_{AB}) \leq \gamma(c \sigma_{AB}) \). 

**Proposition 7 (Classical Communication Bound):** Let \( \rho_{XAB} \) be a tripartite state, for which system \( X \) is classical, i.e.,

\[ \rho_{XAB} := \sum_x p(x)|x\rangle\langle x|_X \otimes \rho_{AB}^x, \]

(17)

where \( \{p(x)\}_x \) is a probability distribution and \( \{\rho_{AB}^x\}_x \) is a set of states. Then

\[ C_\gamma(AX; B)_\rho \leq \log_2 d_X + C_\gamma(A; BX)_\rho, \]

(18)

\[ \Gamma(AX; B)_\rho \leq \log_2 d_X + \Gamma(A; BX)_\rho, \]

(19)

**Proof.** See Appendix E. 

**Proposition 8 (Subadditivity):** Let \( \rho_{A_1A_2B_1B_2} := \sigma_{A_1B_1} \otimes \tau_{A_2B_2} \), where \( \sigma_{A_1B_1} \) and \( \tau_{A_2B_2} \) are bipartite operators. Then the following subadditivity inequality holds

\[ C_\gamma(A_1A_2; B_1B_2)_\rho \leq C_\gamma(A_1; B_1)_\sigma + C_\gamma(A_2; B_2)_\tau. \]

(20)

**Proof.** See Appendix F. 

**Lemma 9:** The following bound holds:

\[ \sup_{\sigma_{AB} \geq 0; \gamma(\sigma_{AB}) \leq 1} F\left( \Phi_{AB}^d, \sigma_{AB} \right) \leq \frac{1}{d}, \]

(22)

where \( \Phi_{AB}^d \) is the maximally classical correlated state from (11) and \( F(\omega, \tau) := \sqrt{\text{Tr} [\sqrt{\omega} \sqrt{\tau}]} \) is the fidelity of states \( \omega \) and \( \tau \) [30].

**Proof.** See Appendix G. 

Recall that the sandwiched Rényi relative entropy of a state \( \rho \) and a positive semi-definite operator \( \sigma \) is defined for \( \alpha \in (0, 1) \cup (1, \infty) \) as [31, 32]

\[ D_\alpha(\rho||\sigma) := \frac{2\alpha}{\alpha-1} \log_2 \left( \sigma^{(1-\alpha)/2} \rho^{1/2} \right). \]

(23)

It converges to the quantum relative entropy [33]

\[ D(\rho||\sigma) := \text{Tr}[\rho \log_2 \rho - \log_2 \sigma] \]

(24)

in the limit \( \alpha \to 1 \), and it is a generalized divergence for \( \alpha \geq 1/2 \). See [26] for further properties.

**Proposition 10:** Let \( \omega_{AB} \) be a state satisfying

\[ F\left( \Phi_{AB}^d, \omega_{AB} \right) \geq 1 - \varepsilon, \]

(25)

for \( \varepsilon \in [0, 1] \). Then, for all \( \alpha > 1 \),

\[ \log_2 d \leq \tilde{D}_\alpha(\omega_{AB}) + \frac{\alpha}{\alpha-1} \log_2 \left( \frac{1}{1-\varepsilon} \right), \]

(26)

where \( \tilde{D}_\alpha(\omega_{AB}) \) is defined from (11) with the underlying divergence taken to be the sandwiched Rényi relative entropy \( \tilde{D}_\alpha \). See Appendix H. 

**IV. DISTILLABLE RANDOMNESS OF A BIPARTITE STATE**

Let \( \rho_{AB} \) be a bipartite state. A protocol for randomness distillation assisted by 1W-LOCC begins with a quantum channel of the form \( \mathcal{E}_{A \rightarrow LM} \), where the output systems are classical. The system \( L \) is communicated to Bob over a noiseless classical channel. After that, he acts with a quantum channel \( \mathcal{D}_{BL \rightarrow M'} \). The state at the end of the protocol is thus

\[ \omega_{MM'} := (\mathcal{D}_{BL \rightarrow M'} \circ \mathcal{E}_{A \rightarrow LM})(\rho_{AB}). \]

(27)

A \((d, \varepsilon)\) protocol for randomness distillation satisfies

\[ p_{\text{err}}((\mathcal{E}, D); \rho_{AB}) := 1 - F(\omega_{MM'}, \Phi_{MM'}^d) \leq \varepsilon. \]

(28)

The one-shot distillable randomness of \( \rho_{AB} \) is defined as

\[ R^e(\rho_{AB}) := \]
and the strong converse distillable randomness as
\[ R(\rho_{AB}) := \inf_{\epsilon \in [0,1]} \liminf_{n \to \infty} \frac{1}{n} R^c(\rho_{AB}^\otimes n), \]
and the strong converse LOCC-assisted distillable randomness
\[ \tilde{R}(\rho_{AB}) := \sup_{\epsilon \in [0,1]} \limsup_{n \to \infty} \frac{1}{n} R^c(\rho_{AB}^\otimes n). \]

We can generalize these definitions to allow for assistance by arbitrary LOCC (see [34] for a detailed account of LOCC). A protocol for randomness distillation assisted by LOCC begins with Alice performing the channel \( \mathcal{C}^{(i)}_{A \to L_i A_i} \), where the system \( L_1 \) is classical and communicated to Bob. Bob then performs the channel \( \mathcal{D}^{(2)}_{L_i B \to L_i B_i} \), where the system \( L_2 \) is classical and communicated to Alice. This process continues for \( k \) rounds; we denote Alice’s other channels by \( \{\mathcal{C}^{(i)}_{L_i-1 A_i \to L_i A_i}\} \), for \( i \in \{3, 5, \ldots\} \), and Bob’s other channels by \( \{\mathcal{D}^{(2)}_{L_i B \to L_i B_i}\} \), for \( i \in \{4, 6, \ldots\} \). The last two channels in the protocol, without loss of generality, are then \( \mathcal{C}^{(k+1)}_{L_1 A_{k+2} \to L_1 A_{k+1}} \) for Alice and \( \mathcal{D}^{(k+1)}_{L_1 B \to L_1 B_1} \) for Bob. The state at the end of the protocol is thus
\[ \omega_{MM'} := (\mathcal{C}^{(k+1)} \circ \mathcal{C}^{(k)} \circ \cdots \circ \mathcal{C}^{(2)} \circ \mathcal{C}^{(1)}) (\rho_{AB}). \]  (32)

A \((d, \varepsilon)\) protocol for LOCC-assisted randomness distillation satisfies
\[ p_{\text{err}}(\mathcal{P}^{(k)}; \rho_{AB}) := 1 - F(\omega_{MM'}, \overline{F}^{d}_{MM'}) \leq \varepsilon, \]  (33)
where \( \mathcal{P}^{(k)} \) is a shorthand for the whole protocol, i.e., \( \mathcal{P}^{(k)} = \{\mathcal{C}^{(1)}, \mathcal{D}^{(2)}, \ldots, \mathcal{C}^{(k)}, \mathcal{D}^{(k+1)}\} \). The one-shot distillable randomness of \( \rho_{AB} \), assisted by LOCC, is defined as
\[ R^c_\varepsilon(\rho_{AB}) := \sup_{k \in \mathbb{N}} \sup_{\mathcal{P}^{(k)}} \left \{ \log_2 d - \sum_{i=1}^{k} \log_2 d_{L_i} : p_{\text{err}}(\mathcal{P}^{(k)}; \rho_{AB}) \leq \varepsilon \right \}. \]  (34)

The LOCC-assisted distillable randomness of a bipartite state \( \rho_{AB} \) is defined as
\[ R_\varepsilon(\rho_{AB}) := \inf_{\varepsilon \in [0,1]} \liminf_{n \to \infty} \frac{1}{n} R^c_\varepsilon(\rho_{AB}^\otimes n), \]  (35)
and the strong converse LOCC-assisted distillable randomness as
\[ \tilde{R}_\varepsilon(\rho_{AB}) := \sup_{\varepsilon \in [0,1]} \limsup_{n \to \infty} \frac{1}{n} R^c_\varepsilon(\rho_{AB}^\otimes n). \]  (36)

The following inequalities hold by definition:
\[ R^c(\rho_{AB}) \leq R^c_\varepsilon(\rho_{AB}), \quad R(\rho_{AB}) \leq R_\varepsilon(\rho_{AB}), \]  (37)
\[ \tilde{R}(\rho_{AB}) \leq \tilde{R}_\varepsilon(\rho_{AB}), \quad R(\rho_{AB}) \leq \tilde{R}_\varepsilon(\rho_{AB}). \]  (38)

We provide upper bounds for \( R^c_\varepsilon(\rho_{AB}) \) and \( \tilde{R}_\varepsilon(\rho_{AB}) \) in the next section.

V. Upper Bounds on the Distillable Randomness

**Theorem 11:** The following bound holds for all \( \alpha > 1 \):
\[ R^c_\varepsilon(\rho_{AB}) \leq \tilde{\Gamma}_\alpha(\rho_{AB}) + \frac{\alpha}{\alpha - 1} \log_2 \left( \frac{1}{1 - \varepsilon} \right), \]  (40)
where \( \tilde{\Gamma}_\alpha(\rho_{AB}) \) is defined from \([4\) and \([23\].

**Proof.** Let us begin by proving the bound
\[ R^c(\rho_{AB}) \leq \tilde{\Gamma}_\alpha(\rho_{AB}) + \frac{\alpha}{\alpha - 1} \log_2 \left( \frac{1}{1 - \varepsilon} \right), \]  (41)
and then we discuss how to generalize the proof afterward. Consider an arbitrary protocol for randomness distillation assisted by 1W-LOCC. Since the final state \( \omega_{MM'} \) satisfies \((28)\), we apply Proposition \([10\) to conclude that
\[ \log_2 d \leq \tilde{\Gamma}_\alpha(M; M')_{\omega} + \frac{\alpha}{\alpha - 1} \log_2 \left( \frac{1}{1 - \varepsilon} \right). \]  (42)
Next we apply data processing under local channels (Proposition \([2\) to conclude that
\[ \tilde{\Gamma}_\alpha(M; M')_{\omega} \leq \tilde{\Gamma}_\alpha(M; BL)_{\mathcal{E}(\rho)}. \]  (43)
We then apply Propositions \([1\) and \([7\) to find that
\[ \tilde{\Gamma}_\alpha(M; BL)_{\mathcal{E}(\rho)} \leq \log_2 d_{L} + \tilde{\Gamma}_\alpha(LM; B)_{\mathcal{E}(\rho)}. \]  (44)
Next we apply data processing under local channels again (Proposition \([2\) to conclude that
\[ \tilde{\Gamma}_\alpha(LM; B)_{\mathcal{E}(\rho)} \leq \tilde{\Gamma}_\alpha(A; B)_{\rho}. \]  (45)
Putting everything together, we finally conclude that
\[ \log_2 d - \log_2 d_{L} \leq \tilde{\Gamma}_\alpha(A; B)_{\rho} + \frac{\alpha}{\alpha - 1} \log_2 \left( \frac{1}{1 - \varepsilon} \right). \]  (46)
Since this holds for an arbitrary randomness distillation protocol, we conclude the desired bound.

To extend this to \( R^c_\varepsilon(\rho_{AB}) \), we can iterate the same reasoning, going backward through a protocol of the form discussed around \((32)\), using Propositions \([10\) and \([2\) to arrive at the following upper bound for a \( k \)-round protocol:
\[ \log_2 d - \sum_{i=1}^{k} \log_2 d_{L_i} \leq \tilde{\Gamma}_\alpha(A; B)_{\rho} + \frac{\alpha}{\alpha - 1} \log_2 \left( \frac{1}{1 - \varepsilon} \right). \]  (47)
Since this upper bound is independent of the number \( k \) of rounds, we conclude the upper bound in \(40\).
\[
\leq \tilde{\Gamma}_\alpha(A; B)_{\rho} + \frac{\alpha}{n(\alpha - 1)} \log_2 \left( \frac{1}{1 - \epsilon} \right), \tag{49}
\]

where we applied subadditivity of \(\tilde{\Gamma}_\alpha\), which follows from Proposition 8 and the fact that \(\tilde{D}_\alpha\) is additive. Taking the limit as \(n \to \infty\), we find that

\[
\limsup_{n \to \infty} \frac{1}{n} R^\epsilon_\rightarrow(\rho_{AB}^\otimes n) \leq \tilde{\Gamma}_\alpha(A; B)_{\rho}.
\tag{50}
\]

Since this holds for all \(\alpha > 1\), we conclude that

\[
\limsup_{n \to \infty} \frac{1}{n} R^\epsilon_\rightarrow(\rho_{AB}^\otimes n) \leq \inf_{\alpha > 1} \tilde{\Gamma}_\alpha(A; B)_{\rho} = \Gamma(A; B)_{\rho}. \tag{51}
\]

The upper bound holds for all \(\epsilon \in [0, 1)\), and so we conclude the desired inequalities in (48).

VI. SEMI-DEFINITE RESTRICTIONS

The upper bounds in Theorems 11 and 12 are not efficiently computable, because the \(\Gamma\)-measure in (4) involves a bilinear optimization. One could attempt to use the approach from [53] to evaluate \(\gamma\), but this does not remove all obstacles to having an efficient method for computing \(\Gamma\). Here we consider instead a semi-definite restriction of the \(\gamma\)-measure in (2), which leads to alternative upper bounds on \(R^\epsilon_\rightarrow(\rho_{AB})\) and \(R^{\epsilon \rightarrow}(\rho_{AB})\).

Indeed, for a given bipartite operator \(\sigma_{AB}\) and state \(\rho_{AB}\), we define the following semi-definite restriction of \(\gamma(\sigma_{AB})\), taken by fixing \(K_A = \rho_A\) in (2):

\[
\beta(\sigma_{AB}, \rho_A) := \inf_{L_B, \rho_A \in \text{Herm}} \left\{ \frac{\text{Tr}[\rho_A \otimes L_B]}{\rho_A \otimes L_B} : T_B(V_{AB} \pm \sigma_{AB}) \geq 0, \rho_A \otimes L_B \pm V_{AB} \geq 0 \right\}.
\tag{52}
\]

It is then clear that \(\gamma(\sigma_{AB}) \leq \beta(\sigma_{AB}, \rho_A) \) \forall \rho_A, as well as that \(\Gamma(\rho_{AB}) \leq \Upsilon^A(\rho_{AB})\), where

\[
\Upsilon^A(\rho_{AB}) := \inf_{\sigma_{AB} \geq 0; \beta(\sigma_{AB}, \rho_A) \leq 1} D(\rho_{AB} \| \sigma_{AB}). \tag{53}
\]

Note that one could also restrict the optimization of \(L_B\) by fixing \(L_B = \rho_B\) and obtain the following quantities:

\[
\beta(\sigma_{AB}, \rho_B) := \inf_{K_A, \rho_A \in \text{Herm}} \left\{ \frac{\text{Tr}[K_A \otimes \rho_B]}{K_A \otimes \rho_B} : T_B(V_{AB} \pm \sigma_{AB}) \geq 0, K_A \otimes \rho_B \pm V_{AB} \geq 0 \right\},
\]

\[
\Upsilon^B(\rho_{AB}) := \inf_{\beta(\sigma_{AB}, \rho_B) \leq 1} D(\rho_{AB} \| \sigma_{AB}). \tag{54}
\]

So then it follows that

\[
\Gamma(\rho_{AB}) \leq \min\{ \Upsilon^A(\rho_{AB}), \Upsilon^B(\rho_{AB}) \}, \tag{55}
\]

as well as

\[
R^\epsilon_\rightarrow(\rho_{AB}) \leq \min\{ \tilde{\Upsilon}^A_{\alpha}(\rho_{AB}), \tilde{\Upsilon}^B_{\alpha}(\rho_{AB}) \} + \alpha' \log_2 \left( \frac{1}{1 - \epsilon} \right),
\]

\[
\tilde{R}^\epsilon_\rightarrow(\rho_{AB}) \leq \min\{ \Upsilon^A(A; B)_\rho, \Upsilon^B(A; B)_\rho \}, \tag{56}
\]

where \(\alpha' = \frac{\alpha}{n}\), as an immediate consequence of (53) and Theorems 11 and 12. To compute the upper bound in the second line of (56) efficiently, one can make use of the relative entropy optimization method from [56]. We remark here that the quantities in (52)–(54) are related to those defined previously in [14]–[16], and this point is discussed further in Appendix A.

As an example, in Figure 1 we plot the upper bound in (56) for an isotropic state, defined for \(p \in [0, 1]\) as \((1 - p)\Phi^d_{AB} + pI_{AB}/d^2\), where \(\Phi^d_{AB} := \frac{1}{d^2} \sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B\). For comparison, we also plot the Holevo information lower bound from [1]. The code for generating this figure is available with the arXiv posting of our paper. We note the similarity with Figure 6 of [17], which is for the dynamical case. Clearly, there is a gap between the lower and upper bounds, and a pertinent question is to close this gap, just as is the case for Figure 6 of [17].

VII. CONCLUSION

In this paper, we returned to the problem of distillable randomness of a bipartite state, providing a number of upper bounds on this quantity that are applicable in both the non-asymptotic and asymptotic regimes. To do so, we introduced a measure of classical correlations contained in a bipartite state. The main measure that we used to provide an upper bound is not clearly efficiently computable; however, we considered a semi-definite restriction that serves as an upper bound.

Going forward from here, it is open to establish tighter upper bounds on the distillable randomness. In future work, we plan to apply the recent lower bound on entanglement cost from [17, Eq. (13)], along with the identity in [38, Theorem 1] that relates entanglement cost and 1W-LOCC distillable randomness. It is also open to generalize these methods to the multipartite case (here, see [39]–[41]).

Acknowledgements—We acknowledge discussions with Dawei Ding, Sumeet Khatri, Yihui Quek, and Peter Shor. LL was partly supported by the Alexander von Humboldt Foundation. BR was supported by the Japan Society for the Promotion of Science (JSPS) KAKENHI Grant No. 21F21015 and the JSPS Postdoctoral Fellowship for Research in Japan. MMW acknowledges support from NSF Grant No. 1907615.
Here we provide some further notation needed to understand the proofs in the following appendices. We denote the unnormalized maximally entangled operator by

$$\Gamma_{RA} := |\Gamma\rangle_R |\Gamma\rangle_A, \quad |\Gamma\rangle_{RA} := \sum_{i=0}^{d-1} |i\rangle_R |i\rangle_A, \quad (57)$$

where $R \simeq A$ with dimension $d$ and $\{|i\rangle_R\}_{i=0}^{d-1}$ and $\{|i\rangle_A\}_{i=0}^{d-1}$ are orthonormal bases. The notation $\simeq A$ means that the systems $R$ and $A$ are isomorphic. The Choi operator of a quantum channel $\mathcal{N}_{A\rightarrow B}$ is denoted by

$$\Gamma_{RB} := \mathcal{N}_{A\rightarrow B}(\Gamma_{RA}). \quad (58)$$

### APPENDIX B

#### PROOF OF PROPOSITION 2 (DATA PROCESSING UNDER LOCAL CHANNELS)

We prove that $\gamma(\rho_{AB}) \geq \gamma(\rho_{A'B'})$, which is equivalent to the inequality (6) in Proposition 2. Let $K_A$, $L_B$, and $V_{AB}$ be arbitrary Hermitian operators satisfying $T_B(V_{AB} \pm \rho_{AB}) \geq 0$ and $K_A \otimes L_B \geq V_{AB} \geq 0$. Consider that the map $T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B$ is completely positive, which follows because

$$(T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B)(\Gamma_{BB}) = (T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B)(\Gamma_{BB}) \quad (59)$$

and

$$(T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B)(\Gamma_{BB}) \geq 0. \quad (60)$$

$$(T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B)(\Gamma_{BB}) \geq 0. \quad (61)$$

The last inequality follows because $\mathcal{M}_{B\rightarrow B'}$ is completely positive and $T_{BB'}$ is a positive map, which in this case is acting on both systems $BB'$ and thus preserves positivity. We also present an alternative proof that $T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B$ is completely positive if $\mathcal{M}_{B\rightarrow B'}$ is. Consider the following chain of equalities for a Kraus decomposition of $\mathcal{M}_{B\rightarrow B'}$ as

$$(T_B' \circ \mathcal{M}_{B\rightarrow B'} \circ T_B)(\cdot) = \sum_{i} M_i(\cdot) M_i^\dagger; \quad (72)$$

Now consider that

$$(\mathcal{N}_{A\rightarrow A'} \otimes (T_{B'} \circ \mathcal{M}_{B\rightarrow B'} \circ T_B))(T_B(V_{AB} \pm \rho_{AB})) = (\mathcal{N}_{A\rightarrow A'} \otimes (T_{B'} \circ \mathcal{M}_{B\rightarrow B'}))(V_{AB} \pm \rho_{AB}) \quad (68)$$

$$(69)$$

$$(T_B(V_{A'B'} \pm \omega_{A'B'})) \geq 0. \quad (70)$$

$$(71)$$

where

$$(72)$$

So it follows that

$$(73)$$

Since $\mathcal{N}_{A\rightarrow A'}$ and $\mathcal{M}_{B\rightarrow B'}$ are completely positive, it follows that

$$(74)$$

which is equivalent to

$$(75)$$

$$\quad (76)$$

$$\quad (77)$$

Also, since $\mathcal{N}_{A\rightarrow A'}$ and $\mathcal{M}_{B\rightarrow B'}$ are trace preserving, it follows that

$$(78)$$

Putting together (76)–(78), we conclude that

$$(79)$$

This concludes the proof of (8).

To see (9), let $\sigma_{AB}$ be an arbitrary positive semi-definite operator satisfying $\gamma(\sigma_{AB}) \leq 1$. Then it follows from (8) that $\tau_{A'B'} := (N_{A\rightarrow A'} \otimes \mathcal{M}_{B\rightarrow B'})(\sigma_{AB})$ satisfies

$$(80)$$

So then, defining $\omega_{A'B'} := (\mathcal{N}_{A\rightarrow A'} \otimes \mathcal{M}_{B\rightarrow B'})(\rho_{AB})$, we find that

$$(81)$$

$$\gamma(\tau_{A'B'}) \leq \gamma(\sigma_{AB}) \leq 1. \quad (82)$$

$$\quad (83)$$
The first inequality follows from the data-processing inequality for $D$, and the second from (50). The equality follows from the definition in (4). Since the inequality holds for all $\sigma_{AB} \geq 0$ satisfying $\gamma(\sigma_{AB}) \leq 1$, we conclude the desired inequality in (83) after taking the infimum.

APPENDIX C

PROOF OF PROPOSITION 4 (NON-NEGATIVITY AND FAITHFULNESS)

First, it follows that $C_\gamma(A;B)_\rho$ takes its minimal value on a product state, and it is equal to the same value for all product states. This is because one can transition from an arbitrary state to a product state by performing local channels that trace out the input and replace with a state. Indeed, let $R_A^\sigma(\cdot) := \text{Tr}_A[\cdot]\sigma_A$ and $R_B^\tau(\cdot) := \text{Tr}_B[\cdot]\tau_B$ be local replacer channels. Then by applying inequality (3) in Proposition 2 we conclude that

$$C_\gamma(A;B)_\rho \geq C_\gamma(A;B)_\omega.$$  

(84)

By the same procedure, one can transition from an arbitrary product state to another arbitrary product state by means of local channels. So the claim stated above follows. The same argument, but using (9), implies that $\Gamma(\rho_{AB})$ takes its minimal value on product states.

We now prove that this minimal value is zero. By definition, for a product state $\omega_{AB} = \sigma_A \otimes \tau_B$, we have

$$\gamma(A;B)_\omega = \inf_{K_{AB} \in \text{Herm}} \left\{ \frac{\text{Tr}[K_{AB} \otimes L_{AB}]}{\text{Tr}[L_{AB}]} : T_B(V_{AB} \pm \sigma_{AB} \otimes \tau_B) \geq 0, K_{AB} \otimes L_{AB} \geq 0 \right\}.$$  

(85)

Applying some of the constraints, we conclude that

$$T_B(\sigma_A \otimes \tau_B) \leq T_B(V_{AB}).$$  

(86)

$$V_{AB} \leq K_{AB} \otimes L_{AB}.$$  

(87)

Now taking a trace over these constraints, we conclude that

$$1 = \text{Tr}[\sigma_A \otimes \tau_B] = \text{Tr}[T_B(\sigma_A \otimes \tau_B)]$$  

(88)

$$\leq \text{Tr}[T_B(V_{AB})] = \text{Tr}[V_{AB}] \leq \text{Tr}[K_{AB} \otimes L_{AB}].$$  

(89)

So this establishes that $\gamma(A;B)_\omega \geq 1$ for every product state $\omega_{AB}$ (and also $\gamma(A;B)_\rho \geq 1$ for every state $\rho_{AB}$, by combining the observation in the first paragraph with $\gamma(A;B)_\omega \geq 1$ for every product state $\omega_{AB}$).

To see the opposite inequality for a product state $\omega_{AB}$, let us make the choice $V_{AB} = T_B(\sigma_A \otimes \tau_B)$, $K_{AB} = \sigma_A$, and $L_{AB} = \tau_B$. For this choice, all constraints are satisfied, in part because the partial transpose map is a positive map when acting on a product state. So it follows that $\gamma(A;B)_\omega \leq 1$, and combining with what we previously showed, we conclude that $\gamma(A;B)_\omega = 1$ for every product state $\omega_{AB}$.

Now we turn to $\Gamma(\rho_{AB})$. Consider that, for an arbitrary positive semi-definite operator $\sigma_{AB}$, the condition $\gamma(\sigma_{AB}) \leq 1$ implies that $\text{Tr}[\sigma_{AB}] \leq 1$ because the following holds for arbitrary $V_{AB}$, $K_{AB}$, and $L_{AB}$ satisfying the constraints in (2):

$$\text{Tr}[\sigma_{AB}] = \text{Tr}[T_B(\sigma_{AB})] \leq \text{Tr}[T_B(V_{AB})] \leq \text{Tr}[K_{AB} \otimes L_{AB}].$$  

(90)

(91)

Then taking an infimum over all $V_{AB}$, $K_{AB}$, and $L_{AB}$ satisfying (2) and applying the assumption $\gamma(\sigma_{AB}) \leq 1$, we conclude that $\text{Tr}[(\sigma_{AB})] \leq 1$. Now applying a trace channel to $D(\rho_{AB}\|\sigma_{AB})$ and the non-negative property of a generalized divergence (i.e., $D(1\|c) \geq 0$, i.e., $\text{Tr}[\rho_{AB}] \geq 0$), we conclude that $\Gamma(\rho_{AB}) \geq 0$ for every state $\rho_{AB}$.

If the state of interest is a product state (i.e., $\omega_{AB} = \sigma_A \otimes \tau_B$), then it follows that $\gamma(\omega_{AB}) \leq 1$, as argued above, so that we can choose $\sigma_{AB} = \omega_{AB}$. With this choice it follows that

$$\Gamma(\omega_{AB}) \leq D(\omega_{AB}\|\omega_{AB}) = 0,$$

with the latter equality following from the zero-value property of generalized divergences. Combining with the previous inequality, we conclude that $\Gamma(\omega_{AB}) = 0$ for every product state $\omega_{AB}$.

Let us now turn to the proof that $C_\gamma$ is faithful, i.e. that $C_\gamma(\omega_{AB}) = 0$ implies $\omega_{AB} = \rho_A \otimes \tau_B$ is a product state, and that $\Gamma$ is also faithful. Provided that the underlying divergence $D$ is lower semicontinuous in its second argument. First, observe that $C_\gamma = \Gamma$ for the particular choice of divergence

$$D(\rho||\sigma) = \begin{cases} -\log c & \sigma = c\rho, \\ +\infty & \text{otherwise}. \end{cases}$$  

(92)

This observation is related to the inequality in (5). Indeed, when performing the optimization for $\Gamma$, consider that choosing $\sigma_{AB}$ to be any operator other than $c\rho_{AB}$ leads to a value of $+\infty$. This then forces $\sigma_{AB}$ to be equal to $c\rho_{AB}$ for some $c > 0$, and the objective function for $\Gamma(\rho_{AB})$ reduces to

$$\inf_{c > 0, c \frac{\rho_{AB}}{\omega_{AB}} \leq 1} D(\rho_{AB}\|c\rho_{AB}) = \inf_{c > 0, c \frac{\rho_{AB}}{\omega_{AB}} \leq 1} -\log_2 c$$

$$= \inf_{c > 0, c \frac{\rho_{AB}}{\omega_{AB}} \leq 1} -\log_2 c$$

$$= \log_2 \gamma(\rho_{AB}),$$  

(93)

following from the scaling property of $D$ and the scale invariance of $\gamma(\rho_{AB})$ (Proposition 5). Since the divergence in (92) happens to be lower semicontinuous in its second argument, it suffices to prove the claim for $\Gamma$.

Thus, let $\omega_{AB}$ be a state such that $\Gamma(\omega_{AB}) = 0$. Due to (49), for all $\delta > 0$ we can find $\sigma_{AB} \geq 0$ such that $\text{Tr}[\sigma_{AB}] \leq \gamma(\sigma_{AB}) \leq 1$ and

$$\delta > D(\omega_{AB}\|\sigma_{AB}) \geq D(1\|\text{Tr}[\sigma_{AB}]) = -\log_2 \text{Tr}[\sigma_{AB}],$$  

(94)

where we also used the data processing inequality and the scaling property for $D$. Combining these two inequalities yields

$$\gamma(\sigma_{AB}) \leq 1 < 2^\delta \text{Tr}[\sigma_{AB}].$$  

(95)

By definition of $\gamma$, we now find a Hermitian operator $V_{AB}$ and positive semi-definite $K_{AB}$ and $L_{AB}$ such that $T_B(V_{AB} \pm \sigma_{AB}) \geq 0$, $K_{AB} \otimes L_{AB} \geq V_{AB} \geq 0$, and $\text{Tr}[K_{AB} \otimes L_{AB}] \leq 1$. This implies that

$$1 \geq \text{Tr}[K_{AB} \otimes L_{AB}]$$

(96)

$$\geq \text{Tr}[V_{AB}]$$

(97)

$$= \text{Tr}[T_B(V_{AB})]$$

(98)

$$\geq \text{Tr}[T_B(\sigma_{AB})].$$  

(99)
\[
\geq 2^{-\delta}, \quad (100)
\]

and thus in turn that
\[
\|K_A \otimes L_B - \sigma_{AB}\|_1 \\
\leq \|K_A \otimes L_B - V_{AB}\|_1 + \|V_{AB} - \sigma_{AB}\|_1 \\
= \text{Tr}[K_A \otimes L_B - V_{AB}] + \|V_{AB} - \sigma_{AB}\|_1 \\
\leq 1 - 2^{-\delta} + \min\{d_A, d_B\} \|T_B(V_{AB} - \sigma_{AB})\|_1 \\
= 1 - 2^{-\delta} + \min\{d_A, d_B\} \text{Tr}[T_B(V_{AB} - \sigma_{AB})] \\
\leq (1 + \min\{d_A, d_B\})(1 - 2^{-\delta}). \quad (105)
\]

In the above calculation, we used the fact that \(\|X_{AB}\|_1 \leq \min\{d_A, d_B\} \|T_B(X_{AB})\|_1\) for every Hermitian operator \(X_{AB}\) (see [42] proof of Proposition 7), as can be seen immediately by writing a spectral decomposition for \(T_B(X_{AB})\) and leveraging the fact that \(\|T_B(\psi_{AB})\|_1 \leq \min\{d_A, d_B\}\) for all pure states \(\psi_{AB}\) [42] Proposition 8).

Since \(\delta > 0\) is arbitrary, we have shown that we can construct a sequence of subnormalized states \(\sigma_{AB}(n)\) with the property that (a) \(\lim_{n \to \infty} D(\omega_{AB}\|\sigma_{AB}(n)) = 0\) and (b) \(\lim_{n \to \infty} \inf K_A, L_B \|\sigma_{AB}(n) - K_A \otimes L_B\|_1 = 0\). Since the set of subnormalized states is compact, up to extracting a subsequence we can assume that \(\lim_{n \to \infty} \sigma_{AB}(n) = \sigma_{AB};\) due to (b) and to the closedness of the set of tensor product operators, we have that \(\sigma_{AB} = \rho_A \otimes \tau_B\) is itself a product subnormalized state. But then (a) together with the lower semicontinuity of \(D\) imply that
\[
0 = \lim_{n \to \infty} D(\omega_{AB}\|\sigma_{AB}(n)) \\
\geq D(\omega_{AB}\|\sigma_{AB}) \\
= D(\omega_{AB}\|\rho_A \otimes \tau_B). \quad (108)
\]

By faithfulness of \(D\), this is only possible if \(\omega_{AB} = \rho_A \otimes \tau_B\), which concludes the proof.

**Appendix D:**

**Proof of Proposition 5 (Dimension Bound)**

The first inequality in (15) follows from recalling (5). So we prove the second inequality in (15). Let us set \(K_A = \rho_A, L_B = I_B\), and \(V_{AB} = \rho_A \otimes I_B\). For these choices, we have that
\[
\text{Tr}[K_A \otimes L_B] = d_B. \quad (109)
\]

We now need to argue that these choices are feasible, i.e., that they satisfy
\[
T_B(V_{AB} \pm \rho_{AB}) \geq 0, \quad (110)
K_A \otimes L_B \pm V_{AB} \geq 0. \quad (111)
\]

The second set of inequalities is trivially satisfied. For the first, consider that we need to show that
\[
T_B(V_{AB} + \rho_{AB}) = \rho_A \otimes I_B + T_B(\rho_{AB}) \\
= \mathcal{P}^+(B)\rho_{AB} \geq 0, \quad (112)
\]
\[
T_B(V_{AB} - \rho_{AB}) = \rho_A \otimes I_B - T_B(\rho_{AB}) \\
= \mathcal{P}^-(B)\rho_{AB} \geq 0. \quad (113)
\]

where the linear maps \(\mathcal{P}^+(B)\) and \(\mathcal{P}^-(B)\) are defined as
\[
\mathcal{P}^+(B)(\cdot) := \text{Tr}_B[\cdot]I_B + T_B(\cdot), \quad (118)
\mathcal{P}^-(B)(\cdot) := \text{Tr}_B[\cdot]I_B - T_B(\cdot). \quad (119)
\]

The Choi operators of these maps are given by
\[
\mathcal{P}^+_B(T_{RB}) = I_{RB} + F_{RB} = 2\Pi^S_{RB}, \quad (120)
\mathcal{P}^-_B(T_{RB}) = I_{RB} - F_{RB} = 2\Pi^A_{RB}. \quad (121)
\]

The Choi operators of these maps are given by
\[
\mathcal{P}^+_B(T_{RB}) = I_{RB} + F_{RB} = 2\Pi^S_{RB}, \quad (120)
\mathcal{P}^-_B(T_{RB}) = I_{RB} - F_{RB} = 2\Pi^A_{RB}. \quad (121)
\]

where \(F_{RB}\) is the unitary swap operator and \(\Pi^S_{RB}\) and \(\Pi^A_{RB}\) are the projections onto the symmetric and antisymmetric subspaces, respectively. Since these operators are positive semi-definite and they are the Choi operators of \(\mathcal{P}^+_B\) and \(\mathcal{P}^-_B\), it follows that \(\mathcal{P}^+_B\) and \(\mathcal{P}^-_B\) are completely positive maps. Thus, the constraints in (110) hold, and we conclude the upper bound \(C_y(A; B)_\rho \leq \log_2 d_B\).

The proof of the other upper bound is similar, and we show it for completeness. Pick \(K_A = I_A, L_B = \rho_B\), and \(V_{AB} = I_A \otimes \rho_B\). For these choices, we have that
\[
\text{Tr}[K_A \otimes L_B] = d_A. \quad (122)
\]

We need to argue that these choices are feasible. The constraint in (111) holds trivially. The first constraints in (110) become
\[
T_B(V_{AB} + \rho_{AB}) = I_A \otimes T_B(\rho_B) + T_B(\rho_{AB}) \geq 0, \quad (123)
T_B(V_{AB} - \rho_{AB}) = I_A \otimes T_B(\rho_B) - T_B(\rho_{AB}) \geq 0. \quad (124)
\]

The inequalities above are equivalent to the following inequalities because they are related by taking a full transpose:
\[
I_A \otimes \rho_B + T_A(\rho_{AB}) \geq 0, \quad (125)
I_A \otimes \rho_B - T_A(\rho_{AB}) \geq 0. \quad (126)
\]

Then we conclude that the constraints are satisfied because \(\mathcal{P}^+_A(\rho_{AB}) = I_A \otimes \rho_B + T_A(\rho_{AB})\) and \(\mathcal{P}^-_A(\rho_{AB}) = I_A \otimes \rho_B - T_A(\rho_{AB})\), and we already proved that \(\mathcal{P}^+_A\) and \(\mathcal{P}^-_A\) are completely positive.

**Appendix E:**

**Proof of Proposition 7 (Classical Communication Bound)**

Let \(K_A, L_B, X\), and \(V_{ABX}\) be arbitrary communication operators for the optimization problem for \(C_y(A; B|X)_\rho\), which satisfy
\[
T_{BX}(V_{ABX} \pm \rho_{ABX}) \geq 0, \quad (127)
K_A \otimes L_B \pm V_{ABX} \geq 0. \quad (128)
\]

Pick
\[
K'_{AX} := K_A \otimes I_X, \quad (129)
L'_{B} := \text{Tr}_X[L_BX], \quad (130)
V'_{ABX} := \Delta_X(V_{ABX}), \quad (131)
\]

where \(\Delta_X(\cdot) := \sum_x |x\rangle\langle x| \cdot |x\rangle\langle x|\) is the completely dephasing channel. Then we find that
\[
\text{Tr}[K'_{AX} \otimes L'] = \text{Tr}[K_A \otimes I_X \otimes \text{Tr}_X[L_BX]] \quad (132)
\]
\[ \text{We then need to show that} \]

\[ T_B(V'_{ABX} \pm \rho_{ABX}) \geq 0, \]

\[ K'_{AX} \otimes L_B' \geq V'_{ABX} \geq 0. \]

Since \( X \) is a completely positive map, we see that

\[ K_A \otimes L_B \pm V_{ABX} \geq 0 \]

\[ \implies K_A \otimes \Xi_X(L_{BX}) \pm \Xi_X(V_{ABX}) \geq 0 \]

\[ \iff K_A \otimes \Xi_X(L_{BX}) \pm V'_{ABX} \geq 0. \]

We also have that \( \Xi_X(L_{BX}) \leq L_B \otimes I_X \), which follows because

\[ \Xi_X(L_{BX}) = \sum_x L^x_B \otimes |x\rangle\langle x|_X \]

\[ \leq \sum_x L^x_B \otimes I_X \]

\[ = L_B \otimes I_X, \]

where

\[ L^x_B := X \langle x|L_{BX}|x\rangle_X. \]

The inequality \( \Xi_X(L_{BX}) \leq L_B \otimes I_X \) implies that

\[ K_A \otimes L_B \pm I_X \pm V'_{ABX} \geq 0 \]

\[ \iff K'_{AX} \otimes L_B' \pm V'_{ABX} \geq 0. \]

Now consider that

\[ T_B(V_{ABX} \pm \rho_{ABX}) \geq 0 \]

\[ \iff \Xi_X(T_B(V_{ABX} \pm \rho_{ABX})) \geq 0 \]

\[ \iff T_B(\Xi_X(V_{ABX}) \pm \Xi_X(\rho_{ABX})) \geq 0 \]

\[ \iff T_B(V'_{ABX} \pm \rho_{ABX}) \geq 0. \]

In the above, we applied the equality \( \Xi_X \circ T_X = \Xi_X \). Since \( K'_{AX}, L'_B \), and \( V'_{ABX} \) are specific choices that satisfy the constraints for \( C_\gamma(AX;B)_\rho \), we conclude the desired inequality after minimizing over all such operators and noticing that the objective function for \( C_\gamma(AX;B)_\rho \) is \( \text{Tr}[K'_{AX} \otimes L_B'] \), which satisfies \((132)-(134)\). This establishes \((18)\).

To see \((19)\), consider that

\[ \log_2 d_X + \Gamma(A;BX)_\rho \]

\[ = \log_2 d_X + \inf_{\sigma_{ABX} \geq 0, \gamma(AX;B)_\rho \leq 1} D(\rho_{ABX} \| \sigma_{ABX}/d_X) \]

\[ = \inf_{\sigma_{ABX} \geq 0, \gamma(AX;B)_\rho \leq 1} D(\rho_{ABX} \| \sigma')_{ABX} \]

\[ = \inf_{\sigma_{ABX} \geq 0, \gamma(AX;B)_\rho \leq 1} D(\rho_{ABX} \| \sigma'_{ABX}) \]

\[ \geq \inf_{\sigma_{ABX} \geq 0, \gamma(AX;B)_\rho \leq 1} D(\rho_{ABX} \| \sigma'_{ABX}) \]

\[ = \Gamma(AX;B)_\rho. \]

The fourth equality follows from Proposition \((6)\) and the subsequent inequality from \((18)\).

**APPENDIX F**

**PROOF OF PROPOSITION \((8)\) (SUBADDITIVITY)**

Let \( K'_{A_1}, L'_{B_1}, \) and \( V'_{A_1B_1} \) be feasible choices for \( C_\gamma(A_1;B_1)_\sigma \) (satisfying the constraints in \((2)\)), and let \( K'_{A_2}, L'_{B_2}, \) and \( V'_{A_2B_2} \) be feasible choices for \( C_\gamma(A_2;B_2)_\tau \). Then it follows that \( K'_{1A_1} \otimes K'_{2A_2}, L'_{B_1} \otimes L'_{B_2}, \) and \( V'_{1A_1B_1} \otimes V'_{2A_2B_2} \) are feasible choices for \( C_\gamma(A_1A_2;B_1B_2)_\rho \). This latter statement is a consequence of the general fact that if \( A, B, C, \) and \( D \) are Hermitian operators satisfying \( A \pm B \geq 0 \) and \( C \pm D \geq 0 \), then \( A \otimes C \pm B \otimes D \geq 0 \). To see this, consider that the original four operator inequalities imply the four operator inequalities \( (A \pm B) \otimes (C \pm D) \geq 0 \), and then summing these four different operator inequalities in various ways leads to \( A \otimes C \pm B \otimes D \geq 0 \).

To see the inequality in \((21)\), let \( \omega_{A_1B_1} \geq 0 \) satisfy \( \gamma(A_1;B_1)_\omega \leq 1 \) and let \( \theta_{A_2B_2} \geq 0 \) satisfy \( \gamma(A_2;B_2)_\theta \leq 1 \). Then, by applying \((20)\), we have that \( \gamma(A_1A_2;B_1B_2)_\omega \geq 1 \), \( \gamma(A_1A_2;B_1B_2)_\omega \leq 1 \), so that

\[ \Gamma(A_1A_2;B_1B_2)_\rho \]

\[ = \inf_{\gamma \leq 1} D(\rho_{A_1A_2B_1B_2} \| \gamma_{A_1A_2B_1B_2}) \]

\[ = \inf_{\gamma \leq 1} D(\sigma_{A_1B_1} \otimes \tau_{A_2B_2} \| \gamma_{A_1A_2B_1B_2}) \]

\[ \leq D(\sigma_{A_1B_1} \otimes \tau_{A_2B_2} \| \omega_{A_1B_1} \otimes \theta_{A_2B_2}) \]

\[ \leq D(\sigma_{A_1B_1} \| \omega_{A_1B_1} \theta_{A_2B_2}) + D(\tau_{A_2B_2} \| \theta_{A_2B_2}). \]

The last inequality follows from the hypothesis that \( D \) is subadditive. Since the inequality holds for all \( \omega_{A_1B_1} \) and \( \theta_{A_2B_2} \) satisfying the constraints for \( \Gamma(A_1;B_1)_\sigma \) and \( \Gamma(A_2;B_2)_\tau \), respectively, we conclude the desired inequality in \((21)\).

**APPENDIX G**

**PROOF OF LEMMA \((9)\)**

Let \( \sigma_{AB} \) satisfy \( \sigma_{AB} \geq 0 \) and let \( K_A, L_B, \) and \( V_{AB} \) be Hermitian operators satisfying the constraints for \( \gamma(\sigma_{AB}) \). Consider that

\[ F(\Xi_{AB}, \sigma_{AB}) \leq F(\Xi_{AB}, (\Xi_A \otimes \Xi_B)(\sigma_{AB})) \]

where \( \Xi \) is a local dephasing channel, defined as

\[ \Xi(\cdot) := \sum_{m=0}^{d-1} |m\rangle\langle m| \otimes |m\rangle\langle m| \]

We then find that

\[ (\Xi_A \otimes \Xi_B)(\sigma_{AB}) \]

\[ = \sum_{\ell,m=0}^{d-1} |\ell\rangle\langle \ell| \otimes |\ell\rangle\langle \ell| \otimes |m\rangle\langle m| AB \sigma_{AB} |\ell\rangle\langle \ell| |m\rangle\langle m| AB \]

\[ = (163) \]
Then the fidelity $F\left(\Phi_{AB}^d, (\Delta_A \otimes \Delta_B) (\sigma_{AB})\right)$ becomes the classical fidelity, i.e.,

$$F\left(\Phi_{AB}^d, (\Delta_A \otimes \Delta_B) (\sigma_{AB})\right) = \sum_{m=0}^{d-1} \frac{1}{d} \sum_{m} \frac{\text{Tr}[\rho_A \rho_B \sigma_{AB}]}{m|m}_{B}.$$

(164)

Then we use the fact that

$$\text{Tr}[|m\rangle\langle m|_A \otimes |m\rangle\langle m|_B] = \text{Tr}[|m\rangle\langle m|]_A \otimes |m\rangle\langle m|_B] = \text{Tr}[|m\rangle\langle m|_A] \text{Tr}[|m\rangle\langle m|_B] = 1.$$ (165)

We can rewrite this as

$$\tilde{\Gamma}_\alpha(\omega_{AB}) + \frac{\alpha}{\alpha-1} \log_2 \left(\frac{1}{1-\varepsilon}\right) \geq \tilde{\Gamma}_\beta(\phi_{AB}^d) \geq \tilde{\Gamma}_1(\phi_{AB}^d) \geq \log_2 d, \quad (178)$$

(179)

where the second inequality follows from $\beta$-monotonicity of the sandwiched Renyi relative entropy (see [26, Prop. 4.29]), and the third from Lemma 9.

**APPENDIX I**

**RELATION TO $\beta$- AND $\Upsilon$-MEASURES OF [14]–[16]**

In this appendix, we discuss the relation of the $\gamma$, $C_\gamma$, and $\Gamma$ measures introduced in the main text, with the $\beta$, $C_\beta$, and $\Upsilon$ measures from [14]–[16].

Indeed, by fixing the operator $K_A$ in (2) to be the marginal operator $A_B$ (where $\sigma_{AB}$ is a bipartite positive semi-definite operator), we arrive at the following quantity:

$$\beta(\sigma_{AB}) := \inf_{\sigma_A \otimes L_B} \left\{ \text{Tr}[\sigma_A \otimes L_B : T_B(\sigma_{AB}) \geq 0, \sigma_A \otimes L_B \geq 0] \right\}.$$ (181)

This is precisely the static version of the $\beta$ measure from [14], Eq. (45). We also define

$$C_\beta(\sigma_{AB}) := C_\beta(A; B) : = \log_2 \beta(\sigma_{AB}).$$

For a bipartite state $\rho_{AB}$, we then define

$$\Upsilon(\rho_{AB}) := \inf_{\beta(\sigma_{AB}) \leq 1} \inf_{\rho_{AB}} \text{D}(\rho_{AB}, \sigma_{AB}).$$

(183)

which is the static version of the $\Upsilon$ measure from [15], Eq. (49)]. The following inequalities clearly hold, by applying definitions:

$$\gamma(\sigma_{AB}) \leq \beta(\sigma_{AB}), \quad \Gamma(\rho_{AB}) \leq \Upsilon(\rho_{AB}).$$

(184)

Thus, $\beta$, $C_\beta$, and $\Upsilon$ can be understood as static counterparts of the corresponding measures of classical correlations of a channel, from [14]–[16]. We wrote them down explicitly above to make the connection with prior literature. However, in the main text, we focused exclusively on $\gamma$, $C_\gamma$, and $\Gamma$ because these quantities lead to tighter upper bounds on the distillable randomness. The semi-definite restrictions of these quantities in Section VI are closely related as well with $\beta$, $C_\beta$, and $\Upsilon$, and as discussed there, they lead to computationally efficient upper bounds on distillable randomness.

We finally note that the static $\beta$- and $\Upsilon$-measures for a bipartite state and the dynamic ones for point-to-point channels are further generalized by the corresponding measures for a bipartite channel, as proposed in [17]. As such, the $\gamma$, $C_\gamma$, and $\Gamma$ measures can be generalized to bipartite channels, as considered in [44], and will be the subject of a future publication.