Heinrich-Heine-Universität Düsseldorf
Math.-Nat. Fakultät
Institut für Theoretische Physik III

Limits on the Generation and Applications of Multipartite Entanglement

Inaugural-Dissertation

zur Erlangung des Doktorgrades der Mathematisch-Naturwissenschaftlichen Fakultät der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Justus Neumann

aus Braunschweig

Düsseldorf, Juli 2026

aus dem Institut für Theoretische Physik III
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Berichterstatter:

1. Prof. Dr. Dagmar Bruß

2. apl. Prof. Dr. Hermann Kampermann

Tag der mündlichen Prüfung:
26.10.2026

Abstract

Multipartite entanglement is a central resource for quantum information tasks involving several spatially separated parties. In contrast to the bipartite case, multipartite entanglement requires a more detailed classification. One has to determine not only whether a state is entangled, but also whether the entanglement is shared among all parties or only among some of them. Another important question is what resources are needed to create such states.

This thesis investigates limitations on the generation and applications of multipartite entanglement. The central framework is that of quantum networks with local operations and shared randomness. In such networks, independent sources distribute quantum states to spatially separated parties. The parties may coordinate their local operations using shared classical randomness, but they do not communicate during the state generation. This provides a preparation-based perspective on multipartite entanglement.

Within this framework, the multipartite entanglement structure of the final state need not coincide with that of the sources used to prepare it. This difference is particularly relevant for Greenberger–Horne–Zeilinger (GHZ) states, which are fundamental resources for multipartite quantum information tasks. Although bipartite sources are sufficient to generate genuinely multipartite entangled states, they are fundamentally limited in their ability to approximate GHZ states. We derive bounds on the maximal fidelity achievable when only bipartite sources are available. These bounds show that some multipartite target states cannot be approximated with high fidelity unless sources are shared by sufficiently many parties.

The network perspective also raises the question of whether multipartite entanglement generated under such restrictions is useful for operational tasks. We address this question for conference key agreement, the multipartite analogue of quantum key distribution. Since GHZ states are natural resources for this task, one might expect that genuinely multipartite entangled states generated in such networks provide an advantage for conference key agreement. We show that this is not necessarily the case for states generated under these network restrictions.

Beyond network restrictions, this thesis also considers limitations on the generation of entanglement from mixed quantum states. This is studied through the notion of absolute separability, which captures states that are too mixed to be transformed into entangled states. We

introduce a strengthened variant in which states remain separable even under all probabilistic unital transformations that preserve the maximally mixed state up to normalization. We characterize the corresponding set in terms of the eigenvalues of the state.

Finally, we study additivity questions for the relative entropy of magic, a resource measure in the resource theory of magic. Magic captures the resources required for universal quantum computation beyond stabilizer states and Clifford operations. We investigate this measure for tensor products of single qubit states and analyze conditions under which it is additive or non-additive.

Zusammenfassung

Multipartite Verschränkung ist eine zentrale Ressource für Quanteninformationsaufgaben, an denen mehrere räumlich getrennte Parteien beteiligt sind. Im Gegensatz zum bipartiten Fall erfordert multipartite Verschränkung eine differenziertere Klassifikation. Dabei muss nicht nur bestimmt werden, ob ein Zustand verschränkt ist, sondern auch, ob die Verschränkung zwischen allen Parteien geteilt wird oder lediglich zwischen einigen von ihnen besteht. Eine weitere wichtige Frage ist, welche Ressourcen zur Erzeugung solcher Zustände erforderlich sind.

Diese Dissertation untersucht Beschränkungen bei der Erzeugung und Anwendung multipartiter Verschränkung. Den zentralen Rahmen bilden Quantennetzwerke mit lokalen Operationen und gemeinsamer Zufälligkeit. In solchen Netzwerken verteilen unabhängige Quellen Quantenzustände an räumlich getrennte Parteien. Die Parteien können ihre lokalen Operationen mithilfe gemeinsamer klassischer Zufälligkeit koordinieren, kommunizieren jedoch während der Zustandserzeugung nicht miteinander. Dies ermöglicht eine präparationsbasierte Betrachtungsweise multipartiter Verschränkung.

In diesem Rahmen muss die multipartite Verschränkungsstruktur des erzeugten Endzustands nicht mit derjenigen der zu seiner Präparation verwendeten Quellen übereinstimmen. Dieser Unterschied ist insbesondere für Greenberger-Horne-Zeilinger-Zustände (GHZ-Zustände) relevant, die grundlegende Ressourcen für multipartite Quanteninformationsaufgaben darstellen. Obwohl bipartite Quellen ausreichen, um echt multipartit verschränkte Zustände zu erzeugen, sind ihre Möglichkeiten zur Approximation von GHZ-Zuständen grundsätzlich begrenzt. Wir leiten Schranken für die maximal erreichbare Fidelität her, wenn ausschließlich bipartite Quellen zur Verfügung stehen. Diese Schranken zeigen, dass bestimmte multipartite Zielzustände nur dann mit hoher Fidelität approximiert werden können, wenn die verwendeten Quellen von hinreichend vielen Parteien geteilt werden.

Die Netzwerkperspektive wirft zudem die Frage auf, ob die unter solchen Einschränkungen erzeugte multipartite Verschränkung für operationelle Aufgaben von Nutzen ist. Wir untersuchen diese Frage für die Konferenzschlüsselvereinbarung, das multipartite Analogon zur Quantenschlüsselverteilung. Da GHZ-Zustände natürliche Ressourcen für diese Aufgabe darstellen, könnte man erwarten, dass echt multipartit verschränkte Zustände, die in solchen

Netzwerken erzeugt werden, einen Vorteil für die Konferenzschlüsselvereinbarung bieten. Wir zeigen, dass dies für Zustände, die unter diesen Netzwerkbeschränkungen erzeugt werden, nicht notwendigerweise der Fall ist.

Neben Netzwerkbeschränkungen behandelt diese Dissertation auch Einschränkungen bei der Erzeugung von Verschränkung aus gemischten Quantenzuständen. Dies wird anhand des Begriffs der absoluten Separabilität untersucht, der Zustände beschreibt, die zu stark gemischt sind, um in verschränkte Zustände transformiert werden zu können. Wir führen eine verstärkte Variante ein, bei der Zustände selbst unter allen probabilistischen unitalen Transformationen separabel bleiben, die den maximal gemischten Zustand bis auf eine Normierung erhalten. Die entsprechende Zustandsmenge charakterisieren wir anhand der Eigenwerte des Zustands.

Abschließend untersuchen wir Additivitätsfragen für die relative Entropie der Magie, ein Ressourcenmaß in der Ressourcentheorie der Magie. Magie beschreibt die Ressourcen, die über Stabilisatorzustände und Clifford-Operationen hinaus für universelle Quantenberechnungen erforderlich sind. Wir untersuchen dieses Maß für Tensorprodukte von Einzelqubitzuständen und analysieren die Bedingungen, unter denen es additiv beziehungsweise nichtadditiv ist.

Acknowledgments

I would like to thank my supervisor, Dagmar Bruß, for the opportunity to carry out this research and for her guidance throughout my PhD.

I also thank Hermann Kampermann for his support, many helpful discussions, and feedback on my work.

I thank Anton Trushechkin for the productive scientific collaboration and his contributions to the projects included in this thesis, and especially for his passion for science, which made our group seminars truly unforgettable. Sorry again about the cup.

I am grateful to Tulja Varun Kondra for the productive cooperation and his contributions to the projects included in this thesis, for sharing his Indian wisdom, and for showing me that serious science can still be approached with a remarkable amount of chill.

I am grateful to Nikolai Wyderka for the productive cooperation and his contributions to the projects included in this thesis, as well as for his calm aura.

I would also like to thank Raphael Brinster, also known as "little Nikolai," for proofreading parts of this thesis, for the many entertaining conversations, and, most importantly, for taking care of my protein intake. Scientific progress requires a lot of resources, after all.

I thank Ghislaine Coulter-de Wit for proofreading parts of this thesis, for contributing to a pleasant working environment, for their openness, and for always having an unexpected fact or figure ready for almost any situation, as well as for their support and the many useful discussions over the past years.

I thank Pedro Barrios Hita for the productive cooperation and his contributions to the projects included in this thesis, as well as for being an awesome office mate whose humour, energy, and unmistakable Spanish temperament ensured that our office was never a boring place.

I thank Carolin Deckers for her contributions to the projects included in this thesis and for trusting me enough to supervise her master's thesis and accompany her through this important stage of her academic life. Bold Move!

I thank Yien Liang for proofreading parts of this thesis, for the useful discussions, and for teaching me the philosophy of pragmatism.

I thank Julia Kunzelmann, in particular, for being so supportive during my initial adjustment

to PhD life and for helping me navigate the associated bureaucracy, which definetly requires more endurance than the research itself. Her support made that transition considerably easier.

Contents

1 Introduction 1
2 Mathematical Framework 3
2.1 Quantum Systems and States 4
2.2 Qubits 5
2.3 Measurements 5
2.4 Quantum Channels 6
3 Entangled States 8
3.1 Bipartite Entanglement 8
3.2 Multipartite Entanglement 9
4 Quantum Resource Theory 14
4.1 Introduction 15
4.2 Definitions 16
4.3 Resource Measures 16
5 Quantum Networks 21
5.1 Introduction 21
5.2 LOSR Quantum Networks 22
5.3 Inflation Theory 24
5.4 Multipartite Entanglement in LOSR Networks 26
6 Conference Key Agreement 29
6.1 Quantum Entropies 29
6.2 Devetak-Winter Key Rate 30
6.3 Multipartite BB84 Protocol 31
7 Absolute Separability 32
7.1 Definition and Basic Properties 33
7.2 Sufficient Conditions for Absolute Separability 34
7.3 Boundary States 35
8 Magic States 36
8.1 Introduction 36

8.2 Definition . . . 37
8.3 Single Qubit Resource Theory of Magic . . . 38
8.4 Relative Entropy of Magic . . . 38
9 Summary of the Results . . . 40
9.1 Multipartite Entanglement in LOSR Networks . . . 40
9.2 QKD in LOSR Networks . . . 51
9.3 Completely Absolute Separable States . . . 56
9.4 Additivity of the Relative Entropy of Magic . . . 60
10 Outlook . . . 62

Eidesstattliche Versicherung **75**

Paper A **77**

Paper B **105**

Paper C **123**

Paper D **139**

1 Introduction

Multipartite entanglement describes quantum correlations shared among more than two quantum systems. It is therefore relevant for quantum information tasks involving several parties, such as conference key agreement [1, 2], quantum metrology [3], and measurement-based quantum computation [4, 5]. Important examples of multipartite entangled states are GHZ states, W states, and graph states [6–8]. GHZ states are natural resources for multipartite cryptographic tasks such as conference key agreement [1, 9], while graph states, in particular cluster states, are fundamental resources for measurement based quantum computation [4, 5, 10].

In the bipartite case, the basic distinction is between separable and entangled states, whereas multipartite systems exhibit a more involved entanglement structure [11–13]. A multipartite state may be fully separable, meaning that it contains no entanglement among the parties. It may also contain entanglement only among some of the parties, but not among all of them. Such states are not fully separable, but their entanglement is not genuinely shared by all parties. This motivates the notion of genuine multipartite entanglement, which captures entanglement that cannot be reduced to entanglement shared only between groups of parties.

Having distinguished different forms of multipartite entanglement, one can ask which states can be prepared under restricted operations and which of these states are useful for operational tasks. Quantum resource theories provide a framework for formulating such questions [14, 15]. In such a theory, one specifies a set of freely available states and operations, and studies which other states can be generated under these restrictions. For entanglement, the free states are typically separable states, while the allowed operations are often chosen to be local operations and classical communication [16, 17].

For multipartite systems, there is more than one natural choice of free states and free operations. One possible approach is to define the free states in terms of multipartite separability classes, such as fully separable or biseparable states [11–13]. Another approach, which is particularly relevant for this thesis, is to classify states by asking how they can be generated. This preparation-based perspective is natural in quantum networks [18–20]. Instead of assuming that a global multipartite state is directly available, one considers a network of quantum sources that distribute states to different parties. The parties then apply local operations to their received systems. In this setting, the structure of entanglement is not determined only by the final state, but also by the resources used to create it.

This leads to a refined classification of multipartite entanglement. A state may be genuinely multipartite entangled in the usual sense and still be obtainable from smaller resources, such as bipartite sources in a network [18]. Conversely, some states cannot be generated in this way.

Quantum networks therefore distinguish between entanglement that is present in the final state and entanglement that is necessary at the level of the sources. This distinction is captured by the notion of genuine network multipartite entanglement [18].

A central model in this thesis is quantum networks with local operations and shared randomness (LOSR). In this model, the parties are allowed to perform local quantum operations and may coordinate their choices using shared classical randomness, but they do not communicate during the state-generation process [18–20]. This restriction is natural when the parties are spatially separated, since communication during the preparation process can introduce waiting times and may require the storage of quantum systems [21–23]. This leads to the question of which multipartite states can be produced from a given network structure. In particular, one can ask whether bipartite sources are sufficient to generate a desired multipartite state, or whether higher-order sources are necessary [24].

Quantum networks are not only useful as a classification tool but they also provide a natural model for future quantum technologies, where many spatially separated users are connected through quantum channels and sources [25, 26]. In this setting, one can study the distribution and preparation of multipartite entangled states, as well as the usefulness of these states for tasks such as conference key agreement [1]. These applications also motivate the question of whether states generated in such networks provide an operational advantage.

The first main contribution of this thesis is the study of limitations on the generation of GHZ states in LOSR quantum networks. Although networks consisting only of bipartite sources can generate states that are genuinely multipartite entangled [18], this thesis shows that their ability to approximate certain target states is strongly limited. In particular, bounds are derived on the maximal fidelity between LOSR network states and multipartite GHZ states. These bounds show that bipartite sources, even when combined with arbitrary local operations and shared randomness, cannot approximate some genuinely multipartite entangled states with high fidelity.

The second main contribution applies the network perspective to conference key agreement. Conference key agreement is the multipartite analogue of quantum key distribution, in which several parties aim to establish a common secret key [1]. Since GHZ states are natural resource states for such protocols [1,2], it is important to understand whether multipartite states generated in LOSR networks can provide an operational advantage. This thesis shows that, in this setting, the presence of genuine multipartite entanglement in LOSR-network states does not by itself guarantee an advantage for conference key agreement.

The third main contribution turns to a fundamental preparation question. Under what conditions can entanglement be generated from mixed states in the first place? This is studied

through absolute separability, a notion describing states that are too mixed to be made entangled by unitary transformations [27–29]. This thesis considers a stronger notion, in which states remain separable even under a broader class of probabilistic unital transformations. The resulting class of completely absolute separable states is characterized by a simple spectral condition involving the largest and smallest eigenvalues of the state.

The final contribution concerns the resource theory of magic [30, 31]. In this theory, stabilizer states and Clifford operations are treated as free states and free operations, respectively. Although stabilizer states include highly structured multipartite states, such as graph states, stabilizer states together with Clifford operations are not sufficient for universal quantum computation [32, 33]. The additional resource is provided by non-stabilizer states known as magic states. This thesis studies the relative entropy of magic for tensor products of single-qubit states and investigates the conditions under which this quantity is additive or non-additive.

This thesis is organized as follows. Chapter 2 introduces the mathematical framework used throughout the thesis, including quantum states, measurements, and quantum channels. Chapter 3 reviews bipartite and multipartite entanglement, focusing on full separability, biseparability, and genuine multipartite entanglement. Chapter 4 introduces the framework of quantum resource theories and discusses resource measures based on the Bures distance and quantum relative entropy. Chapter 5 presents LOSR quantum networks and the network-based approach to multipartite entanglement. Chapter 6 discusses conference key agreement as an operational application of multipartite quantum correlations. Chapter 7 introduces absolute separability and the strengthened variant of completely absolute separability studied in this thesis. Chapter 8 discusses magic states and the relative entropy of magic. In Chapter 9 we present the main results of the thesis, which build on the framework developed in the preceding chapters. Finally, Chapter 10 provides an outlook.

2 Mathematical Framework

This chapter establishes the mathematical framework used throughout the thesis. We first recall the basic formalism of finite dimensional quantum systems, including density operators, composite systems, measurements, and quantum channels. These notions provide the foundation for the later discussion of entanglement, quantum networks, quantum cryptography, and the resource theory of magic. Unless stated otherwise, the definitions in this chapter are taken from [34].

2.1 Quantum Systems and States

A quantum system A is modeled by a complex Hilbert space $\mathcal{H}_A$, which we call the *state space* of the system. Throughout this thesis we only consider finite dimensional Hilbert spaces. Any complex Hilbert space of finite dimension d is isomorphic to the vector space $\mathbb{C}^d$ equipped with an inner product structure. In the special case of a two-dimensional Hilbert space, we call the Hilbert space a *qubit space*. Similarly, we call a d-dimensional Hilbert space a *qudit space*.

The *(quantum) state* of a quantum system is represented by a density operator acting on its Hilbert space. A *density operator* is a linear map $\rho : \mathcal{H} \to \mathcal{H}$ which is positive semidefinite, denoted by $\rho \geq 0$, meaning that $\langle\psi| \rho |\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$, and of unit trace, i.e., $\mathrm{Tr}[\rho] = 1$. In the following, we denote the set of density operators on a Hilbert space $\mathcal{H}$ by $D(\mathcal{H})$ which is a subset of all linear operators from $\mathcal{H}$ to $\mathcal{H}$, i.e., $D(\mathcal{H}) \subseteq L(\mathcal{H}) := \{X : \mathcal{H} \to \mathcal{H} | X \text{ is linear}\}$.

Note that the set of density operators $D(\mathcal{H})$ is a convex set, i.e., if $\rho, \tau \in D(\mathcal{H})$ then $\lambda\rho + (1-\lambda)\tau \in D(\mathcal{H})$ for all $\lambda \in [0, 1]$. The extremal points[1] of $D(\mathcal{H})$ are called *pure states* and they are of the form $|\psi\rangle\langle\psi|$ with some normalized vector $|\psi\rangle \in \mathcal{H}$, i.e., $\langle\psi|\psi\rangle = 1$. Since pure states are completely described by a normalized vector in the Hilbert space, we sometimes also call normalized elements of a Hilbert space pure states.

As a consequence, for any quantum state $\rho \in D(\mathcal{H})$ there exist an index set I together with a probability distribution $\{p_i\}_{i\in I}$ and a set of pure quantum states $\{|\psi_i\rangle\}_{i\in I}$ such that

$$\rho = \sum_{i\in I} p_i \, |\psi_i\rangle\langle\psi_i| \, . \tag{1}$$

Quantum states that are not pure are called *mixed states.*

The composition of two different quantum systems A and B associated with the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, can be modeled by the tensor product of the Hilbert spaces, i.e., $\mathcal{H}_A \otimes \mathcal{H}_B$. The composite system AB associated with the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is called a *bipartite quantum system.* A bipartite quantum system AB is described by a *bipartite state* $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. Here and in the following, we use subscripts to indicate the quantum systems on whose Hilbert spaces a state acts. Thus, the state ρ_{AB} acts on $\mathcal{H}_A \otimes \mathcal{H}_B$. Straightforwardly, we can model multipartite quantum systems $A_1 A_2 \ldots A_N$ with $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N}$, where $\mathcal{H}_{A_i}$ is the Hilbert space associated with the quantum system A_i for $i = 1, 2, \ldots, N$. A corresponding multipartite state is denoted by $\rho_{A_1 A_2 \ldots A_N} \in D(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N})$.

[1] An extremal point is a point that cannot be written as a nontrivial convex combination of two distinct points, i.e., a point $x \in V$ is extremal if $x = \lambda y + (1-\lambda)z$ with $y, z \in V$ and $0 < \lambda < 1$ implies $x = y = z$.

2.2 Qubits

Let $\mathcal{H}$ be a qubit space and let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis of $\mathcal{H}$, i.e., any $|\psi\rangle \in \mathcal{H}$ can be written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with some suitable $\alpha, \beta \in \mathbb{C}$. Furthermore, $\langle 0|0\rangle = 1 = \langle 1|1\rangle$ and $\langle 1|0\rangle = 0 = \langle 0|1\rangle$. From this we can construct a basis for the set of linear operators $L(\mathcal{H})$, the so called *Pauli basis*, consisting of the identity and the three Pauli operators, i.e.,

$$\mathbb{1} := |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \sigma_1 := |0\rangle\langle 1| + |1\rangle\langle 0|, \quad \sigma_2 := -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad \sigma_3 := |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{2}$$

Sometimes we will also denote the Pauli operators by $X \equiv \sigma_1$, $Y \equiv \sigma_2$ and $Z \equiv \sigma_3$.

Any qubit state ρ can be expanded in the Pauli basis as follows:

$$\rho = \frac{1}{2}\left(\mathbb{1} + \sum_{i=1}^{3} r_i \sigma_i\right), \tag{3}$$

with $r_i \in \mathbb{R}$ for $i = 1, 2, 3$. The vector $\vec{r}_\rho := (r_1, r_2, r_3) \in \mathbb{R}^3$ is called the *Bloch vector* of the state ρ. The condition $\mathrm{Tr}[\rho] = 1$ fixes the prefactor $\frac{1}{2}$, while the positive semidefiniteness is equivalent to $|\vec{r}_\rho| \leq 1$. Thus, the set of qubit states can be identified with the unit ball in $\mathbb{R}^3$. This unit ball is called the *Bloch ball*. Hence, instead of describing a qubit state by its density operator, one can equivalently describe it by a point in the Bloch ball. Pure qubit states correspond to points on the surface of the Bloch ball, i.e., to Bloch vectors satisfying $|\vec{r}_\rho| = 1$, while mixed states correspond to points in its interior, for which $|\vec{r}_\rho| < 1$.

2.3 Measurements

Mathematically, measurements are described by positive operator-valued measures. A *positive operator-valued measure (POVM)* is a set of positive operators that satisfy the completeness relation. Formally this means that a set of linear operators $\{M_i\}_{i\in I}$ with some index set I is called a POVM if $M_i \geq 0$ for all $i \in I$ and $\sum_{i\in I} M_i = \mathbb{1}$.

The index set I can be interpreted as the possible measurement outcomes. Given a state ρ together with a POVM, we can induce a probability distribution $\{p(i)\}_{i\in I}$ by

$$p(i) = \mathrm{Tr}[M_i \rho] \tag{4}$$

for all $i \in I$. The probability $p(i)$ can be interpreted as the probability that the result i occurs.

This is also known as the *Born rule*.

After the measurement with the outcome i the corresponding post-measurement state is given by[2]

$$\rho_i = \frac{\sqrt{M_i}\rho\sqrt{M_i}^\dagger}{\mathrm{Tr}[M_i\rho]}. \tag{5}$$

A measurement is called a *projective measurement* if the POVM only consists of operators that are orthogonal projectors, i.e.,

$$M_i^2 = M_i \quad \text{and} \quad M_i M_j = 0 \quad \text{for all } i \neq j. \tag{6}$$

If, in addition, all operators are of rank-one, the measurement is called a *von Neumann measurement*. As an example, note that any orthonormal basis $\{|e_i\rangle\}_{i=0}^{d-1}$ of a d-dimensional Hilbert space induces a POVM by $\{|e_i\rangle\langle e_i|\}_{i=0}^{d-1}$ which is a von Neumann measurement.

2.4 Quantum Channels

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be finite-dimensional Hilbert spaces and let $\mathcal{E}_{A\to B}$ be a linear map that maps linear operators acting on $\mathcal{H}_A$ to linear operators acting on $\mathcal{H}_B$, i.e.,

$$\mathcal{E}_{A\to B} : L(\mathcal{H}_A) \to L(\mathcal{H}_B). \tag{7}$$

The set of linear maps given by (7) is denoted by $\mathcal{L}(\mathcal{H}_A \to \mathcal{H}_B)$. Such linear maps can describe a physical transformation from a quantum system A to a quantum system B.

In order for such a linear map to describe a valid physical transformation, it has to map quantum states to quantum states. This requirement leads to the notion of a quantum channel. To define quantum channels precisely, we first introduce positivity, complete positivity, and trace preservation.

A linear map $\mathcal{E}_{A\to B}$ is called *positive* if it maps positive semidefinite operators to positive semidefinite operators, i.e.,

$$\text{for all } \; X \geq 0 \quad \Longrightarrow \quad \mathcal{E}_{A\to B}(X) \geq 0. \tag{8}$$

A linear map $\mathcal{E}_{A\to B}$ is called *completely positive* if $\mathrm{id}_R \otimes \mathcal{E}_{A\to B}$ is positive for every finite-dimensional auxiliary system R, where id_R denotes the identity map of $\mathcal{L}(\mathcal{H}_R \to \mathcal{H}_R)$,

[2] Note that the post-measurement state is not uniquely determined by the POVM alone. For example, replacing $\sqrt{M_i}$ by $U_i\sqrt{M_i}$, where U_i is unitary, gives the same outcome probabilities but may lead to a different post-measurement state. More generally, different measurement implementations can realize the same POVM.

i.e.,

$$\text{for all } R \text{ and all } X \geq 0 \quad \Longrightarrow \quad \mathrm{id}_R \otimes \mathcal{E}_{A\to B}(X) \geq 0. \tag{9}$$

A linear map $\mathcal{E}_{A\to B}$ is called *trace preserving* if

$$\mathrm{Tr}[\mathcal{E}_{A\to B}(X)] = \mathrm{Tr}[X] \tag{10}$$

for all $X \in L(\mathcal{H}_A)$.

A *quantum channel* is a linear map that is completely positive and trace preserving. In the following, we also call such maps *CPTP maps*. Thus, a quantum channel maps quantum states to quantum states, i.e.,

$$\mathcal{E}_{A\to B}(\rho_A) \in D(\mathcal{H}_B) \tag{11}$$

for every $\rho_A \in D(\mathcal{H}_A)$. The motivation for CPTP maps is the following: the trace preservation ensures that the normalization of states is preserved. Positivity ensures that the output state is positive semidefinite. Complete positivity is the stronger condition required to ensure that the map remains positive when applied to one subsystem of a larger composite system.

Important examples of quantum channels are unitary channels. Unitary channels describe the evolution of closed quantum systems, i.e., quantum systems that do not interact with an environment. If $U : \mathcal{H}_A \to \mathcal{H}_A$ is a unitary operator, i.e., $U^\dagger U = UU^\dagger = \mathbb{1}_A$, where $U^\dagger$ denotes the adjoint of U, then the corresponding unitary channel is given by

$$\mathcal{U}_{A\to A}(\rho_A) = U\rho_A U^\dagger. \tag{12}$$

Quantum channels can be composed. If $\mathcal{E}_{A\to B} : L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ and $\mathcal{N}_{B\to C} : L(\mathcal{H}_B) \to L(\mathcal{H}_C)$ are quantum channels, then their composition

$$\mathcal{N}_{B\to C} \circ \mathcal{E}_{A\to B} \tag{13}$$

is again a quantum channel from A to C.

For composite systems, one can also consider tensor products of channels. If $\mathcal{E}_{A\to A'}$ and $\mathcal{F}_{B\to B'}$ are quantum channels, then

$$\mathcal{E}_{A\to A'} \otimes \mathcal{F}_{B\to B'} = (\mathcal{E}_{A\to A'} \otimes \mathrm{id}_{B'}) \circ (\mathrm{id}_A \otimes \mathcal{F}_{B\to B'}) \tag{14}$$

is a quantum channel from AB to $A'B'$. Such maps describe local transformations applied

independently to different subsystems.

A particularly important class of multipartite quantum channels is given by local operations and classical communication (LOCC). Consider a multipartite system $A_1A_2 \dots A_N$, where the subsystems are held by spatially separated parties. An LOCC protocol is a protocol in which, in each round, every party may apply a local quantum operation to its own subsystem and broadcast classical information about the outcome. The local operations in later rounds may depend on the previously communicated classical outcomes. Therefore, LOCC contains tensor products of local CPTP maps (see, e.g., Eq. (14)), but it does not allow the parties to apply global entangling operations. In particular, LOCC cannot create entanglement between separated parties from separable states [14, 16, 17].

Another important quantum channel is the partial trace, which describes discarding a subsystem. For a bipartite state $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$, the reduced state on subsystem A is defined by

$$\rho_A = \mathrm{Tr}_B[\rho_{AB}], \tag{15}$$

where Tr_B denotes the partial trace over system B. In the following, we use a shorthand notation for reduced states. If a multipartite state is denoted by $\rho_{A_1A_2\dots A_N}$, then reduced states are denoted by keeping only the subsystem labels on which the reduced state acts. For example, for a state ρ_{ABC}

$$\rho_{AB} = \mathrm{Tr}_C[\rho_{ABC}] \tag{16}$$

and

$$\rho_A = \mathrm{Tr}_{BC}[\rho_{ABC}]. \tag{17}$$

3 Entangled States

Entanglement is one of the central features that distinguishes quantum information theory from its classical counterpart. Unlike classical correlations, entanglement enables information processing tasks that cannot be achieved by using only classical resources. Unless stated otherwise, the definitions and standard results presented in this chapter are based on [34] and [13].

3.1 Bipartite Entanglement

A bipartite state ρ_{AB} is called *separable* if there exists an index set I, a probability distribution $\{p_i\}_{i\in I}$, a set of quantum states on subsystem A, i.e., $\{\tau_A^i\}_{i\in I}$ with $\tau_i \in D(\mathcal{H}_A)$ for all $i \in I$ and

a set of quantum states on subsystem B, i.e., $\{\gamma_B^i\}_{i\in I}$ with $\gamma_i \in D(\mathcal{H}_B)$ for all $i \in I$ such that

$$\rho_{AB} = \sum_{i\in I} p_i \, \tau_A^i \otimes \gamma_B^i. \tag{18}$$

In the following, we denote the set of separable states by SEP. A state ρ_{AB} is called *entangled* if it is not separable. An important example of a pure entangled state is the *(generalized) Bell state*

$$\left|\phi_d^+\right\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle_{AB}\,, \tag{19}$$

where we used the shorthand notation $|ii\rangle_{AB} = |i\rangle_A \otimes |i\rangle_B$. Here $\{|i\rangle_A\}_{i=0}^{d-1}$ and $\{|i\rangle_B\}_{i=0}^{d-1}$ form an orthonormal basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. While the definition of separability is conceptually clear, it is often difficult to verify in practice whether a given bipartite state is separable. For this reason, it is useful to introduce criteria that can detect entanglement. One of the most important tools is the positive partial transpose (PPT) criterion. Given a bipartite quantum system AB, the *partial transpose on subsystem B* is defined by

$$T_B(\rho_{AB}) := \sum_{i,j=0}^{d-1} \left(\mathbb{1}_A \otimes |i\rangle\langle j|_B\right) \rho_{AB} \left(\mathbb{1}_A \otimes |i\rangle\langle j|_B\right), \tag{20}$$

where $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis of $\mathcal{H}_B$. In the following, we will also use different notation for the partial transpose like $T_B(\rho_{AB}) \equiv \rho_{AB}^{T_B} \equiv (\mathbb{1}_A \otimes T_B)(\rho_{AB})$. A bipartite state ρ_{AB} is called a *PPT state (or just PPT)* if the partial transpose is positive semidefinite, i.e., $T_B(\rho_{AB}) \geq 0$. Note that the PPT property of a state is independent of the subsystem to which the transpose is applied. Furthermore, the PPT property is also independent of the basis chosen in Eq. (20) (see e.g. [34]). The crucial observation is that every separable state remains positive semidefinite under partial transposition. Therefore, if a state ρ_{AB} is separable, then ρ_{AB} is PPT. Equivalently, if a state ρ_{AB} is not PPT, it is entangled.

3.2 Multipartite Entanglement

In this section, we introduce the basic notions of multipartite entanglement that will be used throughout the remainder of this thesis. While in the bipartite setting the distinction between separable and entangled states is often sufficient, the multipartite case leads to several different notions of separability and entanglement [13, 16]. In particular, notions such as full separability, biseparability, genuine multipartite entanglement, and m-partite entanglement are needed to distinguish whether entanglement is shared only among a subset of parties or genuinely among

all parties. Unless stated otherwise, the definitions and discussion in this section are based on [13].

A state $\rho_{A_1A_2\ldots A_N} \in D(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_N})$ is called *fully separable* if there exists an index set I, a probability distribution $\{p_i\}_{i\in I}$, and set of states $\{\tau^i_{A_1}\}_{i\in I}$ with $\tau^i_{A_1} \in D(\mathcal{H}_{A_1})$ for all $i \in I$, $\{\tau^i_{A_2}\}_{i\in I}$, with $\tau^i_{A_2} \in D(\mathcal{H}_{A_2})$ for all $i \in I, \ldots,$ $\{\tau^i_{A_N}\}_{i\in I}$ with $\tau^i_{A_N} \in D(\mathcal{H}_{A_N})$ for all $i \in I$ such that

$$\rho_{A_1A_2\ldots A_N} = \sum_{i\in I} p_i\, \tau^i_{A_1} \otimes \tau^i_{A_2} \otimes \cdots \otimes \tau^i_{A_N}. \tag{21}$$

In the following we denote the set of fully separable states by $\mathcal{F}^{FS}$.

A multipartite state that is not fully separable is called *entangled*. In many cases the definition of entanglement in the multipartite scenario is too coarse to capture the structure relevant for applications (see e.g. [18]). For example, consider the scenario of an N-partite quantum state $\rho_{A_1A_2\ldots A_N}$ with large N, where only the first two systems are entangled, meaning that the state is of the form

$$\rho_{A_1A_2\ldots A_N} = \sum_{i\in I} p_i\, \tau^i_{A_1A_2} \otimes \tau^i_{A_3} \otimes \cdots \otimes \tau^i_{A_N}. \tag{22}$$

Even though only the first two systems share entanglement, the whole global state is called entangled according to the definition of entanglement. However, states of the form (22) are often not the relevant resource in tasks that require entanglement shared among many parties.

To distinguish states of the form of Eq. (22) from those in which all parties are entangled, the concept of biseparability was introduced [11, 12]. To make the definition precise, it is convenient to first focus on pure states and define biseparability for pure states and then extend it to a general definition for mixed states via convex combinations of pure biseparable states.

Let $S \subset \{A_1, A_2, \ldots, A_N\}$ be a nontrivial subset, i.e., $S \neq \emptyset, S \neq \{A_1, A_2, \ldots, A_N\}$. We denote the complement set by $\bar{S}$. We call $S|\bar{S}$ a *bipartition* of the set $\{A_1, A_2, \ldots, A_N\}$. A pure state $|\psi\rangle_{A_1A_2\ldots A_N}$ is called *biseparable* if there exists a bipartition $S|\bar{S}$ such that

$$|\psi\rangle_{A_1A_2\ldots A_N} = |\varphi\rangle_S \otimes |\tilde{\varphi}\rangle_{\bar{S}}\,. \tag{23}$$

In other words, biseparability means that we can group the parties into two groups S and $\bar{S}$ such that the state $|\psi\rangle_{A_1A_2\ldots A_N}$ is separable with respect to these two groups.

A density operator $\rho_{A_1A_2\ldots A_N}$ is called *biseparable* if there exists an index set I, a probability distribution $\{p_i\}_{i\in I}$, and a set of pure biseparable states, i.e., $\left\{ \left|\psi^i\right\rangle_{A_1A_2\ldots A_N} \right\}_{i\in I}$ where

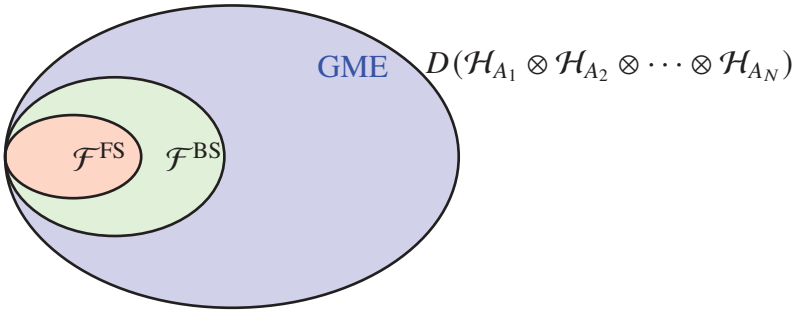


Figure 1: Schematic illustration of different classes of states. The set of fully separable states $\mathcal{F}^{FS}$ (red region) is a subset of the set of biseparable states $\mathcal{F}^{BS}$ (green region). Both sets are convex (see Prop. 1). The set of GME states (blue region) consists of the states that are not biseparable. Note that the set of GME states does not form a convex set.

$|\psi\rangle^i_{A_1A_2\ldots A_N}$ are biseparable states for all $i \in I$ such that

$$\rho_{A_1A_2\ldots A_N} = \sum_{i\in I} p_i \left|\psi^i\right\rangle\!\left\langle\psi^i\right|_{A_1A_2\ldots A_N}. \tag{24}$$

Remark 1. *Note that the states* $\left|\psi^i\right\rangle\!\left\langle\psi^i\right|_{A_1A_2\ldots A_N}$ *in Eq.* (24) *can be biseparable with respect to different bipartitions for different* $i \in I$*. For example, the state*

$$\rho = \frac{1}{3}\left(\left|\phi_d^+\right\rangle\!\left\langle\phi_d^+\right|_{AB} \otimes |0\rangle\!\langle 0|_C + \left|\phi_d^+\right\rangle\!\left\langle\phi_d^+\right|_{AC} \otimes |0\rangle\!\langle 0|_B + \left|\phi_d^+\right\rangle\!\left\langle\phi_d^+\right|_{BC} \otimes |0\rangle\!\langle 0|_A\right), \tag{25}$$

where $\left|\phi_d^+\right\rangle$ *is the Bell state (see Eq.* (19)*), is a biseparable state.*

In the following we denote the set of biseparable states by $\mathcal{F}^{BS}$. A state that is not biseparable is called *genuine multipartite entangled (GME).*

Property 1. *(i) The set of biseparable states is convex.*

(ii) Any fully separable state is biseparable, i.e., $\mathcal{F}^{FS} \subseteq \mathcal{F}^{BS}$ *(see Fig. 1).*

(iii) The set of biseparable states is closed under LOCC, i.e., if ρ *is a biseparable state, it cannot be transformed into a genuinely multipartite entangled state by LOCC operations.*

(iv) The set of biseparable states is not closed under the tensor product, i.e., if ρ *and* τ *are biseparable then* $\rho \otimes \tau$ *is not biseparable in general.*

Property (i) follows directly from the definition (see Eq. (24)). The second property (ii) holds because any fully separable state is separable with respect to every bipartition. Property

(iii) is a consequence of the fact that LOCC cannot create entanglement (see e.g. [35]). The last property (iv) shows that the definition of biseparability allows one to generate genuine multipartite entangled states by simply considering the tensor product of many biseparable states. An example is given in [13]. They show that by taking enough copies of the state (25) one is able to distill the GHZ state (see Eq. (28) in Sec. 3.2.1) , which is a genuine multipartite entangled state. Another example is introduced in [18]: consider the pure biseparable states $|\psi\rangle_{ABC} = \left|\phi_d^+\right\rangle_{AB} \otimes |0\rangle_C$, $|\psi'\rangle_{A'B'C'} = \left|\phi_d^+\right\rangle_{A'C'} \otimes |0\rangle_{B'}$ and $|\psi''\rangle_{A''B''C''} = \left|\phi_d^+\right\rangle_{B''C''} \otimes |0\rangle_{A''}$, where again $\left|\phi_d^+\right\rangle$ is the Bell state given in Eq. (19). The state $|\psi\rangle_{ABC} \otimes |\psi'\rangle_{A'B'C'} \otimes |\psi''\rangle_{A''B''C''}$ is not biseparable anymore with respect to the partition $AA'A''|BB'B''|CC'C''$. An alternative definition, which addresses the issue of closure under the tensor product, is a description of multipartite entanglement via quantum networks, which will be introduced in Sec. 5 (or see [18] for more details).

For systems with more than three parties the classification of multipartite entanglement can be refined further by distinguishing how many parties are involved in the entanglement. Let $|\psi\rangle_{A_1A_2\ldots A_N}$ be an N-partite pure state. The pure state $|\psi\rangle_{A_1A_2\ldots A_N}$ is called *m-partite entangled* if it can be written as

$$|\psi\rangle_{A_1A_2\ldots A_N} = \bigotimes_{i=1}^{K} |\phi_i\rangle\,, \tag{26}$$

where $|\phi_i\rangle$ are at most m partite pure states. Here $K \geq \frac{N}{m}$. A density operator $\rho_{A_1A_2\ldots A_N}$ is called *m-partite entangled* if there exist an index set I, a probability distribution $\{p_i\}_{i\in I}$ and a set of pure m-partite entangled states, i.e., $\left\{\left|\phi^i\right\rangle\right\}_{i\in I}$, where $|\phi_i\rangle$ are m-partite entangled for all $i \in I$ such that

$$\rho_{A_1A_2\ldots A_N} = \sum_{i\in I} p_i \left|\phi^i\right\rangle\!\left\langle\phi^i\right|. \tag{27}$$

In the following we denote the set of m-partite entangled states by $\mathcal{F}_m^{ent}$. In the case of $N = 3$ parties, the set of 2-entangled states coincides with the definition of biseparable states. States that are not m-partite entangled are called *genuine* $(m+1)$*-partite entangled*. Analogously to biseparable states the following properties also hold for m partite entangled states.

Property 2. *(i) The set of m-partite entangled states is convex.*

(ii) Any $(m-1)$*-partite entangled state is an m-partite entangled state, i.e.,* $\mathcal{F}_{m-1}^{ent} \subseteq \mathcal{F}_m^{ent}$.

(iii) The set of m-partite entangled states is not closed under the tensor product.

3.2.1 Important multipartite entangled states

An important example of a multipartite entangled state is the so called *GHZ state* [6], which is the extension of the Bell state (19) to multiple parties

$$\left|\mathrm{GHZ}_{N,d}\right\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N} . \tag{28}$$

The GHZ state is a basic resource in many quantum information tasks like quantum key distribution [1], quantum metrology [3] and error-correction [36].

The qubit GHZ state $\left|\mathrm{GHZ}_{N,2}\right\rangle$ belongs to a broader class of multipartite entangled states, the so called graph states [8, 10]. Graph states were introduced as a structured family of multipartite entangled states that can be described efficiently by simple graphs. Their definition in terms of an underlying graph makes the entanglement structure particularly transparent, since vertices represent quantum systems and edges represent entangling operations between them. In the following we define qubit graph states where the dimension of each subsystem is two.

A *graph* is an ordered pair $\mathcal{G} = (V, E)$ where V is a finite set called the *vertex set* and E is a set called the *edge set* whose elements specify which vertices are adjacent. Formally $E \subseteq \{\{u, v\} | u, v \in V, u \neq v\}$. Let $i \in V$ be a vertex, then the *neighborhood* $N(i) \subset V$ *of the vertex* i is the set of all vertices that are connected to the vertex i by an edge, i.e., $N(i) = \{v \in V |\ \{i, v\} \in E\}$. For the definition of a graph state we associate to each vertex in a given graph $\mathcal{G}$ a quantum system together with a state and to each edge a unitary operation as follows: a *graph state* $|\mathcal{G}\rangle$ corresponding to a graph $\mathcal{G} = (V, E)$ is defined as

$$|\mathcal{G}\rangle := \prod_{\{u,v\}\in E} CZ_{A_u,A_v} \bigotimes_{i\in V} |+\rangle_{A_i} . \tag{29}$$

Here $|+\rangle$ is the eigenstate of the X-Pauli operator with eigenvalue one, i.e., $X|+\rangle = |+\rangle$ (see Eq. (2)). CZ_{A_u,A_v} is a unitary operation acting on the subsystems A_u and A_v. It is called the *controlled-Z gate* and is defined by $CZ_{A_u,A_v} := |0\rangle\langle 0|_{A_u} \otimes \mathbb{1}_{A_v} + |1\rangle\langle 1|_{A_u} \otimes Z_{A_v}$.

Equivalently, one can define graph states in terms of their stabilizer generators [8]. Let $\mathcal{G} = (V, E)$ be a graph. For each vertex $i \in V$ we define the following operator

$$g_i := X_{A_i} \otimes \left(\bigotimes_{j\in N(i)} Z_{A_j} \right) \otimes \left(\bigotimes_{k\in V\setminus(N(i)\cup\{i\})} \mathbb{1}_{A_k} \right), \tag{30}$$

where X_{A_i} and Z_{A_i} are the Pauli operators (2) acting on the system A_i. The graph state $|\mathcal{G}\rangle$

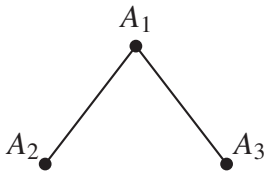


Figure 2: The associated graph state $|\mathcal{G}\rangle$ to the graph is $|\mathcal{G}\rangle = \frac{1}{\sqrt{2}}(|0++\rangle_{A_1A_2A_3} + |1--\rangle_{A_1A_2A_3})$, with generators $g_1 = X \otimes Z \otimes Z$, $g_2 = Z \otimes X \otimes \mathbb{1}$ and $g_3 = Z \otimes \mathbb{1} \otimes X$. This state is equivalent to the state $\left|\mathrm{GHZ}_{3,2}\right\rangle$ (see Eq. (28)) up to local unitaries.

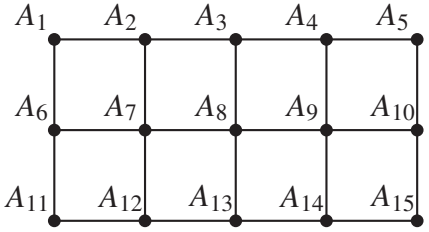


Figure 3: A rectangular 3×5 cluster state $\left|\mathrm{Cl}_{3,5}\right\rangle$. Each vertex represents a qubit initially prepared in $|+\rangle$, and each edge represents a controlled-Z operation between neighboring qubits.

associated to the graph $\mathcal{G}$ is then defined by

$$|\mathcal{G}\rangle\langle\mathcal{G}| := \prod_{l \in V} \frac{\mathbb{1} + g_l}{2}. \tag{31}$$

For a proof that both definitions are equivalent, see, e.g., [10]. As an example, see Fig. 2. Besides their efficient description of multipartite entangled states, graph states have applications in measurement based quantum computation and quantum error correction [10].

In particular, cluster states are an important subclass of graph states since they form the basic resource states for measurement based quantum computation [4, 5]. A *cluster state* is a graph state associated with a lattice graph. For $m, n \in \mathbb{N}$, the rectangular $m \times n$ cluster state is the graph state corresponding to the $m \times n$ rectangular lattice. We denote this state by $\left|\mathrm{Cl}_{m,n}\right\rangle$ (see Fig. 3).

4 Quantum Resource Theory

In this chapter, we introduce the basic framework of quantum resource theories. We first recall the notions of free operations, free states and resource states, and then discuss how resources can be quantified by resource measures. In particular, we introduce two resource measures: one

based on the Bures distance and one based on quantum relative entropy.

The definitions and conventions used in this chapter are taken from [15].

4.1 Introduction

For many physical settings it can be convenient to consider them from the perspective of a resource theory. In this framework, one specifies a subset of the set of states, called the free states, together with a class of operations, called the free operations, which can only map free states to free states. The set of free states and free operations is usually motivated by some physical restrictions of a problem. States that are not free states are called resource states. Important examples are:

1. *The resource theory of entanglement.* Here the free states are the separable states and the physically motivated free operations are LOCC operations [14]. The underlying restriction is that distant parties can only manipulate their systems locally and exchange classical messages, but cannot create entanglement for free. Entangled states are therefore the resource states, which are essential for non-classical tasks such as teleportation [37], entanglement distillation [38, 39], and quantum key distribution [40]. In Sec. 5 and Sec. 9.1 we discuss an extension to the multipartite scenario, namely, the resource theory of genuinely multipartite network entanglement.

2. *The resource theory of purity.* In this theory, the free state is the maximally mixed state, which represents complete randomness. The relevant free operations are noisy operations, i.e., operations generated by unitary transformations, adding maximally mixed ancillas, and discarding subsystems (see [41]). The resource is the degree of purity of a state. The role of purity also appears in the study of absolute separability (see Sec. 7 and 9.3).

3. *The resource theory of magic.* This resource theory is motivated by fault-tolerant quantum computation [42]. In many fault-tolerant architectures, stabilizer states and Clifford operations are comparatively easy to implement, but they do not provide universal quantum computation by themselves. To obtain universality, an additional non-stabilizer resource is needed. Stabilizer states and Clifford operations are therefore treated as free [30]. Moreover, this choice is also motivated by the fact that circuits consisting only of stabilizer states, Clifford operations, and Pauli measurements can be efficiently classically simulated [32, 43]. The magic states are the resource that enables universal quantum computation. In Sec. 8 and Sec. 9.4, we introduce the relative entropy of magic and discuss its additivity.

In this section, we recall the main definitions needed to define a resource theory together with some important distance measures we will use in this thesis.

4.2 Definitions

In this thesis, we use the following operational notion of quantum resource theory. In this formulation, the primitive objects are the free operations, while free states are not specified independently. Instead, the free states are identified with those states that can be prepared for free from the trivial system[3].

Let $\mathcal{F}$ be a mapping that assigns to every pair of physical systems A and B a set of quantum channels $\mathcal{F}(\mathcal{H}_A \to \mathcal{H}_B) \subseteq \mathcal{L}(\mathcal{H}_A \to \mathcal{H}_B)$. The mapping $\mathcal{F}$ is called a *quantum resource theory* if

(i) For any physical system A the identity is contained in $\mathcal{F}(\mathcal{H}_A \to \mathcal{H}_A)$, i.e., $\mathrm{id}_A \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_A)$

(ii) For any three systems A, B, and C, if $\mathcal{E} \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_B)$ and $\mathcal{N} \in \mathcal{F}(\mathcal{H}_B \to \mathcal{H}_C)$ then $\mathcal{N} \circ \mathcal{E} \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_C)$

(iii) For any system A, the trace is contained in the set of free operations, i.e., $\mathrm{Tr}[\cdot] \in \mathcal{F}(\mathcal{H}_A \to \mathbb{C})$.

The first condition (i) simply says that doing nothing is considered as a free operation in a reasonable quantum resource theory. The second condition (ii) ensures closure under composition. The last condition (iii) says that discarding a system is considered as a free operation in a quantum resource theory. The *free states* on system A are defined as the states that can be prepared from the trivial system by free operations. A channel $\rho_{\mathbb{C}\to\mathcal{H}_A} \in \mathcal{F}(\mathbb{C} \to \mathcal{H}_A)$ is therefore equivalent to preparing a free state on system A, i.e., $\rho_A = \rho_{\mathbb{C}\to\mathcal{H}_A}(1)$. In the following we denote the set of free states by $\mathcal{F}(\mathcal{H}_A) := \{\mathcal{E}(1) \,|\, \mathcal{E} \in \mathcal{F}(\mathbb{C} \to \mathcal{H}_A)\}$.

A state ρ is called a *resource state* if it is not a free state, i.e., $\rho \in D(\mathcal{H}_A) \setminus \mathcal{F}(\mathcal{H}_A)$.

4.3 Resource Measures

Given a resource state, one would like to quantify the amount of resource it contains. A *resource measure* M is a map that assigns a real number to quantum states that is monotone and normalized, i.e., $M : \bigcup_{\mathcal{H}_A} D(\mathcal{H}_A) \to \mathbb{R}$,[4] s.t.

[3] The trivial system is the one-dimensional system with Hilbert space $\mathbb{C}$. Its set of density operators is $D(\mathbb{C}) = \{1\}$, where 1 denotes the 1×1 identity matrix.

[4] Note that the union also includes the trivial system $D(\mathbb{C}) = \{1\}$

(i) (Monotone) $M(\mathcal{E}(\rho)) \leq M(\rho)$ for all free operations $\mathcal{E} \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_B)$ and all states $\rho \in D(\mathcal{H}_A)$

(ii) (Normalization) $M(1) = 0$

The first property (i) says that the resource measure cannot increase under free operations. The second property (ii) implies that a resource measure is always nonnegative since $M(\rho) \geq M(\mathrm{Tr}[\rho]) = M(1) = 0$ and that a resource measure vanishes for any free state. This can be seen by considering a free state ρ_A as a channel acting on the trivial system 1, i.e., $\rho_A = \rho_{\mathbb{C}\to A}(1)$. Thus $M(\rho_{\mathbb{C}\to A}(1)) \leq M(1) = 0$. In particular, we call a measure M *faithful* if $M(\rho) = 0 \Leftrightarrow \rho \in \mathcal{F}(\mathcal{H}_A)$.

In the following we introduce two important resource measures. The Bures based resource measure and the relative entropy of resource:

A common quantity to distinguish two different states is the fidelity. The *fidelity* F is a map $F : D(\mathcal{H}_A) \times D(\mathcal{H}_A) \to [0, 1]$ defined by

$$F(\rho, \sigma) := \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^2. \tag{32}$$

Important properties of the fidelity are (see e.g. [34]):

Property 3 (Normalization)**.** *Let $\rho, \sigma \in D(\mathcal{H}_A)$. Then*

$$F(\rho, \sigma) = 1 \quad \Longleftrightarrow \quad \rho = \sigma. \tag{33}$$

If the supports of ρ and σ are orthogonal, then

$$F(\rho, \sigma) = 0. \tag{34}$$

Thus, the fidelity quantifies how close two quantum states are. Identical states have fidelity one, while perfectly distinguishable states have fidelity zero.

Property 4 (Pure states)**.** *Let $\rho \in D(\mathcal{H}_A)$ and let $|\psi\rangle \in \mathcal{H}_A$ be a pure state. Then*

$$F(\rho, |\psi\rangle\langle\psi|) = \langle\psi|\rho|\psi\rangle. \tag{35}$$

Property 5 (Monotonicity under quantum channels)**.** *Let $\mathcal{N} \in \mathcal{L}(\mathcal{H}_{\mathcal{A}} \to H_B)$ be a quantum channel. Then*

$$F(\rho, \sigma) \leq F(\mathcal{N}(\rho), \mathcal{N}(\sigma)) \tag{36}$$

for all $\rho, \sigma \in D(\mathcal{H}_A)$.

This property says that a physical process can make two states less distinguishable, but it cannot make them more distinguishable.

Property 6 (Measurement characterization of the fidelity)**.** *Let* $\rho, \sigma \in D(\mathcal{H}_A)$. *Then*

$$F(\rho, \sigma) = \min_{\{\Lambda_i\}_{i\in I}} \left(\sum_{i\in I} \sqrt{\mathrm{Tr}[\Lambda_i \rho]} \sqrt{\mathrm{Tr}[\Lambda_i \sigma]} \right)^2, \tag{37}$$

where the optimization is taken over all POVMs $\{\Lambda_i\}_{i\in I}$ *on* $\mathcal{H}_A$.

This characterization relates the quantum fidelity to the classical fidelity obtained after a measurement.

The fidelity itself is not a metric on the set of quantum states, since it does not satisfy the triangle inequality, but one can define the *Bures distance* in terms of the fidelity by

$$D_B(\rho, \sigma) := \sqrt{2\left(1 - \sqrt{F(\rho, \sigma)}\right)} \tag{38}$$

(see [44]). Using the Bures distance we can define the *Bures based resource measure* by

$$R_B(\rho) := \inf_{\sigma\in\mathcal{F}(\mathcal{H}_A)} D_B(\rho, \sigma). \tag{39}$$

The Bures based resource measure has a direct geometric interpretation. It quantifies how far a state is from the set of free states with respect to a genuine metric induced by the fidelity [45–47]. Moreover, it is useful when studying approximation problems, for example, how well a resource state can be approximated by free states.

To see that the Bures based resource measure is a proper resource measure, let $\mathcal{E} \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_B)$ be a free operation and let $\rho \in D(\mathcal{H}_A)$. Since $\mathcal{E}$ is free, $\mathcal{E}(\sigma) \in \mathcal{F}(\mathcal{H}_B)$ for all $\sigma \in \mathcal{F}(\mathcal{H}_A)$. Using the definition of the Bures based resource measure (39), we obtain

$$\begin{aligned} R_B(\mathcal{E}(\rho)) &= \inf_{\omega\in\mathcal{F}(\mathcal{H}_B)} D_B(\mathcal{E}(\rho), \omega) \\ &\leq D_B(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \end{aligned} \tag{40}$$

for all $\sigma \in \mathcal{F}(\mathcal{H}_A)$. Since the fidelity is monotone under quantum channels (see Prop. 5) and the Bures distance is monotonically decreasing on $[0, 1]$, it follows that

$$R_B(\mathcal{E}(\rho)) \leq R_B(\rho). \tag{41}$$

Thus, R_B is monotone under free operations. Moreover, the state 1 on the trivial system is free, and hence

$$R_B(1) = \inf_{\sigma \in \mathcal{F}(\mathbb{C})} D_B(1, \sigma) = D_B(1, 1) = 0.$$

Thus, R_B is normalized and therefore defines a resource measure. Additionally, Prop. 3 implies that the Bures based resource measure is a faithful measure.

Another important resource measure is defined via the quantum relative entropy [48].

The *quantum relative entropy* of two states ρ and σ is defined by

$$D(\rho \,\|\, \sigma) := \begin{cases} \mathrm{Tr}\big[\rho(\log \rho - \log \sigma)\big], & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma), \\ +\infty, & \text{otherwise.} \end{cases} \tag{42}$$

The quantum relative entropy satisfies several important properties that make it useful in resource theories (see e.g. [34]).

Property 7 (Non-negativity)**.** *Let $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$. Then*

$$D(\rho \| \sigma) \geq 0.$$

Moreover,

$$D(\rho \| \sigma) = 0 \quad \Longleftrightarrow \quad \rho = \sigma.$$

This property shows that the quantum relative entropy can be interpreted as a distinguishability measure between quantum states. It is always non-negative and vanishes exactly when the two states are identical. However, the relative entropy is not a metric, since it is in general not symmetric and does not satisfy the triangle inequality.

Property 8 (Data-processing inequality)**.** *Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel. Then*

$$D(\mathcal{N}(\rho) \| \mathcal{N}(\sigma)) \leq D(\rho \| \sigma)$$

for all $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$.

Similarly to Prop. 5, the data-processing inequality states that applying the same physical process to both states cannot increase their relative entropy.

Property 9 (Additivity)**.** *Let $\rho_1, \sigma_1 \in \mathcal{D}(\mathcal{H}_A)$ and $\rho_2, \sigma_2 \in \mathcal{D}(\mathcal{H}_B)$. Then*

$$D(\rho_1 \otimes \rho_2 \| \sigma_1 \otimes \sigma_2) = D(\rho_1 \| \sigma_1) + D(\rho_2 \| \sigma_2),$$

whenever the relative entropies are finite.

This property states that the relative entropy of product states decomposes into the sum of the relative entropies of the individual factors.

The *relative entropy of resource* is defined by

$$R_{\mathrm{rel}}(\rho) := \inf_{\sigma \in \mathcal{F}(\mathcal{H}_A)} D(\rho \,\|\, \sigma). \tag{43}$$

This quantity measures the distinguishability of a state from the set of free states. It was first introduced in entanglement theory as the relative entropy of entanglement [45, 46] and later became a central quantity in the general framework of quantum resource theories [14, 49].

To see that the relative entropy of resource is a resource measure, again let $\mathcal{E} \in \mathcal{F}(\mathcal{H}_A \to \mathcal{H}_B)$ be a free operation and let $\rho \in \mathcal{D}(\mathcal{H}_A)$. Since for every free state $\sigma \in \mathcal{F}(\mathcal{H}_A)$, the state $\mathcal{E}(\sigma)$ is free, i.e., $\mathcal{E}(\sigma) \in \mathcal{F}(\mathcal{H}_B)$, we have

$$\begin{aligned} R_{\mathrm{rel}}(\mathcal{E}(\rho)) &= \inf_{\omega \in \mathcal{F}(\mathcal{H}_B)} D(\mathcal{E}(\rho) \| \omega) \\ &\leq D(\mathcal{E}(\rho) \| \mathcal{E}(\sigma)). \end{aligned} \tag{44}$$

By the data-processing inequality for the quantum relative entropy (see Prop. 8), it follows that

$$R_{\mathrm{rel}}(\mathcal{E}(\rho)) \leq D(\rho \| \sigma) \tag{45}$$

for all $\sigma \in \mathcal{F}(\mathcal{H}_A)$. Taking the infimum over all $\sigma \in \mathcal{F}(\mathcal{H}_A)$ yields

$$R_{\mathrm{rel}}(\mathcal{E}(\rho)) \leq R_{\mathrm{rel}}(\rho). \tag{46}$$

Thus, R_{rel} is monotone under free operations.

Finally, since the state 1 on the trivial system is free, we have

$$R_{\mathrm{rel}}(1) = \inf_{\sigma \in \mathcal{F}(\mathbb{C})} D(1 \| \sigma) = D(1 \| 1) = 0.$$

Thus, R_{rel} is normalized and hence also defines a resource measure. If the infimum is attained, we refer to any minimizing free state as a closest free state to ρ in the relative-entropy sense and denote one such minimizer by $\sigma_\rho \in \operatorname{argmin}_{\sigma \in \mathcal{F}(\mathcal{H}_A)} D(\rho \| \sigma)$.

5 Quantum Networks

This chapter introduces quantum networks as a resource theoretic approach to multipartite entanglement. While in Sec. 3.2 we focused on classifying multipartite states according to different notions of separability and entanglement, we now take a preparation based perspective. We first motivate why standard notions such as biseparability are not sufficient for such a preparation based viewpoint. We then define LOSR quantum networks, where parties are connected by bipartite source states and may use local operations coordinated by shared randomness. Afterwards, we discuss inflation theory as a method for deriving necessary conditions for network states. Finally, we explain how multipartite entanglement can be studied within the LOSR network setting and how this leads to the notion of genuinely multipartite network entanglement.

5.1 Introduction

In the theory of multipartite entanglement, several resource theoretic frameworks have been proposed [50, 51]. Their common goal is to distinguish resourceful multipartite states from those that should be regarded as free, and to specify which state transformations are allowed at no cost. In the resource theory of genuine multipartite entanglement, the free states are usually taken to be the biseparable states, while the free operations are required to preserve this set, i.e., they cannot generate genuine multipartite entanglement from biseparable states [51, 52]. This framework can be viewed as a natural extension of the bipartite resource theory of entanglement to the multipartite setting. These approaches are useful for classifying multipartite entangled states and for studying which state transformations are possible under restricted classes of operations.

In this thesis, however, we aim to establish a resource theory of multipartite entanglement in which the free states are those that are technically feasible to prepare. As a first attempt, one might consider 2-partite entangled states, introduced in Sec. 3.2, as the set of free states, since their preparation requires only bipartite entangled resources, which are experimentally well developed [53, 54]. The resource states are then the genuine 3-partite entangled states. However, as pointed out in Sec. 3.2, the definition of 2-partite entanglement is not closed under the tensor product. This means that merely combining two free preparations could produce a resource state.

This motivates the search for a larger class of states that still captures the idea of being easy to prepare in practice. Therefore, in [18] the concept of genuinely multipartite network entanglement via LOSR-quantum networks is introduced.

In this framework, the free states are those that can be prepared from bipartite source states together with local operations and shared randomness (LOSR). That is, the parties are allowed to perform local operations on their quantum systems. Additionally, the parties have access to shared randomness which tells each party which local operation they need to perform. The free operations are therefore the LOSR operations instead of LOCC operations because classical communication introduces time delays and requires quantum memories in order to preserve the quantum systems until the communicated outcomes are received [25, 54, 55]. In contrast, LOSR prohibits communication during the protocol and therefore does not rely on quantum memories.

5.2 LOSR Quantum Networks

A quantum network can be represented by a graph $\mathcal{G} = (V, E)$. For each vertex $i \in V$ we associate a quantum system A_i. For each edge $e = \{i, j\}$ connecting two vertices i and j we associate the Hilbert spaces $\mathcal{H}_{A_{ij}}$ and $\mathcal{H}_{A_{ji}}$ together with a bipartite state $\rho_e = \rho_{A_{ij}A_{ji}} \in D(\mathcal{H}_{A_{ij}} \otimes \mathcal{H}_{A_{ji}})$, which we refer to as a *source state*. We define the Hilbert space that we associate to the quantum system A_i by

$$\mathcal{H}_{A_i} = \bigotimes_{j \in N(i)} \mathcal{H}_{A_{ij}}. \tag{47}$$

The *global source state* is given by

$$\rho_{\text{source}} = \bigotimes_{e \in E} \rho_e. \tag{48}$$

The global source state ρ_{source} is a tensor product of bipartite source states and we also denote it as a *pair entangled network state* or PEN states for short [56]. In the LOSR scenario, the parties have access to a PEN state. Each party can perform local operations (LO) on their quantum systems, i.e., they apply CPTP maps $\mathcal{E}_{A_i \to A_i'} : D(\mathcal{H}_{A_i}) \to D(\mathcal{H}_{A_i'})$ for all $i \in V$. Finally, we also want to consider mixtures of states generated from PEN states by local operations as free states. This can be realized by allowing the parties to have access to a classical random variable, which is shared by all parties, the shared randomness (SR). Overall, we call a state ρ to be an *LOSR (quantum) state* if there exist an index set I, a probability distribution $\{p_\lambda\}_{\lambda \in I}$, a global source state ρ_{source} and sets of local CPTP maps $\{\mathcal{E}^\lambda_{A_i \to A_i'}\}_{\lambda \in I}$ for all $i \in V$ such that

$$\rho_{A_1' A_2' \ldots A_{|V|}'} = \sum_{\lambda \in I} p_\lambda \left(\bigotimes_{i \in V} \mathcal{E}^\lambda_{A_i \to A_i'} \right) (\rho_{\text{source}}), \tag{49}$$

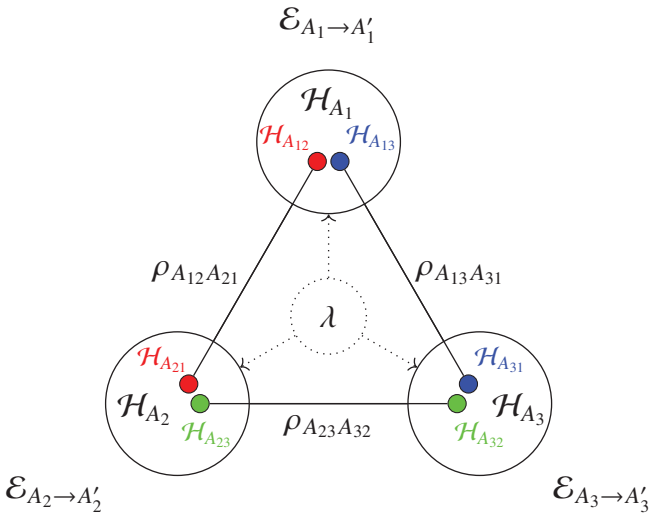


Figure 4: LOSR triangle network. Each pair of parties shares a bipartite source state, denoted by $\rho_{A_{12}A_{21}}$, $\rho_{A_{13}A_{31}}$, and $\rho_{A_{23}A_{32}}$. The parties use the shared classical randomness λ to choose local CPTP maps $\mathcal{E}_{A_1\to A_1'}$, $\mathcal{E}_{A_2\to A_2'}$, and $\mathcal{E}_{A_3\to A_3'}$, which transform their incoming source systems into the output systems A_1', A_2', and A_3'.

(see Fig. 4). States that cannot be brought into the form of Eq. (49) are called *genuinely multipartite network entangled states*. In the following, we denote the set of LOSR states by $\mathcal{F}^{LOSR}$.

Property 10. *(i) For a fixed dimension, $\mathcal{F}^{LOSR}$ is convex.*

(ii) Any 2-partite entangled state is an LOSR state, i.e., $\mathcal{F}_2^{ent} \subseteq \mathcal{F}^{LOSR}$.

(iii) $\mathcal{F}^{\mathrm{LOSR}}$ is closed under LOSR operations but not under LOCC operations.

(iv) $\mathcal{F}^{\mathrm{LOSR}}$ is closed under the tensor product, i.e., if $\rho, \tau \in \mathcal{F}^{\mathrm{LOSR}}$ then $\rho \otimes \tau \in \mathcal{F}^{\mathrm{LOSR}}$.

For the first property (i), note that in the definition of LOSR states (49), the source state ρ_{source} may also depend on the shared randomness λ because the dimension of the source system is not bounded (see [18, 20]). The second property (ii) follows from the fact that any pure 2-entangled state can be considered as a pure global source state, which can be prepared in the network. As discussed before, because of the shared randomness one can also prepare convex combinations of pure 2-entangled states. That $\mathcal{F}^{LOSR}$ is closed under LOSR operations follows directly from the definition. However, LOCC operations can generate genuine network entangled states. For example, in Sec. 9.1.4 it is shown how one can generate a GHZ state via a teleportation protocol. Property (iv) can be shown as follows. Let $\rho, \tau \in \mathcal{F}_{\mathrm{LOSR}}$. For notational simplicity, we assume that the two states are defined with respect to the same network topology

and that the corresponding local systems have the same dimensions. By definition, there exist probability distributions $\{p_\lambda\}_\lambda$ and $\{q_\mu\}_\mu$, bipartite source states $\{\sigma_e^\lambda\}_{e\in E}$ and $\{\omega_e^\mu\}_{e\in E}$, and local CPTP maps $\mathcal{E}^\lambda_{A_i\to A_i'}$ and $\mathcal{F}^\mu_{A_i\to A_i'}$, such that

$$\rho = \sum_\lambda p_\lambda \left(\bigotimes_{i\in V} \mathcal{E}^\lambda_{A_i\to A_i'}\right)\left(\bigotimes_{e\in E} \sigma_e^\lambda\right) \tag{50}$$

and

$$\tau = \sum_\mu q_\mu \left(\bigotimes_{i\in V} \mathcal{F}^\mu_{\tilde{A}_i\to \tilde{A}_i'}\right)\left(\bigotimes_{e\in E} \omega_e^\mu\right). \tag{51}$$

It follows that

$$\begin{aligned}\rho\otimes\tau &= \left[\sum_\lambda p_\lambda \left(\bigotimes_{i\in V} \mathcal{E}^\lambda_{A_i\to A_i'}\right)\left(\bigotimes_{e\in E} \sigma_e^\lambda\right)\right]\otimes\left[\sum_\mu q_\mu \left(\bigotimes_{i\in V} \mathcal{F}^\mu_{\tilde{A}_i\to \tilde{A}_i'}\right)\left(\bigotimes_{e\in E} \omega_e^\mu\right)\right] \\ &= \sum_{\lambda,\mu} p_\lambda q_\mu \left(\bigotimes_{i\in V} \mathcal{E}^\lambda_{A_i\to A_i'}\otimes\mathcal{F}^\mu_{\tilde{A}_i\to \tilde{A}_i'}\right)\left(\bigotimes_{e\in E} \sigma_e^\lambda\otimes\omega_e^\mu\right).\end{aligned} \tag{52}$$

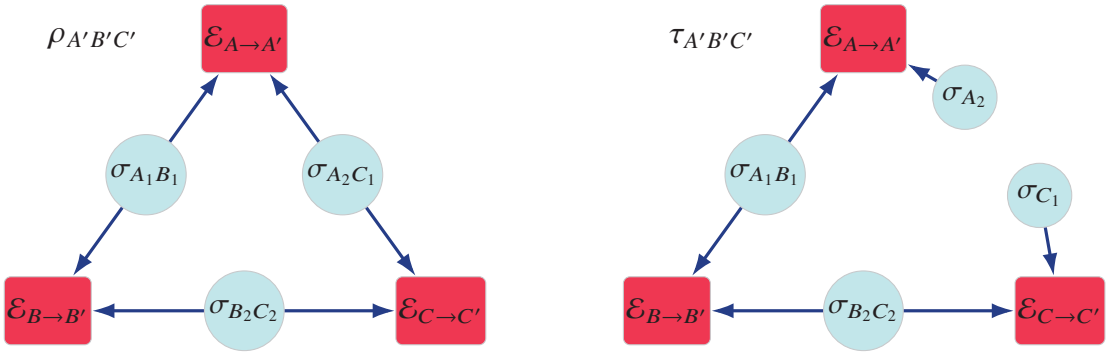
For every edge $e = \{i, j\}$, the state $\sigma_e^\lambda \otimes \omega_e^\mu$ is again a valid bipartite source state. Moreover, $\mathcal{E}^\lambda_{A_i\to A_i'}\otimes\mathcal{F}^\mu_{\tilde{A}_i\to \tilde{A}_i'}$ is again a local CPTP map for party i. Thus, $\rho\otimes\tau$ has again the form of an LOSR state.

5.3 Inflation Theory

To characterize the set of LOSR states $\mathcal{F}^{\mathrm{LOSR}}$, we need techniques that can show whether a state can be prepared in an LOSR network scenario. The inflation technique, introduced in [57, 58], is a tool for deriving necessary conditions on quantum networks. In the following, we show how the inflation technique can be applied to LOSR networks. Here, we only consider the LOSR networks with three participants which we also call the LOSR triangle network. For that we will first focus on networks without the shared randomness because the inflation technique is only applicable to networks where no source is shared by all participants.

To make this more precise, we denote the set of LOSR states where no shared randomness is required for preparation in the network by $\mathcal{F}^{\mathrm{LO}} \subseteq \mathcal{F}^{\mathrm{LOSR}}$. Consider the following two quantum networks given in Fig. 5. Fig. 5a represents states of the form

$$\rho_{A'B'C'} = \mathcal{E}_{A\to A'}\otimes\mathcal{E}_{B\to B'}\otimes\mathcal{E}_{C\to C'}[\sigma_{A_1B_1}\otimes\sigma_{B_2C_2}\otimes\sigma_{A_2C_1}] \tag{53}$$



(a) (b)

Figure 5: Original and inflated triangle networks. (a) In the original triangle network, each pair of parties shares a bipartite source state, and local channels generate the state $\rho_{A'B'C'}$. (b) In the inflated network, the source $\sigma_{A_2C_1}$ is replaced by its marginals σ_{A_2} and σ_{C_1}, yielding the state $\tau_{A'B'C'}$.

while Fig. 5b represents states of the form

$$\tau_{A'B'C'} = \mathcal{E}_{A\to A'} \otimes \mathcal{E}_{B\to B'} \otimes \mathcal{E}_{C\to C'}[\sigma_{A_1B_1} \otimes \sigma_{B_2C_2} \otimes \sigma_{A_2} \otimes \sigma_{C_1}]. \tag{54}$$

Here $\mathcal{E}_A : D(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}) \to D(\mathcal{H}_{A'})$, $\mathcal{E}_B : D(\mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}) \to D(\mathcal{H}_{B'})$, $\mathcal{E}_C : D(\mathcal{H}_{C_1} \otimes \mathcal{H}_{C_2}) \to D(\mathcal{H}_{C'})$ are CPTP maps acting locally on the subsystems of the parties and map the source state into the target state $\rho_{A'B'C'}$ and $\tau_{A'B'C'}$, respectively. σ_{A_2} and σ_{C_1} are the reduced density operators of the state $\sigma_{A_2C_1}$, i.e., $\sigma_{A_2} = \mathrm{Tr}_{C_1}[\sigma_{A_2C_1}]$ and $\sigma_{C_1} = \mathrm{Tr}_{A_2}[\sigma_{A_2C_1}]$.

The crucial fact is that the inflated state (54) reduces to a product state after tracing out subsystem B':

$$\begin{aligned}\mathrm{Tr}_{B'}[\tau_{A'B'C'}] &= \mathcal{E}_{A\to A'} \otimes (\mathrm{Tr}_{B'} \circ \mathcal{E}_{B\to B'}) \otimes \mathcal{E}_{C\to C'}[\sigma_{A_1B_1} \otimes \sigma_{B_2C_2} \otimes \sigma_{A_2} \otimes \sigma_{C_1}] \\ &= \mathcal{E}_{A\to A'} \otimes \mathcal{E}_{C\to C'}[\mathrm{Tr}_{B_1B_2}[\sigma_{A_1B_1} \otimes \sigma_{B_2C_2}] \otimes \sigma_{A_2} \otimes \sigma_{C_1}] \\ &= \mathcal{E}_{A\to A'}(\sigma_{A_1} \otimes \sigma_{A_2}) \otimes \mathcal{E}_{C\to C'}(\sigma_{C_1} \otimes \sigma_{C_2}) = \tau_{A'} \otimes \tau_{C'},\end{aligned} \tag{55}$$

where in the second step we used that $\mathcal{E}_B$ is a trace preserving map.

In order to derive necessary conditions for LOSR states, we consider inequalities for an arbitrary state $\omega_{A'B'C'}$ that depend only on its one- and two-body reduced states which hold for all tripartite states (not just LOSR states), i.e., inequalities of the form

$$f(\omega_{A'}, \omega_{B'}, \omega_{C'}, \omega_{A'B'}, \omega_{A'C'}, \omega_{B'C'}) \leq 0 \qquad \forall \omega_{A'B'C'} \in D(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_{C'}) \tag{56}$$

for some function f. For the inflated state $\tau_{A'B'C'}$ (54) this inequality reduces to

$$f(\tau_{A'}, \tau_{B'}, \tau_{C'}, \tau_{A'B'}, \tau_{A'} \otimes \tau_{C'}, \tau_{B'C'}) \leq 0. \tag{57}$$

We now compare the marginals of the triangle network state $\rho_{A'B'C'}$ and the inflated state $\tau_{A'B'C'}$:

$$\begin{aligned} \tau_{A'} &= \rho_{A'} & \tau_{B'} &= \rho_{B'} & \tau_{C'} &= \rho_{C'} \\ \tau_{A'B'} &= \rho_{A'B'} & \tau_{B'C'} &= \rho_{B'C'}. \end{aligned} \tag{58}$$

Therefore, using Eq. (57) together with the marginal relations above, we obtain

$$f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'C'}) = f(\tau_{A'}, \tau_{B'}, \tau_{C'}, \tau_{A'B'}, \tau_{A'} \otimes \tau_{C'}, \tau_{B'C'}) \leq 0. \tag{59}$$

In this way we derive a nontrivial inequality which holds for all LO triangle network states. Analogous inequalities can be derived by considering different cuts or multiple cuts in Fig. 5b. In total we can summarize:

Theorem 1. *Let $f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'C'}, \rho_{B'C'}) \leq 0$ be an inequality which holds for all tripartite states $\rho_{A'B'C'}$. If $\rho_{A'B'C'}$ is a state of the form* (53)*, i.e., $\rho_{A'B'C'} \in \mathcal{F}^{LO}$, then*

$$\begin{aligned} f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'} \otimes \rho_{B'}, \rho_{A'C'}, \rho_{B'C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'C'}, \rho_{B'} \otimes \rho_{C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'} \otimes \rho_{B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'} \otimes \rho_{B'}, \rho_{A'C'}, \rho_{B'} \otimes \rho_{C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'} \otimes \rho_{C'}) &\leq 0 \\ f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'} \otimes \rho_{B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'} \otimes \rho_{C'}) &\leq 0 \end{aligned} \tag{60}$$

In the case where the function $F(\rho_{A'B'C'}) \equiv f(\rho_{A'}, \rho_{B'}, \rho_{C'}, \rho_{A'B'}, \rho_{A'} \otimes \rho_{C'}, \rho_{B'C'})$ is a convex function, the inequality also holds for LOSR states.

5.4 Multipartite Entanglement in LOSR Networks

In this section, we recall what is known about the set of LOSR states $\mathcal{F}^{\text{LOSR}}$. Understanding the structure of $\mathcal{F}^{\text{LOSR}}$ is important for clarifying which multipartite correlations can already be

produced from bipartite resources. On the other hand, we also introduce criteria which identify which state preparation necessarily requires genuinely multipartite resources.

5.4.1 LOSR Triangle Network

In contrast to the usual resource theory of genuine multipartite entanglement, where the free states are biseparable, we take the LOSR states as the free states $\mathcal{F}^{\mathrm{LOSR}}$. As discussed in Sec. 5.2, every biseparable state can be prepared in such a network scenario, i.e., $\mathcal{F}^{\mathrm{BS}} \subseteq \mathcal{F}^{\mathrm{LOSR}}$. Interestingly, it is shown in [18, 59] that the set of LOSR states $\mathcal{F}^{\mathrm{LOSR}}$ is actually strictly larger than the set of biseparable states, i.e.,

$$\mathcal{F}^{\mathrm{BS}} \subsetneq \mathcal{F}^{\mathrm{LOSR}}. \tag{61}$$

Thus, the set of LOSR states provides a strictly larger free set than the one used in the usual resource theory of genuine multipartite entanglement. In other words, in the LOSR network setting one is able to prepare states that are GME.

Since the set of LOSR states is difficult to characterize explicitly, it is natural to quantify the distance of a target state from this set. In this way, one asks not only whether the target state is within the set of LOSR states, but also how well it can be approximated using LOSR states.

In the context of state preparation, this is naturally measured by the maximal fidelity with the target state. Equivalently, one may consider the Bures distance from the target state to the set of LOSR states (see Eq. (38)).

As we discussed in Sec. 3.2, important multipartite entangled states are graph states. In the case of three parties, the only nontrivial graph state is the three-qubit GHZ state $\left|\mathrm{GHZ}_{3,2}\right\rangle$ (see Eq. (28)). For this state, the minimal Bures distance (38) to the set of biseparable states (see Eq. (39)) is known [12, 13]

$$R_B^{BS}\left(\left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|\right) = \inf_{\sigma\in\mathcal{F}^{BS}} D_B(\left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|, \sigma) = \sqrt{2-\sqrt{2}} \approx 0.765. \tag{62}$$

Equivalently, if a state ρ_{ABC} is biseparable then $F(\rho_{ABC}, \left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|) \leq \frac{1}{2}$. In [18] it is shown that there exist LOSR states whose fidelity with the GHZ state is about 0.517, i.e.,

$$R_B^{LOSR}\left(\left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|\right) = \inf_{\sigma\in\mathcal{F}^{LOSR}} D_B(\left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|, \sigma) \leq 0.750. \tag{63}$$

If the Bures distance is sufficiently small, the LOSR quantum networks could be a powerful tool to perform quantum tasks that require GHZ states. Therefore, one would also like to know

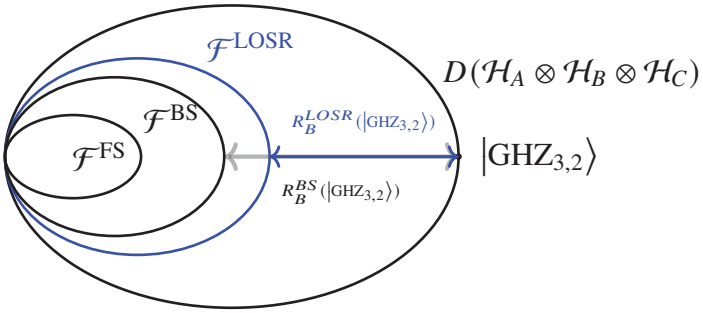


Figure 6: Illustration of the Bures distance from the three-qubit GHZ state to the biseparable set and to the LOSR set. LOSR states can approximate the GHZ state better than biseparable states, as explicit LOSR constructions exceed the biseparable fidelity threshold $1/2$ [18].

how small the Bures distance can be or equivalently how large the maximal fidelity can be at most. Some upper bounds are derived in [18, 20, 24, 60] using inflation technique (see Sec. 5.3). In particular, in [24, 60] an analytical bound of

$$\max_{\rho \in \mathcal{F}^{LOSR}} F(\rho, |\mathrm{GHZ}_{3,2}\rangle\langle\mathrm{GHZ}_{3,2}|) \leq 0.9 \tag{64}$$

is derived. Numerically, in [18] the bound can be improved to

$$\max_{\rho \in \mathcal{F}^{LOSR}} F(\rho, |\mathrm{GHZ}_{3,2}\rangle\langle\mathrm{GHZ}_{3,2}|) \leq (1 + \sqrt{3})/4 \approx 0.683. \tag{65}$$

For higher local dimension, we have [60]

$$\max_{\rho \in \mathcal{F}^{LOSR}} F(\rho, |\mathrm{GHZ}_{3,d}\rangle\langle\mathrm{GHZ}_{3,d}|) \leq \frac{1 + 2\sqrt{2d} + 2d}{3d + 2\sqrt{2d}}. \tag{66}$$

Thus, the GHZ state lies strictly outside the LOSR set, but it can still be approximated nontrivially by LOSR states. However, the gap between the known upper and lower bounds is too large, to determine whether LOSR is only a small extension of the biseparable set or whether it is actually a very powerful setting for approximate GHZ preparation.

5.4.2 LOSR Networks with More Than Three Parties

In the scenario of more than three parties, the situation is more involved because there are more graph states that can be chosen to be the target state than the GHZ state. As in the tripartite case, no connected graph state involving at least three parties can be prepared exactly within the LOSR network setting. However, much less is known in the case of more than three parties

than in the tripartite setting. General no-go results exclude connected graph state preparation with fidelity larger than 0.9, i.e.,

$$\max_{\rho \in \mathcal{F}^{LOSR}} F(\rho, |\mathcal{G}\rangle\langle\mathcal{G}|) \leq 0.9. \tag{67}$$

In particular, nontrivial general lower bounds on the maximal fidelity achievable with LOSR states are still unknown.

In Sec. 9.1, we address this question by deriving improved upper bounds on the fidelity achievable in LOSR networks (also see [59]).

6 Conference Key Agreement

Conference key agreement (CKA) is the multipartite generalization of quantum key distribution [1]. While standard quantum key distribution considers two parties that want to establish a shared secret key, in conference key agreement several parties aim to generate one common secret key that is known to all participants and unknown to any eavesdropper.

In the quantum setting, conference key agreement can be implemented by distributing multipartite entangled states among the parties and performing suitable local measurements [2]. The security of the resulting key depends on how strongly the parties are correlated with each other and how much information an adversary may have about the measurement outcomes. For this reason, entropic quantities play a central role in the analysis of CKA protocols [61, 62].

In this section, we first introduce the quantum entropies that are needed to quantify correlations and information leakage. We then recall the Devetak-Winter key rate [61], which gives an achievable asymptotic secret key rate in terms of mutual informations. Finally, we discuss a multipartite version of the BB84 protocol as an example of a CKA protocol and explain how the key rate can be evaluated in this setting.

6.1 Quantum Entropies

When a state ρ_A is expressed in its spectral decomposition, its von Neumann entropy quantifies the uncertainty associated with the corresponding eigenvalue distribution.

Within the setting of quantum key distribution, entropies are also useful to measure for instance the information an adversary can gain during a quantum key distribution protocol [61, 62]. The

von Neumann entropy of a state $\rho_A \in D(\mathcal{H}_A)$ is defined by

$$H(\rho_A) = -\operatorname{Tr}\left[\rho_A \log_2(\rho_A)\right] \tag{68}$$

with the convention $0 \log_2 0 = 0$. Note that the entropy only depends on the spectrum of the state ρ_A, i.e.,

$$H(\rho_A) = -\sum_{i=0}^{d-1} \lambda_i \log_2(\lambda_i), \tag{69}$$

where $\{\lambda_i\}_{i=0}^{d-1}$ are the eigenvalues of the state ρ_A.

In particular, the von Neumann entropy vanishes for pure states, which means there is no uncertainty about the state itself, and it is maximal for the maximally mixed state $\rho_A = \frac{1}{d}\mathbb{1}_A$. In the following, we will also use the notation $H(A)_\rho = H(\rho_A)$. In composite quantum systems, entropy is also an important tool for characterizing correlations between subsystems, including entanglement. For example, for pure bipartite states, the entropy of a reduced state also has an entanglement interpretation. If ρ_{AB} is a pure state, then nonzero $H(A)_\rho = H(B)_\rho$ indicates entanglement between A and B. The *quantum mutual information* is defined by

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(AB)_\rho. \tag{70}$$

The quantum mutual information measures the total amount of correlations between the subsystems A and B.

6.2 Devetak-Winter Key Rate

In the entanglement based description of a QKD protocol, two parties, say Alice (A) and Bob (B), start by sharing a bipartite quantum state ρ_{AB}. To analyze security, one considers a purification $|\psi\rangle\langle\psi|_{ABE}$, where the purifying system E is assigned to an eavesdropper called Eve (E). After Alice performs her measurement, the state becomes a classical quantum quantum state (cqq state for short) of the following form

$$\rho_{XBE} = \sum_x p_x \, |x\rangle\langle x|_X \otimes \rho_{BE}^x, \tag{71}$$

where X denotes Alice's classical outcome.

An important quantity that describes the achievable asymptotic[5] key rate is the Devetak-Winter

[5]Here, asymptotic refers to the limit in which the number of distributed signals, i.e., the quantum systems

key rate [61], which is given by

$$r_{DW} = I(X : B)_\rho - I(X : E)_\rho \tag{72}$$

where ρ is the cqq state (see Eq. (71)). The first term $I(X : B)_\rho$ quantifies how much information is available to Bob about Alice's classical raw key. The second term $I(X : E)_\rho$ quantifies how much information Eve can gain during the protocol. For conference key agreement, the Devetak-Winter rate for two parties can be extended to N parties as follows [2, 63]: The idea is to replace Bob by several parties $B_1, \ldots, B_{N-1}$. After Alice's measurement, the relevant state becomes

$$\rho_{XB_1\cdots B_{N-1}E} = \sum_x p(x) \ |x\rangle\langle x|_X \otimes \rho^x_{B_1\cdots B_{N-1}E}. \tag{73}$$

Now the final key must be recovered not just by one Bob, but by all Bobs $B_1, B_2, \ldots B_{N-1}$. Therefore, the protocol is limited by the party with the weakest correlation to Alice's raw key. For this reason, the bipartite term $I(X:B)_\rho$ is replaced by the minimum over all parties, i.e.,

$$\min_{i=1,2,\ldots,N-1} I(X:B_i)_\rho. \tag{74}$$

Eve's information is still quantified by $I(X : E)_\rho$, since secrecy must hold against the eavesdropper exactly as before. This leads to the multipartite one-way extension

$$r^{CKA}_{DW} = \min_{i=1,2,\ldots N-1} I(X:B_i)_\rho - I(X:E)_\rho \tag{75}$$

(see [61, 63] for more details).

6.3 Multipartite BB84 Protocol

The multipartite BB84 protocol is one of the simplest and most natural examples of a conference key agreement protocol [2, 64]. It is based on the distribution of a GHZ state in each protocol round. The idea of the protocol is the following: A source prepares the multipartite GHZ state $\left|\mathrm{GHZ}_{N,2}\right\rangle$ and distributes one subsystem to each of the parties $A, B_1, \ldots, B_{N-1}$. However, in a realistic scenario, the parties do not share a perfect GHZ state but rather a noisy state, say $\rho_{AB_1B_2\ldots B_{N-1}}$. Then the parties randomly measure either in the Z-basis, i.e., $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, or in the X-basis, i.e., $\{|+\rangle\langle +|, |-\rangle\langle -|\}$. If all parties measure in the Z-basis, they use the

distributed in the individual protocol rounds, tends to infinity. We assume that the protocol rounds are independent and identically distributed.

measurement outcomes partly for the key generation and partly for the parameter estimation. If all parties measure in the X-basis, they use all the outcomes for the parameter estimation. In the parameter estimation, the parties publicly compare the measurement outcomes in order to estimate how much noise is present in the quantum channel, and therefore how much information an eavesdropper could have gained. More formally the parties compute

$$E_X = \frac{1 - \mathrm{Tr}\left[X^{\otimes N} \rho_{AB_1B_2\ldots B_{N-1}}\right]}{2} \tag{76}$$

and

$$E_{AB_i} = \frac{1 - \mathrm{Tr}\left[Z_A \otimes Z_{B_i} \rho_{AB_i}\right]}{2} \tag{77}$$

for all $i = 1, 2, \ldots, N-1$ which can be interpreted as error rates. Finally, the parties perform the classical post-processing steps of the protocol. First, Alice broadcasts sufficient information for the Bobs to correct their raw keys and match her key. Finally, the parties perform privacy amplification to extract a shorter final secret conference key.

In the multipartite BB84 protocol, the multipartite Devetak-Winter key rate reduces to [64]

$$r_{\mathrm{BB84}} = 1 - h\left(E_X\right) - \max_{i=1,2,\ldots,N-1} h\left(E_{AB_i}\right) \tag{78}$$

where h is the binary entropy defined as

$$h(p) = -p \log_2 p - (1-p) \log_2 (1-p), \tag{79}$$

for $p \in [0, 1]$. The asymptotic key rate for the BB84 protocol can be considered as a map from the input source state to the real numbers, i.e., $r_{\mathrm{BB84}} : D(\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2} \otimes \cdots \otimes \mathcal{H}_{B_{N-1}}) \to \mathbb{R}$. In the ideal situation, the parties share a GHZ state as the input state. In this case the error rates (76) and (77) are zero and the asymptotic key rate becomes 1, i.e., $r_{\mathrm{BB84}}\left(\left|\mathrm{GHZ}_{N,2}\right\rangle\!\left\langle\mathrm{GHZ}_{N,2}\right|\right) = 1$.

In Sec. 9.2 we will use this key rate expression to analyze conference key agreement in LOSR networks and present the bounds obtained in [65].

7 Absolute Separability

In the previous sections, bipartite entanglement was treated as a freely available resource. In practice, however, even bipartite entanglement can be difficult to create and preserve, especially over long distances because quantum systems and channels are typically affected by

noise [26, 66, 67]. If the noise is too strong, it can destroy all entanglement between the two subsystems [68]. Some mixed states can even be so noisy that no global unitary can transform them into entangled states. These states are called absolute separable and they were introduced in [27]. Since unitaries preserve the spectrum of a state, absolute separability is a spectral property and is therefore also sometimes called separability from spectrum. Although the problem is fully solved for qubit–qudit systems [28], no complete characterization is known in general dimensions. In this chapter, we recall the definition of absolute separable states and the results known so far.

7.1 Definition and Basic Properties

In the following, let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\dim(\mathcal{H}_A) = d_A$ and $\dim(\mathcal{H}_B) = d_B$. The eigenvalues of ρ_{AB} are denoted by $\mathrm{Spec}(\rho_{AB}) = (\lambda_1, \lambda_2, \ldots, \lambda_{d_A d_B})$ where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{d_A d_B}$. A bipartite state ρ_{AB} is called *absolutely separable* if

$$U\rho_{AB}U^\dagger \tag{80}$$

is separable for all unitaries U. In the following, we denote the set of absolute separable states by AS. Note that the property of absolute separability is entirely determined by the eigenvalues of the state because global unitaries can change the eigenvectors of a state but leave the eigenvalues invariant.

A simple example of an absolute separable state is the maximally mixed state $\rho_{AB} = \frac{\mathbb{1}}{d_A d_B}$ as it is invariant under all unitary transformations. Since a complete characterization of absolute separable states is not known, it is therefore useful to consider a larger class of states which provides necessary conditions for absolute separability, namely the set of absolute PPT states:

A state ρ_{AB} is called *absolutely PPT* if

$$U\rho_{AB}U^\dagger \tag{81}$$

is PPT for all unitaries U. The set of absolute PPT states is denoted by $APPT$. The set of absolute PPT states is especially useful as it can be fully characterized by a finite family of linear matrix inequalities [69]. Any such linear matrix inequality can be considered as a necessary condition on absolute PPT states and therefore also for absolute separable states. The following important eigenvalue inequality is obtained from this linear matrix inequality characterization.

Theorem 2 ([69], [29]). *Let ρ_{AB} be an absolute PPT state. Then*

$$\lambda_1 \leq \lambda_{d_A d_B - 1} + 2\sqrt{\lambda_{d_A d_B} \lambda_{d_A d_B - 2}} \tag{82}$$

In the case where one local dimension of a subsystem is 2 , i.e., $\dim(\mathcal{H}_A) = 2$ or $\dim(\mathcal{H}_B) = 2$, the set of absolute PPT states is even fully characterized by inequality (82). Interestingly, it was shown that in this case the set of absolute PPT states is equivalent to the set of absolute separable states:

Theorem 3 ([28]). *Let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\dim(\mathcal{H}_A) = 2$ and $\dim(\mathcal{H}_B) = d_B$. Then the following statements are equivalent:*

1. *ρ_{AB} is absolute separable.*
2. *ρ_{AB} is absolute PPT.*
3. $\lambda_1 \leq \lambda_{2d_B - 1} + 2\sqrt{\lambda_{2d_B} \lambda_{2d_B - 2}}$.

For higher dimensions, absolute PPT provides only necessary conditions for absolute separability. It is therefore natural to also look for sufficient conditions that guarantee that a state is absolute separable.

7.2 Sufficient Conditions for Absolute Separability

Complementary to the necessary conditions, several sufficient criteria for absolute separability are known:

Theorem 4 ([70]). *A state ρ_{AB} is absolute separable if*

$$\mathrm{Tr}\left[\rho^2\right] \leq \frac{1}{d_A d_B - 1}. \tag{83}$$

The condition in Thm. 4 depends only on the purity of the state. It shows that all states with sufficiently small purity, or equivalently states which are sufficiently close to the maximally mixed state, are absolutely separable. This gives a ball of absolute separable states around the maximally mixed state with respect to the Hilbert–Schmidt norm.

Theorem 5 ([71]). *A state ρ_{AB} is absolute separable if*

$$\lambda_{d_A d_B} \geq \frac{1}{d_A d_B + 2} \qquad \text{or} \qquad \lambda_1 \leq \frac{1}{d_A d_B - 1} \tag{84}$$

Thm. 5 can be viewed as simple extremal eigenvalue criteria ensuring that a state is sufficiently mixed to be absolute separable.

7.3 Boundary States

To characterize the set of absolute separable states one might ask about its boundary points. One way to find such points is by considering the intersection of the boundary of absolute PPT states together with sufficient conditions for absolute separability. An important class of states on the boundary of AS are states with eigenvalues

$$\mathrm{Spec}(\rho) = \left(\frac{1}{d_A d_B - 1}, \frac{1}{d_A d_B - 1}, \ldots, \frac{1}{d_A d_B - 1}, 0\right). \tag{85}$$

It is easy to see that states with this spectrum lie on the boundary of the set of absolutely separable states. Indeed, they are on the boundary of the set of states described by Thm. 4 which implies that they are absolute separable. In addition, they are on the boundary of the set of states described by Thm. 2 which implies that they are on the boundary of absolute PPT states. Surprisingly, this is the only class of absolute separable states which are not of full rank, i.e., states where $\lambda_{d_A d_B} = 0$. To see this, note first that inequality (82) implies that no absolute PPT state can have rank less than $d_A d_B - 1$. Otherwise, $\lambda_1 \leq 0$ which is a contradiction. Furthermore, for states of rank $d_A d_B - 1$, inequality (82) yields $\lambda_1 \leq \lambda_{d_A d_B - 1}$, which implies that $\lambda_1 = \lambda_2 = \cdots = \lambda_{d_A d_B - 1} = \frac{1}{d_A d_B - 1}$. Another example is provided by states that have the same spectrum as the state

$$\rho_{AB} = \frac{\mathbb{1} - \left|\phi_d^+\right\rangle\!\left\langle\phi_d^+\right|^{T_B}}{d_A d_B - 1} \tag{86}$$

where $\left|\phi_d^+\right\rangle$ is the Bell state given in Eq. (19) with $d := \min\{d_A, d_B\}$. This state is on the boundary of PPT states as $\left\langle\phi_d^+\right| \rho_{AB}^{T_B} \left|\phi_d^+\right\rangle = 0$ and also on the boundary of the set of states described by Thm. 4 since

$$\mathrm{Tr}\left[\rho_{AB}^2\right] = \frac{\mathrm{Tr}[\mathbb{1}] - 2\,\mathrm{Tr}\left[|\phi^+\rangle\!\langle\phi^+|^{T_B}\right] + \mathrm{Tr}\left[|\phi^+\rangle\!\langle\phi^+|^{T_B} |\phi^+\rangle\!\langle\phi^+|^{T_B}\right]}{(d_A d_B - 1)^2} = \frac{d_A d_B - 2 + 1}{(d_A d_B - 1)^2} = \frac{1}{d_A d_B - 1}. \tag{87}$$

In the case where $d_A = d_B$ the state (86) reduces to a Werner state [72].

8 Magic States

In this chapter, we introduce the resource theory of magic states. In Sec. 8.1, we motivate this theory from the perspective of universal quantum computation. In particular, we discuss Clifford operations, the Gottesman Knill theorem, and the role of non-Clifford resources in obtaining universality. In Sec. 8.2, we define stabilizer states, magic states, and the corresponding free operations. In Sec. 8.3, we specialize to the single-qubit setting, where the set of free states admits a simple geometric description as they form an octahedron inside the Bloch ball. Finally, in Sec. 8.4, we introduce the relative entropy of magic and discuss its additivity properties under tensor products, which will be relevant for the results presented later in this thesis.

8.1 Introduction

In the previous section (Sec. 7) we considered the action of global unitary transformations on bipartite quantum states. In this scenario, we fix a bipartite tensor product structure $\mathcal{H}_A \otimes \mathcal{H}_B$ and ask whether a state ρ_{AB} remains separable under every global unitary transformation U acting on the composite system.

In quantum computation, the role of unitary transformations is different. Here unitary transformations are considered from a more operational point of view. A quantum algorithm may be described abstractly by a unitary acting on many qubits, but in an actual implementation such a unitary has to be decomposed into a sequence of elementary gates which typically act on one or two qubits. Compositions of such gates can then approximate arbitrary unitaries on an n qubit system. This leads to the question of universality. Which restricted sets of gates are sufficient to implement general quantum computations?

A particularly important class of gates is given by the Clifford unitaries. They are defined by the property that they map Pauli operators to Pauli operators [43]. This class contains important operations such as Hadamard gates, Pauli gates, and the entangling controlled-NOT gate (see e.g. [73]). Nevertheless, Clifford operations alone do not provide universal quantum computation. Indeed, according to the Gottesman Knill theorem, quantum circuits which consist only of Clifford unitaries, Pauli measurements, and classical processing can be efficiently simulated on a classical computer [32].

To obtain universality, one needs a non-Clifford gate. A standard example is the T gate. One way to implement such a gate is by using an ancillary magic state. By using only stabilizer operations together with this ancillary state, one can implement an effective T gate [31, 33].

This observation motivates a resource-theoretic viewpoint. In the resource theory of magic, stabilizer states and stabilizer operations are treated as free [30, 31]. They are treated as free not

because they are necessarily unentangled or structurally simple, but because they belong to a class of processes that remains efficiently classically simulable. States that cannot be written as convex combinations of stabilizer states are called magic states, and they are considered as a resource in this setting.

This also shows that magic is conceptually different from entanglement. In Sec. 5, entanglement and particularly graph states were considered as resources. However, graph states are stabilizer states and are therefore considered as free in the setting of universal quantum computation. Thus, a state may be highly entangled and still belong to the free set of the resource theory of magic.

8.2 Definition

Let $\mathcal{H}^{\otimes n}$ be the Hilbert space of an n qubit system, i.e., $\dim(\mathcal{H}) = 2$. Furthermore, let C_n be the *Clifford group on n qubits*, which is the set of unitaries that map Pauli operators to Pauli operators, i.e.,

$$C_n := \{U \mid UPU^\dagger \in \mathcal{P}_n \text{ for all } P \in \mathcal{P}_n\}, \tag{88}$$

where U is a unitary operator and $\mathcal{P}_n$ is the n qubit Pauli group, i.e.,

$$\mathcal{P}_n := \{\alpha P_1 \otimes P_2 \otimes \cdots \otimes P_n \mid \alpha \in \{\pm 1, \pm i\}, P_j \in \{\mathbb{1}, X, Y, Z\}\} \tag{89}$$

(see e.g. [43]). Here X, Y, Z are the Pauli operators (see Eq. (2)). The *set of pure stabilizer states* is defined by

$$\mathcal{S} := \{U(|0\rangle\langle 0|^{\otimes n})U^\dagger \mid U \in C_n\}. \tag{90}$$

The set of free states can then be defined as the convex hull of the pure stabilizer states, namely

$$\mathcal{F}^{\text{STAB}}(\mathcal{H}^{\otimes n}) := \left\{\sigma \in D(\mathcal{H}^{\otimes n}) \mid \sigma = \sum_j p_j S_j,\ 0 \le p_j \le 1,\ \sum_j p_j = 1,\ S_j \in \mathcal{S}\right\}. \tag{91}$$

States in the set $D(\mathcal{H}^{\otimes n}) \setminus \mathcal{F}^{\text{STAB}}(\mathcal{H}^{\otimes n})$ are called *magic states*. We take the free operations to be Clifford unitaries, stabilizer state preparations, Pauli measurements, classical randomness, and discarding subsystems [30, 31].

8.3 Single Qubit Resource Theory of Magic

In the following, we describe the resource theory of magic for a single qubit system. The pure single qubit stabilizer states are precisely the six eigenstates of the Pauli operators X, Y, and Z defined in Eq. (2) (see e.g. [73]). In the Bloch vector representation (see Sec. 2.2), these states correspond to the six vectors

$$\begin{aligned} s_1 &= (1,0,0), & s_2 &= (0,1,0), & s_3 &= (0,0,1) \\ s_4 &= (-1,0,0), & s_5 &= (0,-1,0), & s_6 &= (0,0,-1). \end{aligned} \tag{92}$$

The convex hull of these six points forms an octahedron inside the Bloch ball. Important examples of qubit magic states are the so called T-type states and H-type states [33, 74]. Up to Clifford unitaries, these states can be represented by

$$|T\rangle\langle T| = \frac{1}{2}\left(\mathbb{1} + \frac{1}{\sqrt{3}}(X+Y+Z)\right) \tag{93}$$

and

$$|H\rangle\langle H| = \frac{1}{2}\left(\mathbb{1} + \frac{1}{\sqrt{2}}(X+Y)\right). \tag{94}$$

These states are particularly important because, together with Clifford unitaries, they enable universal quantum computation [33, 74].

8.4 Relative Entropy of Magic

In order to quantify the amount of magic a quantum state has we use as a measure the relative entropy of magic, i.e.,

$$R_{\text{rel}}^{\text{magic}}(\rho) := \inf_{\sigma \in \mathcal{F}^{\text{STAB}}(\mathcal{H}^{\otimes n})} D(\rho||\sigma), \tag{95}$$

where $D(\cdot||\cdot)$ denotes the quantum relative entropy (see Eq. (42) and Eq. (43)).

A particularly important structural question is whether the relative entropy of magic is additive under tensor products. Since the tensor product of two stabilizer states is again a stabilizer state, the relative entropy of magic is in general subadditive, i.e.,

$$R_{\text{rel}}^{\text{magic}}(\rho \otimes \tau) \leq R_{\text{rel}}^{\text{magic}}(\rho) + R_{\text{rel}}^{\text{magic}}(\tau). \tag{96}$$

In some cases the relative entropy of magic becomes additive. Let $\sigma_\rho \in \operatorname{argmin}_{\sigma\in\mathcal{F}^{\mathrm{STAB}}(\mathcal{H}_A)} D(\rho\|\sigma)$ and $\sigma_\tau \in \operatorname{argmin}_{\sigma\in\mathcal{F}^{\mathrm{STAB}}(\mathcal{H}_A)} D(\tau\|\sigma)$. If $\sigma_\rho \otimes \sigma_\tau$ is the closest stabilizer state to the state $\rho \otimes \tau$, then the relative entropy of magic is additive. This, however, is not true in general. Explicit counterexamples are known even for tensor products of single qubit states, showing that additivity is not a generic property of the relative entropy of magic (see [75]). Nevertheless, additivity holds for important classes of magic states. A sufficient condition is that all but possibly one of the single-qubit states commute with their closest stabilizer states [75]. More precisely, if $\{\rho_i\}_{i=1,2,\ldots,N}$ are single qubit states and $\{\sigma_i \in \operatorname{argmin}_{\sigma\in\mathcal{F}^{\mathrm{STAB}}(\mathcal{H})} D(\rho_i\|\sigma)\}_{i=1,2,\ldots,N}$ are the corresponding closest stabilizer states such that

$$[\rho_i, \sigma_i] = 0 \tag{97}$$

for all but possibly one value of i, then the relative entropy of magic is additive, i.e.,

$$R^{\mathrm{magic}}_{\mathrm{rel}}\left(\bigotimes_{i=1}^{N} \rho_i\right) = \sum_{i=1}^{N} R^{\mathrm{magic}}_{\mathrm{rel}}(\rho_i). \tag{98}$$

This result applies in particular to the standard single qubit magic states lying on symmetry axes of the stabilizer octahedron, including the H-type states (94) and T-type states (93), as well as their depolarized versions (see [75] for more details). For example, the closest state to the T-type state (93) is given by

$$\tilde{\sigma} = \frac{1}{2}\left(\mathbb{1} + \frac{1}{3}(X + Y + Z)\right) \in \operatorname*{argmin}_{\sigma\in\mathcal{F}^{\mathrm{STAB}}(\mathcal{H})} D(|T\rangle\langle T| \,\|\, \sigma). \tag{99}$$

It is easy to see that $[|T\rangle\langle T|, \tilde{\sigma}] = 0$. Hence,

$$R^{\mathrm{magic}}_{\mathrm{rel}}(|T\rangle\langle T|^{\otimes n}) = n\, R^{\mathrm{magic}}_{\mathrm{rel}}(|T\rangle\langle T|). \tag{100}$$

Thus, the sufficient condition above is closely related to the structure of non-additivity. Indeed, in Sec. 9.4 we show that, for tensor products of single qubit magic states, additivity fails for a large class of states which do not commute with their closest stabilizer states (see [76] for more details).

9 Summary of the Results

In this chapter, we summarize the main results of this thesis. First, we discuss the results on multipartite entanglement in LOSR networks and present limitations on the preparation of genuinely multipartite entangled states from bipartite resources [59]. We then study the role of LOSR networks in conference key agreement, and show how the network restrictions constrain the achievable key rate [65]. Afterwards, we consider a strengthened version of absolute separability, called complete absolute separability, and characterize states which remain separable even under probabilistic unital transformations and postselection [77]. Finally, we discuss the additivity of the relative entropy of magic for tensor products of single-qubit magic states [76].

9.1 Multipartite Entanglement in LOSR Networks

In this section, we recall the main results of [59]. The section is structured as follows. In Sec. 9.1.1 we recall the tripartite LOSR network setting and present fidelity bounds for the approximation of GHZ states. In Sec. 9.1.2 we extend this discussion to networks with more than three parties and consider multipartite GHZ and graph states. In Sec. 9.1.3, we study LOSR networks whose underlying graph is not fully connected and derive corresponding bounds on the achievable fidelity with GHZ and W states. Finally, in Sec. 9.1.4, we allow LOCC operations and treat classical communication as a resource. In this setting, we derive the minimal amount of classical communication required to generate multipartite GHZ states from bipartite sources.

9.1.1 Tripartite LOSR Network

We begin with the tripartite triangle scenario. This is the simplest fully connected network in which one can ask how much genuinely multipartite entanglement can be generated in such networks. We show that LOSR networks are strongly limited in their ability to approximate highly entangled multipartite target states. In particular, we derive upper bounds on the maximal fidelity between LOSR states and GHZ states. We show that the maximal achievable fidelity is upper bounded by a quantity that decreases with the local dimension. This gives us novel sufficient conditions for detecting states outside $\mathcal{F}^{\mathrm{LOSR}}$ and therefore serve as witnesses for genuine network multipartite entanglement.

Theorem 6. *The maximum fidelity between a three partite LOSR state and the d-dimensional*

GHZ state is at most $1/\sqrt{d}$*, i.e.,*

$$\max_{\rho_{ABC}\in\mathcal{F}^{LOSR}} F(\rho_{ABC}, |GHZ_{3,d}\rangle\langle GHZ_{3,d}|) \leq \frac{1}{\sqrt{d}} \tag{101}$$

Proof. First, note that every LOSR state has the form

$$\rho_{ABC} = \sum_{\lambda\in I} p_\lambda \rho^\lambda_{ABC} \tag{102}$$

where each ρ^λ_{ABC} is a network state obtained from bipartite sources using only local operations. Since the target state is a pure state, the fidelity becomes linear (see Prop. 4), i.e.,

$$F(\rho_{ABC}, |\mathrm{GHZ}_{3,d}\rangle\langle \mathrm{GHZ}_{3,d}|) = \sum_{\lambda\in I} p_\lambda F(\rho^\lambda_{ABC}, |\mathrm{GHZ}_{3,d}\rangle\langle \mathrm{GHZ}_{3,d}|) \tag{103}$$

Thus, to maximize the fidelity, we can restrict ourselves to LOSR states without shared randomness as the shared randomness mixture cannot increase the maximum. Using Prop. 6, we can upper bound the fidelity by choosing a fixed POVM. Here, we choose the von Neumann measurement in the computational basis, i.e., $\{|ijk\rangle\langle ijk|\}_{i,j,k\in\{0,\dots,d-1\}}$. Thus,

$$F(\rho^\lambda_{ABC}, |\mathrm{GHZ}_{3,d}\rangle\langle \mathrm{GHZ}_{3,d}|) \leq \left(\sum_{i,j,k\in\{0,1,\dots,d-1\}} \sqrt{\mathrm{Tr}\left[|ijk\rangle\langle ijk|\,\rho^\lambda_{ABC}\right]}\, |\langle ijk|\mathrm{GHZ}_{3,d}\rangle| \right)^2 \tag{104}$$

$$= \frac{1}{d}\left(\sum_{i\in\{0,1,\dots,d-1\}} \sqrt{\mathrm{Tr}\left[|iii\rangle\langle iii|\,\rho^\lambda_{ABC}\right]} \right)^2$$

$$= \frac{1}{d}\left(\sum_{i\in\{0,1,\dots,d-1\}} \sqrt{p(i,i,i)} \right)^2$$

Hence, the fidelity can be upper bounded in terms of the probabilities that the parties measure the same outcome i (see Eq. (4)). We now use another restriction for networks with bipartite source states and local operations but without shared randomness which was established in [78]. It states that for each local projective measurement $\{P_i\}_{i=0}^{d-1}$ and all triangle network states without shared randomness,

$$\mathrm{Tr}\big(\rho P_i \otimes P_j \otimes P_k\big) \leq \sqrt{\mathrm{Tr}(\rho P_i \otimes \mathbb{1} \otimes \mathbb{1})\,\mathrm{Tr}\big(\rho \mathbb{1} \otimes P_j \otimes \mathbb{1}\big)\,\mathrm{Tr}(\rho \mathbb{1} \otimes \mathbb{1} \otimes P_k)} \tag{105}$$

holds. Therefore, the probability that all the parties measure the same outcome i can be upper bounded as follows:

$$p(i,i,i) \leq \sqrt{p_A(i)p_B(i)p_C(i)}, \tag{106}$$

where $p_A(i) = \mathrm{tr}(\rho\,|i\rangle\langle i| \otimes \mathbb{1} \otimes \mathbb{1})$, $p_B(i) = \mathrm{tr}(\rho \mathbb{1} \otimes |i\rangle\langle i| \otimes \mathbb{1})$ and $p_C(i) = \mathrm{tr}(\rho \mathbb{1} \otimes \mathbb{1} \otimes |i\rangle\langle i|)$ are the marginal probabilities of the single parties to measure outcome i. To estimate the right hand side of Eq. (106) we need to introduce the Matusita fidelity (see [79, 80]). Let $\{p_{A_1}(i)\}_{i\in I}, \{p_{A_2}(i)\}_{i\in I}, \ldots, \{p_{A_N}(i)\}_{i\in I}$ be possibly different probability distributions. The *Matusita fidelity* is then defined by

$$\tilde{F}\left(\{p_{A_1}(i)\}_{i\in I}, \{p_{A_2}(i)\}_{i\in I}, \ldots, \{p_{A_N}(i)\}_{i\in I}\right) = \sum_{i\in I} \left(p_{A_1}(i)p_{A_2}(i)\ldots p_{A_N}(i)\right)^{\frac{1}{N}}. \tag{107}$$

An important property of the Matusita fidelity is that it is bounded by one [80], i.e.,

$$\tilde{F}\left(\{p_{A_1}(i)\}_{i\in I}, \{p_{A_2}(i)\}_{i\in I}, \ldots, \{p_{A_N}(i)\}_{i\in I}\right) \leq 1 \tag{108}$$

Therefore,

$$\sum_{i\in I} \sqrt{p(i,i,i)} \leq d^{\frac{1}{4}} \sum_{i\in I} \left(p_A(i)p_B(i)p_C(i)\frac{1}{d}\right)^{\frac{1}{4}} \leq d^{\frac{1}{4}} \tag{109}$$

Inserting (109) into (104) yields the desired result. □

Compared with the earlier analytic bound of [60] (see Eq. (66)), the bound in Thm. 6 is uniformly stronger for all local dimensions (see Fig. 7). Moreover, the asymptotic behavior of the bound given by Thm. 6 is qualitatively different. The previous analytic bound converges to $\frac{2}{3}$, while the new bound decays as $d^{-\frac{1}{2}}$ and therefore tends to zero. This means that in large local dimension, the network model has asymptotically vanishing ability to reproduce the target state.

Corollary 1. *Let $\mathcal{F}^{LOSR}$ denote the set of tripartite states that can be prepared in a three partite LOSR network. Then the maximum fidelity is bounded by*

$$\max_{\rho_{ABC}\in\mathcal{F}^{LOSR}} F(\rho_{ABC}, \left|GHZ_{3,2}\right\rangle\!\left\langle GHZ_{3,2}\right|^{\otimes n}) \leq 2^{-\frac{n}{2}} \tag{110}$$

Proof. Note that $\left|\mathrm{GHZ}_{3,2}\right\rangle^{\otimes n} \cong \left|\mathrm{GHZ}_{3,2^n}\right\rangle$ (see e.g. [81]). □

The corollary shows that the maximal fidelity decays exponentially with the number of copies

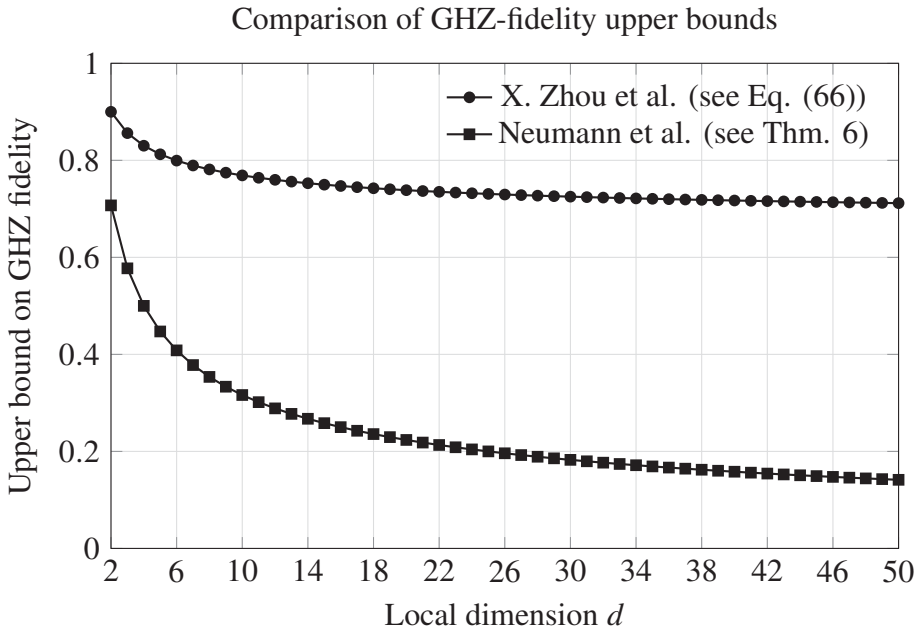


Figure 7: Comparison of analytic upper bounds on the maximal GHZ fidelity achievable by tripartite LOSR network states. While the bound of [60] remains finite in the large-d limit, the bound of [59] scales as $1/\sqrt{d}$ and hence tends to zero, showing a much stronger limitation on GHZ state preparation in high local dimension.

of the GHZ state they want to generate. Therefore, the limitations of LOSR networks become stronger in the many copy setting.

In the case where the target state is simply the single copy qubit GHZ state, i.e., $\left|\mathrm{GHZ}_{3,2}\right\rangle$ we can improve the upper bound:

Theorem 7. *For every three qubit LOSR state, i.e.,* $\rho_{ABC} \in D(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ *s.t.* $\dim \mathcal{H}_A = \dim \mathcal{H}_B = \dim \mathcal{H}_C = 2$*, we have*

$$\max_{\rho_{ABC} \in \mathcal{F}^{LOSR}} F(\rho_{ABC}, \left|GHZ_{3,2}\right\rangle\!\left\langle GHZ_{3,2}\right|) < 0.61. \tag{111}$$

The proof is based on inflation technique together with Prop. 6 (see [59] for more details). The novel upper bounds show that LOSR networks are less promising for multipartite state preparation than one might initially expect. Although LOSR networks can generate states that are genuinely multipartite entangled, their ability to approximate highly resourceful states such as GHZ states remains strongly limited. Thus, whereas previous bounds [18, 20, 24, 60] did not exclude the possibility that LOSR networks remain useful to approximate the GHZ state, our bounds show that this is not the case. In particular, for large local dimension the best achievable fidelity tends to zero.

9.1.2 LOSR Network with Many Parties

We now turn to an LOSR network setting with at least four parties. The following results show that increasing the number of parties does not overcome the limitations found in the tripartite case. In fact, for $N \geq 4$ the maximal fidelity with the N-partite GHZ state is already bounded by $1/d$, which is the same value that is attainable by a fully separable state. We also obtain an exponentially decaying bound for cluster states, showing that LOSR networks remain strongly limited for other multipartite target states as well.

Theorem 8. *In an LOSR network with $N \geq 4$ nodes, the maximal fidelity with $\left|GHZ_{N,d}\right\rangle$ is bounded by $1/d$, i.e.,*

$$\max_{\rho_{A_1A_2\ldots A_N} \in \mathcal{F}^{LOSR}} F(\rho_{A_1A_2\ldots A_N}, \left|GHZ_{N,d}\right\rangle\!\left\langle GHZ_{N,d}\right|) \leq \frac{1}{d} \tag{112}$$

Proof. The proof is analogous to the proof of Thm. 6. Again, we obtain an upper bound on the fidelity by applying the von Neumann measurement in the computational basis (see Prop. 6)

$$\begin{aligned}
\max_{\rho_{A_1A_2\ldots A_N} \in \mathcal{F}^{LOSR}} F(\rho_{A_1A_2\ldots A_N}, \left|\mathrm{GHZ}_{N,d}\right\rangle\!\left\langle \mathrm{GHZ}_{N,d}\right|) &\leq \frac{1}{d}\left(\sum_{i=0}^{d-1}\sqrt{p(i,i,\ldots,i)}\right)^2 \\
&\leq \frac{1}{d}\left(\sum_{i=0}^{d-1}\left(p_{A_1}(i)p_{A_2}(i)\ldots p_{A_N}(i)\right)^{\frac{1}{4}}\right)^2 \\
&\leq \frac{1}{d}\left(\sum_{i=0}^{d-1}\left(p_{A_1}(i)p_{A_2}(i)p_{A_3}(i)p_{A_4}(i)\right)^{\frac{1}{4}}\right)^2 \\
&\leq \frac{1}{d}
\end{aligned} \tag{113}$$

In the second step, we used the extension of the Finner inequality (106) to more parties (see [78]) and in the last step, we again used the fact that the Matusita fidelity is bounded by one. □

The bound of Thm. 8 is tight and can be saturated by a fully separable state. For example, the state $\rho_{A_1A_2\ldots A_N} = |i\rangle\!\langle i|^{\otimes N}$ for $i = 0, 1, 2, \ldots, d-1$ reaches the fidelity bound of (112). Thus, in LOSR networks, the achievable fidelity with the GHZ state cannot exceed what one can obtain without distributing any bipartite entanglement at all.

The previous bounds for GHZ states given in Thm. 6 can also be used to derive fidelity bounds for other multipartite target states. The idea is to group the parties of a larger network into three sets and apply local unitaries within each group. If the target state can be transformed in this way into multiple copies of a three-partite GHZ state, then any LOSR preparation of

the original state would also imply an LOSR preparation of these GHZ states in an effective triangle network. Hence, the fidelity bounds from the tripartite case can be extended to larger multipartite states (see [59] for more details).

This can be applied in particular to cluster states. For an $m \times n$ cluster state, one can choose a tripartition that allows the extraction of $\lfloor mn/3 \rfloor$ copies of the three-qubit GHZ state. Combining this extraction with Thm. 6 gives the following bound.

Theorem 9. *The maximal fidelity with the $m \cdot n$-partite cluster state $\left|Cl_{m,n}\right\rangle$ in LOSR networks of nm parties is bounded by*

$$\max_{\rho_{A_1A_2\ldots A_{nm}} \in \mathcal{F}^{LOSR}} F(\rho_{A_1A_2\ldots A_{nm}}, \left|Cl_{m,n}\right\rangle\!\left\langle Cl_{m,n}\right|) \leq \frac{1}{2^{\frac{1}{2}\lfloor \frac{mn}{3} \rfloor}}, \tag{114}$$

where $\lfloor \cdots \rfloor$ indicates the floor function.

The proof can be found in [59].

Thus, the maximal fidelity with cluster states decreases exponentially with the number of qubits. This shows that the limitations of LOSR networks are not specific to GHZ states and also apply to other important graph states.

9.1.3 Non Fully Connected Networks

In the previous section, we focused on fully connected LOSR networks in which every pair of parties shares an entangled source state. We now turn to a more restrictive and practically relevant setting, where at least two parties are not directly connected by a bipartite source. This can happen, for instance, because a source is absent, or the network topology does not allow a direct connection between the two parties.

Theorem 10. *Let $\rho_{A_1A_2\ldots A_N}$ be a state that can be prepared in an LOSR network whose underlying graph is not complete. Then*

$$F(\rho_{A_1A_2\ldots A_N}, \left|GHZ_{N,d}\right\rangle\!\left\langle GHZ_{N,d}\right|) \leq \frac{1}{d}. \tag{115}$$

Proof. Let $\rho_{A_1A_2\ldots A_N}$ be a state that can be generated by an LOSR network that is not fully connected. Again w.l.o.g. we can drop the shared randomness (see proof of Thm. 6). Suppose that there is no source connecting A_i and A_j. After tracing out all systems except A_i and A_j, the state $\rho_{A_1A_2\ldots A_N}$ reduces to a product state, i.e.,

$$\mathrm{Tr}_{A_1A_2\ldots\hat{A}_i\ldots\hat{A}_j\ldots A_N}[\rho_{A_1A_2\ldots A_N}] = \rho_{A_i} \otimes \rho_{A_j}, \tag{116}$$

where $\hat{}$ denotes omission. The GHZ state reduces to the classically correlated state

$$\mathrm{Tr}_{A_1A_2\ldots\hat{A}_i\ldots\hat{A}_j\ldots A_N}\left[\left|\mathrm{GHZ}_{N,d}\right\rangle\!\left\langle\mathrm{GHZ}_{N,d}\right|\right] = \frac{1}{d}\sum_{k=0}^{d-1}|kk\rangle\langle kk|_{A_iA_j} \equiv \rho^{cc}_{A_iA_j} \tag{117}$$

Since fidelity is monotone under CPTP maps (see Prop. 5)

$$\begin{aligned} F\left(\rho_{A_1A_2\ldots A_N}, \left|\mathrm{GHZ}_{N,d}\right\rangle\!\left\langle\mathrm{GHZ}_{N,d}\right|\right) &\leq F\left(\rho_{A_i}\otimes\rho_{A_j}, \rho^{cc}_{A_iA_j}\right) \\ &\leq F\left(\Delta\left(\rho_{A_i}\otimes\rho_{A_j}\right), \Delta\left(\rho^{cc}_{A_iA_j}\right)\right) \\ &= F\left(\Delta\left(\rho_{A_i}\otimes\rho_{A_j}\right), \rho^{cc}_{A_iA_j}\right), \end{aligned} \tag{118}$$

where Δ is the dephasing channel defined by

$$\Delta(\rho) = \sum_{k,l=0}^{d-1}|kl\rangle\langle kl|\,\rho\,|kl\rangle\langle kl| \tag{119}$$

After dephasing, the state $\rho_{A_i}\otimes\rho_{A_j}$ remains a product state that is diagonal in the computational basis, i.e.,

$$\Delta(\rho_{A_i}\otimes\rho_{A_j}) = \left(\sum_{k=0}^{d-1}a_k\,|k\rangle\langle k|\right)\otimes\left(\sum_{l=0}^{d-1}b_l\,|l\rangle\langle l|\right), \tag{120}$$

where $a_k, b_l \geq 0$ for all k and l and $\sum_{k=0}^{d-1}a_k = \sum_{l=0}^{d-1}b_l = 1$. Hence,

$$\sqrt{\rho^{cc}_{A_iA_j}}\,\Delta\left(\rho_{A_i}\otimes\rho_{A_j}\right)\sqrt{\rho^{cc}_{A_iA_j}} = \frac{1}{d}\sum_{k=0}^{d-1}a_kb_k\,|kk\rangle\langle kk|_{A_iA_j} \tag{121}$$

Therefore, using the definition of the fidelity (see (32))

$$\begin{aligned} F\left(\Delta\left(\rho_{A_i}\otimes\rho_{A_j}\right), \rho^{cc}_{A_iA_j}\right) &= \frac{1}{d}\left(\sum_{k=0}^{d-1}\sqrt{a_kb_k}\right)^2 \\ &\leq \frac{1}{d}\left(\sum_{k=0}^{d-1}a_k\right)\left(\sum_{l=0}^{d-1}b_l\right) \\ &= \frac{1}{d} \end{aligned} \tag{122}$$

where in the second step we used the Cauchy-Schwarz inequality. □

Thm. 10 shows that the absence of even one bipartite source already rules out any advantage for GHZ-state preparation in such networks even in the tripartite case.

The same idea can also be used to derive upper bounds on other multipartite entangled states such as the W-state.

Theorem 11. *Let $\rho_{A_1A_2\ldots A_N}$ be a state which can be prepared in a not fully connected LOSR network. Then, for the N-qubit W state*

$$|W_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} |0\rangle^{\otimes(k-1)} |1\rangle |0\rangle^{\otimes(N-k)}, \tag{123}$$

one has

$$F(\rho_{A_1A_2\ldots A_N}, |W_N\rangle\langle W_N|) \leq \frac{N + \sqrt{N^2-4}}{2N}. \tag{124}$$

Proof. Let $\rho_{A_1A_2\ldots A_N}$ be generated by a not fully connected LOSR network. Thus, there exist two parties, say A_i and A_j, who do not share a bipartite source state. Again we focus on a fixed value of the shared randomness. In this case, the sources are independent and, since no source connects A_i and A_j, the reduced state on A_iA_j is a product state, i.e., $\rho_{A_iA_j} = \rho_{A_i} \otimes \rho_{A_j}$. The reduced state of $|W_N\rangle$ on A_iA_j is

$$\omega^W_{A_iA_j} \equiv \mathrm{Tr}_{A_1\ldots\hat{A}_i\ldots\hat{A}_j\ldots A_N}\left[|W_N\rangle\langle W_N|\right] = \frac{N-2}{N} |00\rangle\langle 00| + \frac{2}{N} \left|\phi_2^+\right\rangle\left\langle\phi_2^+\right|, \tag{125}$$

where $\hat{}$ denotes omission and $\left|\phi_2^+\right\rangle$ is the Bell state given in (19).

By monotonicity of the fidelity under the partial trace (see Prop. 5), we get

$$F(\rho_{A_1A_2\ldots A_N}, |W_N\rangle\langle W_N|) \leq F(\rho_{A_i} \otimes \rho_{A_j}, \omega^W_{A_iA_j}). \tag{126}$$

Applying the dephasing channel Δ in the computational basis (see Eq. (119)) and again using monotonicity of the fidelity gives

$$F(\rho_{A_i} \otimes \rho_{A_j}, \omega^W_{A_iA_j}) \leq F\left(\Delta(\rho_{A_i} \otimes \rho_{A_j}), \Delta(\omega^W_{A_iA_j})\right). \tag{127}$$

We have

$$\Delta(\omega^W_{A_iA_j}) = \frac{N-2}{N} |00\rangle\langle 00| + \frac{1}{N} |01\rangle\langle 01| + \frac{1}{N} |10\rangle\langle 10|. \tag{128}$$

Furthermore,

$$\Delta(\rho_{A_i}) = x\,|0\rangle\langle 0| + (1-x)\,|1\rangle\langle 1|\,, \qquad \Delta(\rho_{A_j}) = y\,|0\rangle\langle 0| + (1-y)\,|1\rangle\langle 1| \tag{129}$$

for some $x, y \in [0,1]$. Hence

$$\Delta(\rho_{A_i} \otimes \rho_{A_j}) = xy\,|00\rangle\langle 00| + x(1-y)\,|01\rangle\langle 01| + (1-x)y\,|10\rangle\langle 10| + (1-x)(1-y)\,|11\rangle\langle 11|\,. \tag{130}$$

Since both states are now diagonal in the same basis, the fidelity reduces to the classical fidelity, i.e.,

$$F\left(\Delta(\rho_{A_i} \otimes \rho_{A_j}), \Delta(\omega^W_{A_iA_j})\right) = \frac{1}{N}\left(\sqrt{N-2}\sqrt{xy} + \sqrt{x(1-y)} + \sqrt{(1-x)y}\right)^2. \tag{131}$$

To write the following expressions in a more compact form, we introduce

$$u \equiv \begin{pmatrix} \sqrt{x} \\ \sqrt{1-x} \end{pmatrix}, \qquad v \equiv \begin{pmatrix} \sqrt{y} \\ \sqrt{1-y} \end{pmatrix} \tag{132}$$

such that $\|u\| = \|v\| = 1$, and $\sqrt{N-2}\sqrt{xy} + \sqrt{x(1-y)} + \sqrt{(1-x)y} = u^T K v$, where

$$K = \begin{pmatrix} \sqrt{N-2} & 1 \\ 1 & 0 \end{pmatrix}. \tag{133}$$

Therefore,

$$u^T K v \leq \|K\|_\infty, \tag{134}$$

where $\|\cdot\|_\infty$ denotes the operator norm. Thus

$$F\left(\Delta(\rho_{A_i} \otimes \rho_{A_j}), \Delta(\omega^W_{A_iA_j})\right) \leq \frac{1}{N}\|K\|^2_\infty. \tag{135}$$

Since

$$KK^T = \begin{pmatrix} N-1 & \sqrt{N-2} \\ \sqrt{N-2} & 1 \end{pmatrix}, \tag{136}$$

we get

$$\|K\|_\infty^2 = \frac{N + \sqrt{N^2 - 4}}{2}, \tag{137}$$

which yields the desired result. □

In contrast to the GHZ state, the state $\mathrm{Tr}_{A_1 \ldots \hat{A}_i \ldots \hat{A}_j \ldots A_N} \left[|W_N\rangle\langle W_N| \right]$ does not reduce to a perfectly classically correlated state. Therefore, the resulting bound is weaker than the GHZ bound. Nevertheless, it still shows that a missing link imposes a nontrivial restriction. A not fully connected LOSR network cannot prepare the W state with high fidelity.

9.1.4 Multipartite Entanglement with LOCC

The main results of [59] show that LOSR networks are not sufficient to generate resourceful GME states that can be used for quantum tasks that require multipartite entanglement. In particular, Theorems 6, 8, and 10 establish strong no go results. They show that the capabilities of LOSR networks for preparing multipartite entangled states are rather limited. Therefore, one needs to investigate alternative network architectures that include classical communication. Because the use of classical communication generally entails time delays, the inclusion of quantum memories becomes necessary. A key next step is therefore to determine the minimal amount of classical communication required to prepare highly entangled states in network settings. Such an analysis would enable concrete estimates of memory lifetimes and waiting times [21–23]. In this section, we again consider quantum networks with bipartite source states. Here, however, we also allow for LOCC operations rather than only LOSR operations. Nevertheless, in this framework classical communication is treated as a resource, and the central question is the minimum amount of classical communication required to generate resourceful states such as the GHZ state. In this context, classical communication is quantified in bits, and the relevant question is to determine the minimum number of bits required to generate a GHZ state.

We start with the simplest nontrivial example, namely the tripartite LOSR network. In the following, we introduce a protocol that shows that one bit of classical communication is sufficient to generate the state $\left|\mathrm{GHZ}_{3,2}\right\rangle$ [82, 83].

Step 1: Initial state: Consider three parties Alice (A), Bob (B), and Charlie (C). Alice holds two qubits, denoted A_1 and A_2. Suppose that, initially, the network contains two Bell

pairs,

$$\left|\phi_2^+\right\rangle_{A_1B} \otimes \left|\phi_2^+\right\rangle_{A_2C}, \tag{138}$$

where $\left|\phi_2^+\right\rangle$ is the Bell state given in Eq. (19). Using the qubit ordering (A_1, B, A_2, C), we expand

$$\begin{aligned}\left|\phi_2^+\right\rangle_{A_1B} \otimes \left|\phi_2^+\right\rangle_{A_2C} &= \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)_{A_1B} \otimes \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)_{A_2C} \\ &= \frac{1}{2}\Big(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\Big).\end{aligned} \tag{139}$$

Step 2: Alice applies a local CNOT: Alice applies a CNOT gate with control qubit A_1 and target qubit A_2.

This transforms the state (138) into

$$\begin{aligned}\mathrm{CNOT}_{A_1,A_2}\left|\phi_2^+\right\rangle_{A_1B} \otimes \left|\phi_2^+\right\rangle_{A_2C} &= \frac{1}{2}\Big(|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle\Big) \\ &= \frac{1}{2}\Big[(|000\rangle + |111\rangle)_{A_1BC}\,|0\rangle_{A_2} + (|001\rangle + |110\rangle)_{A_1BC}\,|1\rangle_{A_2}\Big].\end{aligned} \tag{140}$$

Step 3: Alice measures A_2 in the computational basis:
Alice measures qubit A_2 in the Z-basis $\{|0\rangle, |1\rangle\}$.

- If the measurement outcome is 0, then the post-measurement state of (A_1, B, C) is

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \left|\mathrm{GHZ}_{3,2}\right\rangle. \tag{141}$$

- If the measurement outcome is 1, then the post-measurement state is

$$\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle). \tag{142}$$

Step 4: One-bit communication and correction:
Alice sends her one-bit measurement outcome to Charlie.

- If the outcome is 0, Charlie applies the identity operation I.
- If the outcome is 1, Charlie applies the Pauli X operator.

Thus, one bit of classical communication is sufficient to generate a GHZ state from two Bell pairs. This is optimal since the GHZ state cannot be prepared in LOSR networks without classical communication (see, e.g., Thm. 6). The same idea can be extended to more parties as follows:

Theorem 12. *In an LOSR network with N parties* $(N-2)$ *bits of classical communication are necessary and sufficient to generate the GHZ state* $\left|GHZ_{N,2}\right\rangle$.

We first prove sufficiency. We can argue by induction. For $N = 3$, the claim follows from the protocol above. Suppose the N parties can generate an N partite GHZ state $\left|\mathrm{GHZ}_{N,2}\right\rangle$ using at most $N-2$ bits of classical communication. Now introduce one additional party, and suppose one of the existing parties, say Alice, shares a Bell pair with that new party. Alice then performs the same steps as in the three partite construction: she applies a local CNOT between her GHZ qubit and her half of the Bell pair, measures the Bell-pair qubit in the computational basis, and sends the one bit measurement outcome to the new party. Depending on that bit, the new party either does nothing or applies a Pauli X correction. After this correction, the state shared by all $N+1$ parties is the $(N+1)$ partite GHZ state $\left|\mathrm{GHZ}_{N+1,2}\right\rangle$. It remains to prove necessity: Suppose, for contradiction, that at most $N-3$ bits are sufficient to prepare the state $\left|\mathrm{GHZ}_{N,2}\right\rangle$. In this scenario, the N parties can be divided into three groups that do not communicate classically with each other. We now merge each group into one "supernode". This can only make the protocol more powerful, because parties inside the same supernode are now allowed to perform arbitrary joint operations. In this way, the scenario reduces to a tripartite LOSR network in which the parties generate the three qubit GHZ state. This, however, is not possible (see, e.g., Thm. 6).

9.2 QKD in LOSR Networks

The results of the previous sections show that LOSR networks are highly restricted in their ability to prepare resourceful GME states with high fidelity. Nevertheless, some GME states can be prepared in a nontrivial way. In particular, in the tripartite case, the set of LOSR states is strictly larger than the set of biseparable states. In fact, in [59], we show that LOSR networks can produce states that are genuinely multipartite entangled and quantitatively close to the GHZ state with a fidelity of

$$\max_{\rho_{ABC}\in\mathcal{F}^{LOSR}} F\left(\rho_{ABC}, \left|\mathrm{GHZ}_{3,2}\right\rangle\!\left\langle\mathrm{GHZ}_{3,2}\right|\right) > 0.548. \tag{143}$$

This raises the question whether such approximate GHZ type states are already sufficient to provide an advantage in concrete multipartite quantum information tasks. A particularly natural task to study in this context is conference key agreement (see Sec. 6).

In particular, the multipartite BB84 protocol is a suitable benchmark for the operational usefulness of those states because the ideal resource state for this protocol is precisely the multipartite GHZ state (see Sec. 6.3). In this section, we recall the main results of [65] and derive upper bounds on the conference key rate achievable from LOSR-network states.

In the following, we consider the multipartite BB84 key rate (see Eq. (78)) under the restriction that the shared input state is a LOSR state. An upper bound can be derived by using the inflation technique described in Sec. 5.3.

Lemma 1. *Let ρ_{ABC} be a state that can be prepared in a network with bipartite source states and local operations, i.e., a state of the form in Eq.* (53)*. Then*

$$\mathrm{Tr}[\rho_{AB} Z_A \otimes Z_B] + \mathrm{Tr}[\rho_{AC} Z_A \otimes Z_C] \leq 1 + \mathrm{Tr}[\rho_B Z_B]\,\mathrm{Tr}[\rho_C Z_C]. \tag{144}$$

Proof. First, note that $|0\rangle\langle 0| = \frac{1}{2}(\mathbb{1} + Z)$ and $|1\rangle\langle 1| = \frac{1}{2}(\mathbb{1} - Z)$. Therefore, for any state $\tilde{\rho}_{ABC}$, we have

$$0 \leq \mathrm{Tr}[\tilde{\rho}\,|100\rangle\langle 100|] + \mathrm{Tr}[\tilde{\rho}\,|011\rangle\langle 011|] \tag{145}$$

$$= \frac{1}{4}\left(1 - \mathrm{Tr}[\tilde{\rho}_{ABC} Z_A \otimes Z_B] - \mathrm{Tr}[\tilde{\rho}_{ABC} Z_A \otimes Z_C] + \mathrm{Tr}[\tilde{\rho}_{ABC} Z_B \otimes Z_C]\right) \tag{146}$$

That is, for all states $\tilde{\rho}_{ABC}$

$$\mathrm{Tr}[\tilde{\rho}_{AB} Z_A \otimes Z_B] + \mathrm{Tr}[\tilde{\rho}_{AC} Z_A \otimes Z_C] \leq 1 + \mathrm{Tr}[\tilde{\rho}_{BC} Z_B \otimes Z_C] \tag{147}$$

is satisfied. Now, consider the following cut inflated state obtained by replacing the source $\sigma_{B_2C_2}$ by its marginals σ_{B_2} and σ_{C_2} (see Sec. 5.3), i.e.,

$$\tau_{ABC} = \mathcal{E}_{A_1A_2\to A} \otimes \mathcal{E}_{B_1B_2\to B} \otimes \mathcal{E}_{C_1C_2\to C}\left[\sigma_{A_1B_1} \otimes \sigma_{A_2C_1} \otimes \sigma_{B_2} \otimes \sigma_{C_2}\right], \tag{148}$$

where

$$\sigma_{B_2} = \mathrm{Tr}_{C_2}[\sigma_{B_2C_2}], \qquad \sigma_{C_2} = \mathrm{Tr}_{B_2}[\sigma_{B_2C_2}]. \tag{149}$$

Because the node B and the node C do not share a source state in the cut inflation network, the

inequality (147) reduces to

$$\mathrm{Tr}[\tau_{AB} Z_A \otimes Z_B] + \mathrm{Tr}[\tau_{AC} Z_A \otimes Z_C] \leq 1 + \mathrm{Tr}[\tau_B Z_B]\,\mathrm{Tr}[\tau_C Z_C]. \tag{150}$$

We can do the marginal comparison to the state that can be prepared in the triangle network, i.e. with the state given by Eq. (53):

$$\rho_{AB} = \tau_{AB} \qquad \rho_{AC} = \tau_{AC} \tag{151}$$

$$\rho_B = \tau_B \qquad \rho_C = \tau_C. \tag{152}$$

Thus, we can replace each term in inequality (150) in terms of the state ρ_{ABC} s.t.

$$\mathrm{Tr}[\rho_{AB} Z_A \otimes Z_B] + \mathrm{Tr}[\rho_{AC} Z_A \otimes Z_C] \leq 1 + \mathrm{Tr}[\rho_B Z_B]\,\mathrm{Tr}[\rho_C Z_C] \tag{153}$$

□

Note that Lemma 1 does not hold for LOSR states in general. For instance, the state

$$\rho_{ABC} = \frac{1}{2}\left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) \tag{154}$$

is a LOSR state, i.e., $\rho_{ABC} \in \mathcal{F}^{LOSR}$, since it is fully separable but it does not satisfy the inequality (144). Although Lemma 1 is not directly applicable to all LOSR states, it can still be used as a technical ingredient to derive a constraint that holds for the set of LOSR states itself.

Lemma 2. *Let $\rho_{ABC} \in \mathcal{F}^{LOSR}$, then*

$$\mathrm{Tr}[X_A \otimes X_B \otimes X_C \rho_{ABC}]^2 + \mathrm{Tr}[Z_A \otimes Z_B \rho_{AB}] + \mathrm{Tr}[Z_A \otimes Z_C \rho_{AC}] \leq 2. \tag{155}$$

Proof. Suppose $\tilde{\rho}_{ABC}$ is a state that can be prepared in a network with bipartite source states and local operations, i.e., a state of the form of Eq. (53). Note that for any state ρ the sum of the squares of expectation values of pairwise anticommuting observables is bounded by 1, i.e. if $\{A_i\}_i$ is a set of pairwise anticommuting observables with eigenvalues ± 1, then $\sum_i \mathrm{Tr}[\rho A_i]^2 \leq 1$. In particular, we have

$$\begin{aligned} \mathrm{Tr}[X_A \otimes X_B \otimes X_C \tilde{\rho}_{ABC}]^2 + \mathrm{Tr}[Z_B \tilde{\rho}_B]^2 &\leq 1 \\ \mathrm{Tr}[X_A \otimes X_B \otimes X_C \tilde{\rho}_{ABC}]^2 + \mathrm{Tr}[Z_C \tilde{\rho}_C]^2 &\leq 1 \end{aligned} \tag{156}$$

That is

$$\left|\mathrm{Tr}[Z_B\tilde{\rho}_B]\right|\left|\mathrm{Tr}[Z_C\tilde{\rho}_C]\right| \leq 1 - \mathrm{Tr}[X_A \otimes X_B \otimes X_C\tilde{\rho}_{ABC}]^2. \tag{157}$$

Together with Lemma 1 this yields

$$\mathrm{Tr}[X_A \otimes X_B \otimes X_C\tilde{\rho}_{ABC}]^2 + \mathrm{Tr}[Z_A \otimes Z_B\tilde{\rho}_{AB}] + \mathrm{Tr}[Z_A \otimes Z_C\tilde{\rho}_{AC}] \leq 2 \tag{158}$$

Since the left hand side of the inequality (158) is a convex function in $\tilde{\rho}_{ABC}$, the inequality (158) also holds for convex combinations of states that can be prepared in a network with bipartite source states and local operations. Therefore, the inequality (158) also holds for any state that can be prepared in a LOSR network. □

Theorem 13. *For tripartite qubit states prepared in a tripartite LOSR network, the maximal multipartite BB84 key rate (see Eq.* (78)*) satisfies*

$$\max_{\rho_{ABC}\in\mathcal{F}^{LOSR}} r_{\mathrm{BB84}}(\rho_{ABC}) = \max_{\rho_{ABC}\in\mathcal{F}^{BS}} r_{\mathrm{BB84}}(\rho_{ABC}) = 1 - h\left(\frac{1}{4}\right) \approx 0.188. \tag{159}$$

Proof. Let $\rho_{ABC} \in \mathcal{F}^{LOSR}$ be a state that can be prepared in a LOSR network. From Lemma 2 it follows that

$$\mathrm{Tr}[X_A \otimes X_B \otimes X_C\rho_{ABC}]^2 + 2\min\left\{\mathrm{Tr}[Z_A \otimes Z_B\rho_{AB}], \mathrm{Tr}[Z_A \otimes Z_C\rho_{AC}]\right\} \leq 2. \tag{160}$$

Now let $\min\left\{\mathrm{Tr}[Z_A \otimes Z_B\rho_{AB}], \mathrm{Tr}[Z_A \otimes Z_C\rho_{AC}]\right\} = \frac{1}{2} + \varepsilon$ for some $\varepsilon \geq 0$. [6] Then

$$|\mathrm{Tr}[X_A \otimes X_B \otimes X_C\rho_{ABC}]| \leq \sqrt{1-2\varepsilon}. \tag{161}$$

Inserting inequality (161) into the definition of the asymptotic key rate (78), we obtain an upper bound for the asymptotic key rate:

$$r_{\mathrm{BB84}} \leq \max_{0\leq\varepsilon\leq\frac{1}{2}} \left\{1 - h\left(\frac{1-\sqrt{1-2\varepsilon}}{2}\right) - h\left(\frac{\frac{1}{2}-\varepsilon}{2}\right)\right\} \tag{162}$$

$$= 1 - h\left(\frac{1}{4}\right) \approx 0.188 \tag{163}$$

[6] If this minimum is at most $1/2$, then the bit-error contribution is already at least $h(1/4)$, so the desired upper bound follows immediately. Hence only the case where the minimum is larger than $1/2$ needs to be optimized.

The tightness can be seen, for instance, by choosing the following biseparable state

$$\rho = \frac{1}{2}\left(\left|\phi^+\right\rangle\left\langle\phi^+\right|_{AB} \otimes |+\rangle\langle+|_C + \left|\phi^+\right\rangle\left\langle\phi^+\right|_{AC} \otimes |+\rangle\langle+|_B\right) \tag{164}$$

which gives rise to a key rate of $1 - h\left(\frac{1}{4}\right)$ (see [84]). □

Thm. 13 has an interesting conceptual implication. At first glance, the result is somewhat surprising. Although LOSR networks can generate tripartite states that are genuinely multipartite entangled and even approximate the GHZ state with nontrivial fidelity (see Eq. (143)), this does not lead to any advantage for conference key agreement in the multipartite BB84 protocol. Indeed, the maximal achievable key rate in the LOSR setting coincides exactly with the maximal key rate attainable by biseparable states (see Eq. (164)). Hence, the genuinely multipartite entangled states that can be prepared in a LOSR network do not give an operational advantage in this setting.

The restriction to LOSR networks also leads to bounds beyond the specific multipartite BB84 protocol. In particular, one can consider more general conference key agreement protocols and ask about the limitations in LOSR networks.

Theorem 14. *Let $\rho_{A_1B_1B_2\ldots B_{N-1}}$ be a LOSR state. Then the multipartite Devetak-Winter key rate for N participants* (75) *is upper bounded by*

$$r_{DW}^{CKA} \leq \frac{H(A_1)}{N-1}, \tag{165}$$

where $H(A_1)$ is the von Neumann entropy of the reduced state of A_1 (see Eq. (68)*). The bound can be reached by a bipartite QKD strategy.*

The proof can be found in [65]. Here, a bipartite QKD strategy means that the distinguished party A_1 establishes independent secret keys with each other participant by standard two-party QKD. These pairwise keys are then combined by public classical communication into a common conference key shared by all N participants. Thus, in this setting, genuinely multipartite key generation strategies do not provide an advantage over pairwise QKD for the multipartite Devetak-Winter rate. These results suggest that the absence of an advantage in the BB84 protocol is not only a feature of this particular protocol. Instead, it reflects a more general limitation of LOSR networks (see [65] for more details).

9.3 Completely Absolute Separable States

Absolute separability is usually defined by requiring that a bipartite state remains separable under arbitrary global unitary transformations (see Sec. 7). Equivalently, and more operationally, a state is absolutely separable if no deterministic unital channel can transform it into an entangled state (see below or [85]).

This deterministic picture changes once one allows postselection. Some absolutely separable states can be mapped to entangled states by stochastic unital maps followed by postselection. Consequently, absolute separability does not in general exclude entanglement extraction with nonzero probability [77]. This observation motivates a stronger notion, namely completely absolute separability. We call a state completely absolute separable if it remains separable after every probabilistic unital transformation and postselection. In this section, we present the main results of [77] in which we characterize this class of states.

A *unital channel* Λ is a CPTP map satisfying $\Lambda(\mathbb{1}) = \mathbb{1}$. Unital channels have an operational meaning in the resource theory of purity. Purity quantifies the deviation of a state from the maximally mixed state, and unital channels are precisely the resource non-generating operations for this choice of free state [14, 86].

Proposition 1. *A state ρ_{AB} is absolute separable if and only if $\Lambda(\rho_{AB})$ is separable for all unital channels Λ.*

Proof. First, assume that ρ_{AB} remains separable under all unital channels, i.e., $\Lambda(\rho_{AB}) \in S$ for all unital channels Λ. Then ρ_{AB} remains separable also under all unitary channels Λ_U as they form a subclass of unital channels: $\Lambda_U(\rho_{AB}) = U\rho_{AB}U^\dagger$ and $\Lambda_U(\mathbb{1}) = U\mathbb{1}U^\dagger = \mathbb{1}$. Now assume that ρ_{AB} is absolute separable. Note that a unital operation Λ cannot make a state less mixed, i.e., $\Lambda(\rho) \prec \rho$ (see e.g. [87], [88]). Moreover, if $\sigma \prec \rho$, then there exists an index set I, a probability distribution $\{p_i\}_{i\in I}$ and a set of unitaries $\{U_i\}_{i\in I}$ such that

$$\sigma = \sum_{i\in I} p_i U_i \rho_{AB} U_i^\dagger \tag{166}$$

(see [87]). Applying this to $\sigma = \Lambda(\rho_{AB})$ gives

$$\Lambda(\rho_{AB}) = \sum_{i\in I} p_i U_i \rho_{AB} U_i^\dagger . \tag{167}$$

Note that $U_i\rho_{AB}U_i^\dagger$ is absolute separable for all $i \in I$. This, together with the fact that the set of absolute separable states is convex shows that $\Lambda(\rho_{AB})$ is absolute separable as well. □

The set of absolute separable states is therefore characterized by bipartite states that remain separable under all deterministic unital channels. We now extend this setting by allowing probabilistic unital operations.

Although absolute separable states cannot be transformed into entangled states by deterministic unital channels, some of them can be transformed into entangled states with nonzero probability by a probabilistic unital operation (see [77] for an example). We therefore define a subset of AS which also remains separable under all probabilistic unital channels:

A *probabilistic unital operation* $\tilde{\Lambda}$ is a completely positive, trace-nonincreasing map satisfying

$$\tilde{\Lambda}(\mathbb{1}) = c\mathbb{1} \tag{168}$$

for some $c \in (0, 1]$.

A state ρ_{AB} is called *completely absolute separable* if and only if

$$\frac{\tilde{\Lambda}(\rho_{AB})}{\mathrm{Tr}\big[\tilde{\Lambda}(\rho_{AB})\big]} \in SEP \tag{169}$$

for all probabilistic unital channels $\tilde{\Lambda}$. The set of completely absolute separable states is denoted by CAS.

Theorem 15. *Let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state with $d_A \leq d_B$. Then the following statements are equivalent:*

(i) ρ_{AB} *is completely absolute separable.*

(ii) $\rho_{AB} \otimes \frac{\mathbb{1}_{B'}}{d_{B'}} \in D(\mathcal{H}_A \otimes \mathcal{H}_{BB'})$ *is absolute separable for all* $d_{B'} \in \mathbb{N}$.

(iii) $\rho_{AB} \otimes \frac{\mathbb{1}_{B'}}{d_{B'}} \in D(\mathcal{H}_A \otimes \mathcal{H}_{BB'})$ *is absolute PPT for all* $d_{B'} \in \mathbb{N}$.

(iv) $\frac{\lambda_1}{\lambda_{d_A d_B}} \leq \frac{d_A+1}{d_A-1}$.

The proof can be found in [77]. The theorem has two important consequences. First, Thm. 15 (iv) shows that the set of completely absolute separable states is completely characterized by the largest and smallest eigenvalue of the state. Second, Thm. 15 (ii) shows that completely absolute separable states remain absolute separable after tensoring with arbitrary maximally mixed ancillas.

This raises the question whether absolute separability itself is stable under tensor products. The answer is negative. To see this, consider the absolutely separable state ρ_{AB} with spectrum

given in (85) together with the maximally mixed state $\tau_{AB} = \frac{\mathbb{1}_k}{k}$ of arbitrary dimension k. The state $\rho_{AB} \otimes \tau_{AB}$ has the following spectrum

$$\mathrm{Spec}(\rho_{AB} \otimes \tau_{AB}) = \left(\frac{1}{k(d_A d_B - 1)}, \frac{1}{k(d_A d_B - 1)}, \ldots, \frac{1}{k(d_A d_B - 1)}, \underbrace{0, 0, \ldots, 0}_{k\text{-times}} \right) \tag{170}$$

which cannot be absolute separable as it violates inequality (82).

In fact, we can show that any absolute separable state that is different from the maximally mixed state can be activated by a finite number of copies.

Proposition 2. *Let ρ_{AB} be an absolute separable state, which is not maximally mixed, i.e., $\rho_{AB} \in AS \setminus \{\frac{\mathbb{1}}{d_A d_B}\}$. Then there exists a finite number $n \in \mathbb{N}$ s.t. $\rho_{AB}^{\otimes n} \notin AS$.*

Proof. We will prove the result for absolute PPT states as they are a superset of absolute separable states. First, note that if a state ρ_{AB} is absolute PPT then its eigenvalues have to obey the inequality (82). For the spectrum of $n \geq 2$ copies of the state ρ_{AB}, we get

$$\mathrm{Spec}(\rho_{AB}^{\otimes n}) = (\lambda_1^n, \ldots, \lambda_{d_A d_B}^{n-1} \lambda_{d_A d_B - 1}, \lambda_{d_A d_B}^{n-1} \lambda_{d_A d_B - 1}, \lambda_{d_A d_B}^n) \tag{171}$$

In order for $\rho_{AB}^{\otimes n}$ to be absolute PPT the eigenvalues of $\rho_{AB}^{\otimes n}$ have to satisfy

$$\begin{aligned} \lambda_1^n &\leq \lambda_{d_A d_B}^{n-1} \lambda_{d_A d_B - 1} + 2\sqrt{\lambda_{d_A d_B}^{2n-1} \lambda_{d_A d_B - 1}} \\ &= \lambda_{d_A d_B}^n \left(\frac{\lambda_{d_A d_B - 1}}{\lambda_{d_A d_B}} + 2 \left(\frac{\lambda_{d_A d_B - 1}}{\lambda_{d_A d_B}} \right)^{\frac{1}{2}} \right) \end{aligned} \tag{172}$$

Thus, if we choose $n > \frac{\ln\left(\left(\frac{\lambda_{d_A d_B - 1}}{\lambda_{d_A d_B}} + 2\left(\frac{\lambda_{d_A d_B - 1}}{\lambda_{d_A d_B}}\right)^{\frac{1}{2}}\right)\right)}{\ln\left(\frac{\lambda_1}{\lambda_{d_A d_B}}\right)}$ the state $\rho_{AB}^{\otimes n}$ violates the inequality (172) and is therefore not absolute PPT. Note that if ρ_{AB} is not of full rank, i.e., $\lambda_{d_A d_B} = 0$, then already two copies of the state ρ_{AB} violate the inequality (82). □

Therefore, demanding closure under arbitrary tensor products is too strong, since no nontrivial subset of absolute separable states can exist, which is closed under the tensor product. This provides a second motivation for considering completely absolutely separable states. Instead of requiring stability under the tensor product in general, we only consider stability under tensoring with some "free" ancillas. In the resource theory of purity, the natural free ancillas are maximally mixed states, since they carry no purity resource. Thm. 15 (ii) shows that the

states which remain absolute separable even under attaching the maximally mixed states are exactly the completely absolute separable states.

Since CAS is a subset of AS, it is natural to compare the geometry of these two sets. The next proposition shows that, for equal local dimensions, the boundaries of AS and CAS have only a very small intersection. In fact, their common boundary is characterized by a single spectrum.

Proposition 3. *Let* $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$. *Then*

$$\partial AS \cap \partial CAS = \left\{ \rho_{AB} \mid Spec(\rho_{AB}) = Spec\left(\frac{\mathbb{1} - (|\phi^+\rangle\langle\phi^+|)^{T_B}}{d^2 - 1} \right) \right\} \tag{173}$$

Proof. First, we show that in the case $d_A = d_B = d$ any state ρ_{AB} which is completely absolute separable lies within the set of states defined by Thm. 4. Note that

$$(\lambda_1 - \lambda_i)(\lambda_i - \lambda_{d^2}) \geq 0 \tag{174}$$

for all $i = 1, 2, \ldots, d^2$. Summing (174) over i yields

$$\begin{aligned} 0 &\leq \sum_{i=1}^{d^2} (\lambda_1 - \lambda_i)(\lambda_i - \lambda_{d^2}) \\ &= -\sum_{i=1}^{d^2} \lambda_i^2 + \sum_{i=1}^{d^2} \lambda_i \lambda_1 + \sum_{i=1}^{d^2} \lambda_i \lambda_{d^2} - \sum_{i=1}^{d^2} \lambda_1 \lambda_{d^2} \\ &= -\operatorname{Tr}\left[\rho_{AB}^2\right] + \lambda_1 + \lambda_{d^2} - d^2 \lambda_1 \lambda_{d^2} \end{aligned} \tag{175}$$

Since ρ_{AB} is completely absolutely separable, it satisfies the eigenvalue inequality (iv), i.e., $\frac{\lambda_1}{\lambda_{d^2}} \leq \frac{d+1}{d-1}$. Inserting this into (175) gives

$$\operatorname{Tr}\left[\rho_{AB}^2\right] \leq \left(\frac{d+1}{d-1} + 1 \right) \lambda_{d^2} - d^2 \frac{d+1}{d-1} \lambda_{d^2}^2 \tag{176}$$

The right hand side of (176) is a quadratic concave function in λ_{d^2}, where its maximum is obtained by

$$\lambda_{d^2} = \frac{1}{d(d+1)} \tag{177}$$

(176) together with (177) gives

$$\mathrm{Tr}\big[\rho_{AB}^2\big] \leq \frac{1}{d^2-1}. \tag{178}$$

Hence, for equal local dimensions, the set of completely absolute separable states is a subset of the set of states defined by Thm. 4. Second, we assume that the state ρ_{AB} is on the boundary of CAS, i.e., $\frac{\lambda_1}{\lambda_{d^2}} = \frac{d+1}{d-1}$ and on the boundary of the set of states defined by Thm. 4, i.e., $\mathrm{Tr}\big[\rho_{AB}^2\big] = \frac{1}{d^2-1}$. We already showed that for a state that is completely absolute separable, the minimal eigenvalue λ_{d^2} has to be given by (177) in order to be on the boundary of the set of states given by Thm. 4. Since we demand that the state is also on the boundary of the set of completely absolute separable states, i.e., $\rho_{AB} \in \partial CAS$, the maximal eigenvalue has to be $\lambda_1 = \frac{1}{d(d-1)}$. Therefore, it follows from (175) that

$$\sum_{i=1}^{d^2} (\lambda_1 - \lambda_i)(\lambda_i - \lambda_{d^2}) = 0 \tag{179}$$

which implies that $(\lambda_1 - \lambda_i)(\lambda_i - \lambda_{d^2}) = 0$ for all $i = 1, 2, \ldots, d^2$ as each term in the sum cannot be negative. Therefore, for each i either $\lambda_i = \lambda_1$ or $\lambda_i = \lambda_{d^2}$. This uniquely determines the spectrum and is given by

$$\mathrm{Spec}\,(\rho_{AB}) = \left(\frac{1}{d(d-1)}, \frac{1}{d(d-1)}, \ldots, \frac{1}{d(d-1)}, \frac{1}{d(d+1)}, \frac{1}{d(d+1)}, \ldots, \frac{1}{d(d+1)}\right) \tag{180}$$

which is exactly the spectrum of the state $\rho_{AB} = \frac{\mathbb{1} - (|\phi^+\rangle\langle\phi^+|)^{T_B}}{d^2-1}$.

□

As a final remark, note that the eigenvalue property given by Thm. 15 (iv) also serves as a novel sufficient condition of separability. In particular, for quantum systems with unequal local dimensions it can detect separable states that remain undetected by other sufficient separability conditions such as Thm. 4 and Thm. 5 that only depend on the total dimension of the system. Examples of such states can be found in [77].

9.4 Additivity of the Relative Entropy of Magic

In Sec. 8.4, we discussed a sufficient condition under which the relative entropy of magic is additive for tensor products of single qubit states. In this section, we recall the results of [76] in

which we discuss to what extent this condition is also necessary. To state the result, we first identify a special class of stabilizer states. For a single qubit, the stabilizer set has the geometry of an octahedron inside the Bloch ball. The relevant states are those that lie on one of the facets of this octahedron, rather than on an edge or vertex. We call such states facet states. To make this precise, let σ be a single qubit stabilizer state. We call a stabilizer state a *facet state* if it is on the boundary of the stabilizer set, i.e., $\sigma \in \partial\mathcal{F}^{\mathrm{STAB}}(\mathcal{H})$ and has no zero Bloch coordinate. More formally, the set of facet states is defined as

$$F_{\mathrm{facet}}(\mathcal{H}) := \left\{\sigma \in \mathcal{F}^{\mathrm{STAB}}(\mathcal{H}) \,\middle|\, \sigma = \frac{1}{2}\left(\mathbb{1} + \sum_{i=1}^{3} r_i\sigma_i\right),\ |r_1| + |r_2| + |r_3| = 1,\ r_i \neq 0\ \forall i\right\}, \tag{181}$$

where σ_i with $i = 1, 2, 3$ are the Pauli operators (see Eq. (2)). With this notation, the following theorem gives a sufficient condition for the nonadditivity of the relative entropy of magic.

Theorem 16. *Let $\rho^{(i)} \in D(\mathcal{H}_i) \setminus \mathcal{F}^{STAB}(\mathcal{H}_i)$ with $i = 1, \ldots, n$ be single qubit magic states and $\sigma^{(i)} \in \mathcal{F}^{STAB}(\mathcal{H}_i)$ their closest stabilizer states. The relative entropy of magic of their tensor product $\rho = \bigotimes_{i=1}^{n} \rho^{(i)}$ cannot be additive if both of the following conditions hold*

1. $\left[\rho^{(i)}, \sigma^{(i)}\right] \neq 0$ *for at least two $i \in \{1, \ldots, n\}$,*
2. *at least one $\sigma^{(i)}$ with $\left[\rho^{(i)}, \sigma^{(i)}\right] \neq 0$ is a facet state, i.e., $\sigma^{(i)} \in F_{\mathrm{facet}}(\mathcal{H}_i)$.*

The proof can be found in [76]. The idea of the proof is to use an inverse form of the closest stabilizer state problem. Instead of starting from a magic state and minimizing over all stabilizer states, one starts from a boundary stabilizer state together with a supporting hyperplane and characterizes all magic states to which this stabilizer state is closest. For single qubit states, this inverse problem can be written explicitly in terms of Bloch vectors. This gives a closed form description of the magic states associated with a given closest stabilizer state.

Using this characterization, one can also see when a magic state commutes with its closest stabilizer state. In the single qubit picture, commutativity corresponds to the case in which the closest stabilizer state and the associated supporting hyperplane are aligned in a symmetric way. This happens, for example, at the centers of facets or edges of the stabilizer octahedron. Away from these symmetric points, the closest stabilizer state and the magic state generally do not commute.

We then assume, for contradiction, that the relative entropy of magic is additive for the tensor product state. Under this assumption, the tensor product of the individual closest stabilizer states would also have to be a closest stabilizer state of the full tensor product. The inverse

characterization then forces a particular operator to define a supporting hyperplane of the multi qubit stabilizer set. The central step is then to show that this operator cannot be a valid supporting hyperplane (see [76] for full proof and more details).

The theorem therefore shows that, apart from remaining edge cases, the sufficient commutativity condition given in [75] is close to being necessary. A further novelty of the theorem is that it provides a continuous family of nonadditive examples, rather than only isolated counterexamples known so far.

10 Outlook

In this thesis, we investigated limitations on the generation and use of multipartite entanglement in quantum networks with bipartite source states, local operations, and shared randomness.

Although bipartite sources can generate genuinely multipartite entangled states, the fidelity bounds derived in this thesis show that they are limited in their ability to prepare specific multipartite target states. For GHZ states, those networks provide at most a limited advantage in the tripartite case. For four or more parties, their maximal fidelity does not exceed that attainable by fully separable states. More generally, connected graph states cannot be prepared with high fidelity in such networks. For cluster states, the corresponding fidelity bounds even decrease exponentially with the number of qubits. This suggests that future work should quantify how much additional resource, such as classical communication, quantum memory or direct multipartite sources, is required to prepare a given target state.

A similar distinction between multipartite entanglement and its operational usefulness appears in conference key agreement. For the key rates in this network setting, the optimal strategy is to first distill pairwise keys and then merge them into a common conference key. An important direction is therefore to identify network assumptions under which genuinely multipartite strategies outperform such pairwise methods.

Mixed bipartite states provide another setting in which entanglement generation can be fundamentally restricted. In this thesis, we showed that completely absolute separability can be characterized by a simple spectral condition. These are precisely the states that remain separable under all probabilistic unital transformations, even when postselection is allowed.

A similar structural viewpoint appears in the final part of the thesis, where the relevant free set is no longer the set of separable states but the set of stabilizer states. We derived a sufficient condition for the non-additivity of the relative entropy of magic for tensor products of single-qubit magic states. In this result, non-additivity is linked to the failure of commutativity

between the individual magic states and their closest stabilizer states, together with the condition that at least one of the relevant closest stabilizer states lies on a facet of the single-qubit stabilizer polytope. A further direction is to ask whether comparable geometric criteria can be formulated for correlated multi-qubit states.

Bibliography

[1] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. Quantum conference key agreement: A review. *Adv. Quantum Technol.*, 3(11):2000025, 2020. Link: https://doi.org/10.1002/qute.202000025.

[2] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.*, 19(9):093012, 2017. Link: https://doi.org/10.1088/1367-2630/aa8487.

[3] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen. Optimal frequency measurements with maximally correlated states. *Phys. Rev. A*, 54:R4649–R4652, 1996. Link: https://doi.org/10.1103/PhysRevA.54.R4649.

[4] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001. Link: https://doi.org/10.1103/PhysRevLett.86.5188.

[5] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, 2003. Link: https://doi.org/10.1103/PhysRevA.68.022312.

[6] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. Link: https://doi.org/10.1007/978-94-017-0849-4_10.

[7] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, 2000. Link: https://doi.org/10.1103/PhysRevA.62.062314.

[8] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69(6):062311, 2004. Link: https://doi.org/10.1103/PhysRevA.69.062311.

[9] K. Chen and H.-K. Lo. Multi-partite quantum cryptographic protocols with noisy GHZ states. *Quantum Inf. Comput.*, 7(8):689–715, 2007. Link: https://doi.org/10.26421/QIC7.8-1.

[10] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications. In G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti, editors, *Quantum Computers, Algorithms and Chaos*, volume 162 of *Proceedings of the International School of Physics "Enrico Fermi"*, pages 115–218. IOS Press, Amsterdam, 2006. Link: https://doi.org/10.3254/1-58603-660-2-115.

[11] W. Dür, J. I. Cirac, and R. Tarrach. Separability and distillability of multiparticle quantum systems. *Phys. Rev. Lett.*, 83(17):3562–3565, 1999. Link: https://doi.org/10.1103/PhysRevLett.83.3562.

[12] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. *Phys. Rev. Lett.*, 87(4):040401, 2001. Link: https://doi.org/10.1103/PhysRevLett.87.040401.

[13] O. Gühne and G. Tóth. Entanglement detection. *Phys. Rep.*, 474(1):1–75, 2009. Link: https://doi.org/10.1016/j.physrep.2009.02.004.

[14] E. Chitambar and G. Gour. Quantum resource theories. *Rev. Mod. Phys.*, 91:025001, 2019. Link: https://doi.org/10.1103/RevModPhys.91.025001.

[15] G. Gour. *Quantum Resource Theories*. Cambridge University Press, 2025. Link: https://doi.org/10.1017/9781009560870.

[16] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865–942, 2009. Link: https://doi.org/10.1103/RevModPhys.81.865.

[17] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, and A. Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Commun. Math. Phys.*, 328:303–326, 2014. Link: https://doi.org/10.1007/s00220-014-1953-9.

[18] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens. Genuine network multipartite entanglement. *Phys. Rev. Lett.*, 125(24):240505, 2020. Link: https://doi.org/10.1103/PhysRevLett.125.240505.

[19] T. Kraft, S. Designolle, C. Ritz, N. Brunner, O. Gühne, and M. Huber. Quantum entanglement in the triangle network. *Phys. Rev. A*, 103(6):L060401, 2021. Link: https://doi.org/10.1103/PhysRevA.103.L060401.

[20] K. Hansenne, Z.-P. Xu, T. Kraft, and O. Gühne. Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques. *Nat. Commun.*, 13(1):496, 2022. Link: https://doi.org/10.1038/s41467-022-28006-3.

[21] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy. Multiplexed memory-insensitive quantum repeaters. *Phys. Rev. Lett.*, 98(6):060502, 2007. Link: https://doi.org/10.1103/PhysRevLett.98.060502.

[22] E. Shchukin, F. Schmidt, and P. van Loock. Waiting time in quantum repeaters with probabilistic entanglement swapping. *Phys. Rev. A*, 100(3):032322, 2019. Link: https://doi.org/10.1103/PhysRevA.100.032322.

[23] L. T. Weinbrenner, L. Vandré, T. Coopmans, and O. Gühne. Aging and reliability of quantum networks. *Phys. Rev. A*, 109(5):052611, 2024. Link: https://doi.org/10.1103/PhysRevA.109.052611.

[24] Y.-X. Wang, Z.-P. Xu, and O. Gühne. Quantum LOSR networks cannot generate graph states with high fidelity. *npj Quantum Inf.*, 10(1):11, 2024. Link: https://doi.org/10.1038/s41534-024-00806-z.

[25] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018. Link: https://doi.org/10.1126/science.aam9288.

[26] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.*, 95(4):045006, 2023. Link: https://doi.org/10.1103/RevModPhys.95.045006.

[27] M. Kuś and K. Życzkowski. Geometry of entangled states. *Phys. Rev. A*, 63(3):032307, 2001. Link: https://doi.org/10.1103/PhysRevA.63.032307.

[28] N. Johnston. Separability from spectrum for qubit-qudit states. *Phys. Rev. A*, 88(6):062330, 2013. Link: https://doi.org/10.1103/PhysRevA.88.062330.

[29] S. Arunachalam, N. Johnston, and V. Russo. Is absolute separability determined by the partial transpose? *Quantum Inf. Comput.*, 15(7–8):694–720, 2015. Link: https://www.rintonpress.com/xxqic15/qic-15-78/0694-0720.pdf.

[30] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson. The resource theory of Stabilizer quantum computation. *New J. Phys.*, 16:013009, 2014. Link: https://doi.org/10.1088/1367-2630/16/1/013009.

[31] M. Howard and E. Campbell. Application of a resource theory for magic states to fault-tolerant quantum computing. *Phys. Rev. Lett.*, 118(9):090501, 2017. Link: https://doi.org/10.1103/PhysRevLett.118.090501.

[32] S. Aaronson and D. Gottesman. Improved simulation of Stabilizer circuits. *Phys. Rev. A*, 70(5):052328, 2004. Link: https://doi.org/10.1103/PhysRevA.70.052328.

[33] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, 2005. Link: https://doi.org/10.1103/PhysRevA.71.022316.

[34] S. Khatri and M. M. Wilde. Principles of quantum communication theory: A modern approach, 2024. arXiv:2011.04672 [quant-ph]; Preliminary version of a book in progress; Link: https://arxiv.org/abs/2011.04672.

[35] S. Szalay. Multipartite entanglement measures. *Phys. Rev. A*, 92(4):042329, 2015. Link: https://doi.org/10.1103/PhysRevA.92.042329.

[36] Y. S. Weinstein and S. D. Buchbinder. Use of Shor states for the [[7,1,3]] quantum error-correcting code. *Phys. Rev. A*, 86:052336, 2012. Link: https://doi.org/10.1103/PhysRevA.86.052336.

[37] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993. Link: https://doi.org/10.1103/PhysRevLett.70.1895.

[38] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76(5):722–725, 1996. Link: https://doi.org/10.1103/PhysRevLett.76.722.

[39] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996. Link: https://doi.org/10.1103/PhysRevA.54.3824.

[40] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991. Link: https://doi.org/10.1103/PhysRevLett.67.661.

[41] M. Horodecki, P. Horodecki, and J. Oppenheim. Reversible transformations from pure to mixed states and the unique measure of information. *Phys. Rev. A*, 67(6):062104, 2003. Link: https://doi.org/10.1103/PhysRevA.67.062104.

[42] E. T. Campbell, B. M. Terhal, and C. Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, 2017. Link: https://doi.org/10.1038/nature23460.

[43] D. Gottesman. The heisenberg representation of quantum computers. In *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1998. Link: https://arxiv.org/abs/quant-ph/9807006.

[44] D. Bures. An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite w^*-algebras. *Trans. Am. Math. Soc.*, 135:199–212, 1969. Link: https://doi.org/10.2307/1995012.

[45] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78(12):2275–2279, 1997. Link: https://doi.org/10.1103/PhysRevLett.78.2275.

[46] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, 1998. Link: https://doi.org/10.1103/PhysRevA.57.1619.

[47] A. Streltsov, H. Kampermann, and D. Bruß. Linking a distance measure of entanglement to its convex roof. *New J. Phys.*, 12:123004, 2010. Link: https://doi.org/10.1088/1367-2630/12/12/123004.

[48] H. Umegaki. Conditional expectation in an operator algebra. iv. entropy and information. *Kodai Math. Sem. Rep.*, 14(2):59–85, 1962. Link: https://doi.org/10.2996/kmj/1138844604.

[49] F. G. S. L. Brandão and G. Gour. Reversible framework for quantum resource theories. *Phys. Rev. Lett.*, 115(7):070503, 2015. Link: https://doi.org/10.1103/PhysRevLett.115.070503.

[50] J. I. de Vicente, C. Spee, and B. Kraus. The maximally entangled set of multipartite quantum states. *Phys. Rev. Lett.*, 111:110502, 2013. Link: https://doi.org/10.1103/PhysRevLett.111.110502.

[51] P. Contreras-Tejada, C. Palazuelos, and J. I. de Vicente. Resource theory of entanglement with a unique multipartite maximally entangled state. *Phys. Rev. Lett.*, 122(12):120503, 2019. Link: https://doi.org/10.1103/PhysRevLett.122.120503.

[52] W. Zhou and F. Buscemi. General state transitions with exact resource morphisms: A resource-theoretic approach. *J. Math. Phys.*, 61:102201, 2020. Link: https://doi.org/10.1063/5.0015603.

[53] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017. Link: https://doi.org/10.1126/science.aan3211.

[54] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson. Realization of a multinode quantum network of remote solid-state qubits. *Science*, 372(6539):259–264, 2021. Link: https://doi.org/10.1126/science.abg1919.

[55] M. Pompili, C. Delle Donne, I. te Raa, B. van der Vecht, M. Skrzypczyk, G. Ferreira, L. de Kluijver, A. J. Stolk, S. L. N. Hermans, P. Pawełczak, W. Kozlowski, R. Hanson, and S. Wehner. Experimental demonstration of entanglement delivery using a quantum network stack. *npj Quantum Inf.*, 8:121, 2022. Link: https://doi.org/10.1038/s41534-022-00631-2.

[56] P. Contreras-Tejada, C. Palazuelos, and J. I. de Vicente. Asymptotic survival of genuine multipartite entanglement in noisy quantum networks depends on the topology. *Phys. Rev. Lett.*, 128(22):220501, 2022. Link: https://doi.org/10.1103/PhysRevLett.128.220501.

[57] E. Wolfe, R. W. Spekkens, and T. Fritz. The inflation technique for causal inference with latent variables. *J. Causal Inference*, 7(2):20170020, 2019. Link: https://doi.org/10.1515/jci-2017-0020.

[58] E. Wolfe, A. Pozas-Kerstjens, M. Grinberg, D. Rosset, A. Acín, and M. Navascués. Quantum inflation: A general approach to quantum causal compatibility. *Phys. Rev. X*, 11(2):021043, 2021. Link: https://doi.org/10.1103/PhysRevX.11.021043.

[59] J. Neumann, T. V. Kondra, K. Hansenne, L. T. Weinbrenner, H. Kampermann, O. Gühne, D. Bruß, and N. Wyderka. No quantum advantage without classical communication: fundamental limitations of quantum networks, 2025. arXiv:2503.09473 [quant-ph]; Link: https://arxiv.org/abs/2503.09473.

[60] X. Zhou, Z.-P. Xu, L.-L. Sun, C. Wu, and S. Yu. Exploring the boundary of quantum network states from inside out. *Commun. Phys.*, 9(1):3, 2025. Link: https://doi.org/10.1038/s42005-025-02435-0.

[61] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A*, 461(2053):207–235, 2005. Link: https://doi.org/10.1098/rspa.2004.1372.

[62] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106(11):110506, 2011. Link: https://doi.org/10.1103/PhysRevLett.106.110506.

[63] R. Augusiak and P. Horodecki. Multipartite secret key distillation and bound entanglement. *Phys. Rev. A*, 80(4):042307, 2009. Link: https://doi.org/10.1103/PhysRevA.80.042307.

[64] F. Grasselli, H. Kampermann, and D. Bruß. Finite-key effects in multipartite quantum key distribution protocols. *New J. Phys.*, 20(11):113014, 2018. Link: https://doi.org/10.1088/1367-2630/aaec34.

[65] J. Neumann, H. Kampermann, D. Bruß, and A. Trushechkin. Bounds on quantum conference key agreement in pair-entangled networks, 2026. arXiv:2605.18399 [quant-ph]; Link: https://arxiv.org/abs/2605.18399.

[66] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81(26):5932–5935, 1998. Link: https://doi.org/10.1103/PhysRevLett.81.5932.

[67] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8(1):15043, 2017. Link: https://doi.org/10.1038/ncomms15043.

[68] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement breaking channels. *Rev. Math. Phys.*, 15(06):629–641, 2003. Link: https://doi.org/10.1142/S0129055X03001709.

[69] R. Hildebrand. Positive partial transpose from spectra. *Phys. Rev. A*, 76(5):052325, 2007. Link: https://doi.org/10.1103/PhysRevA.76.052325.

[70] L. Gurvits and H. Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Phys. Rev. A*, 66(6):062311, 2002. Link: https://doi.org/10.1103/PhysRevA.66.062311.

[71] J. Abellanet-Vidal, G. Müller-Rigat, G. Rajchel-Mieldzioć, and A. Sanpera. Sufficient criteria for absolute separability in arbitrary dimensions via linear map inverses. *Rep. Prog. Phys.*, 88(10):107601, 2025. Link: https://doi.org/10.1088/1361-6633/ae0cfa.

[72] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40(8):4277–4281, 1989. Link: https://doi.org/10.1103/PhysRevA.40.4277.

[73] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 10th anniversary edition, 2010. Link: https://doi.org/10.1017/CBO9780511976667.

[74] B. W. Reichardt. Quantum universality from magic states distillation applied to CSS codes. *Quantum Inf. Process.*, 4:251–264, 2005. Link: https://doi.org/10.1007/s11128-005-7654-8.

[75] R. Rubboli, R. Takagi, and M. Tomamichel. Mixed-state additivity properties of magic monotones based on quantum relative entropies for single-qubit states and beyond. *Quantum*, 8:1492, 2024. Link: https://doi.org/10.22331/q-2024-10-04-1492.

[76] C. Deckers, J. Neumann, H. Kampermann, and D. Bruß. The relative entropy of magic and its nonadditivity, 2026. arXiv:2605.22392 [quant-ph]; Link: https://arxiv.org/abs/2605.22392.

[77] T. V. Kondra, P. Barrios Hita, J. Neumann, H. Kampermann, and D. Bruß. Fundamental limitations on entanglement extraction from purity, 2026. arXiv:2605.29197 [quant-ph]; Link: https://arxiv.org/abs/2605.29197.

[78] M.-O. Renou, Y. Wang, S. Boreiri, S. Beigi, N. Gisin, and N. Brunner. Limits on correlations in networks for quantum and no-signaling resources. *Phys. Rev. Lett.*, 123(7):070403, 2019. Link: https://doi.org/10.1103/PhysRevLett.123.070403.

[79] K. Matusita. On the notion of affinity of several distributions and some of its applications. *Ann. Inst. Stat. Math.*, 19(1):181–192, 1967. Link: https://doi.org/10.1007/BF02911675.

[80] T. Nuradha, H. K. Mishra, F. Leditzky, and M. M. Wilde. Multivariate fidelities. *J. Phys. A: Math. Theor.*, 58(16):165304, 2025. Link: https://doi.org/10.1088/1751-8121/adc645.

[81] T. Kraft, C. Ritz, N. Brunner, M. Huber, and O. Gühne. Characterizing genuine multilevel entanglement. *Phys. Rev. Lett.*, 120(6):060502, 2018. Link: https://doi.org/10.1103/PhysRevLett.120.060502.

[82] A. Pirker, J. Wallnöfer, and W. Dür. Modular architectures for quantum networks. *New J. Phys.*, 20:053054, 2018. Link: https://doi.org/10.1088/1367-2630/aab05f.

[83] S. S. Chelluri, S. Khatri, and P. van Loock. A resource- and computationally-efficient protocol for multipartite entanglement distribution in Bell-pair networks, 2025. arXiv:2412.04252 [quant-ph]; Link: https://arxiv.org/abs/2412.04252.

[84] G. Carrara, H. Kampermann, D. Bruß, and G. Murta. Genuine multipartite entanglement is not a precondition for secure conference key agreement. *Phys. Rev. Res.*, 3(1):013264, 2021. Link: https://doi.org/10.1103/PhysRevResearch.3.013264.

[85] S. N. Filippov, K. Yu. Magadov, and M. A. Jivulescu. Absolutely separating quantum maps and channels. *New J. Phys.*, 19:083010, 2017. Link: https://doi.org/10.1088/1367-2630/aa7e06.

[86] A. Streltsov, H. Kampermann, S. Wölk, M. Gessner, and D. Bruß. Maximal coherence and the resource theory of purity. *New J. Phys.*, 20:053058, 2018. Link: https://doi.org/10.1088/1367-2630/aac484.

[87] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. Link: https://doi.org/10.1017/9781316848142.

[88] P. M. Alberti and A. Uhlmann. *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing*. Springer, 1982. Link: https://books.google.com/books?id=cVHTS7cjkqsC.

Eidesstattliche Versicherung

Ich versichere an Eides Statt, dass die Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der „Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Universität Düsseldorf“ erstellt worden ist.
Zur sprachlichen Korrektur und stilistischen Überarbeitung einzelner Textpassagen wurde ein KI-gestütztes Sprachmodell verwendet. Die inhaltliche Konzeption, die wissenschaftliche Argumentation, die Berechnungen, die Ergebnisse und die Schlussfolgerungen dieser Arbeit stammen von mir.

Düsseldorf, den 07.07.2026

_____
Name

Paper A

No quantum advantage without classical communication: fundamental limitations of quantum networks

The following text is reproduced from the preprint

Justus Neumann, Tulja Varun Kondra, Kiara Hansenne, Lisa T. Weinbrenner, Hermann Kampermann, Otfried Gühne, Dagmar Bruß, and Nikolai Wyderka
No quantum advantage without classical communication: fundamental limitations of quantum networks arXiv preprint, 2025. arXiv:2503.09473 [quant-ph].

Statement of contribution

My main contribution consisted of deriving upper bounds on the performance of quantum networks with local operations and shared randomness. I derived the upper bounds in Results 1, 2, and 5. The upper bound in Result 4 was derived jointly with Otfried Gühne, Tulja Varun Kondra and Nikolai Wyderka. Nikolai Wyderka derived Result 3 and the lower bounds. The results were interpreted and discussed together with Tulja Varun Kondra, Kiara Hansenne, Lisa T. Weinbrenner, Hermann Kampermann, Otfried Gühne, Dagmar Bruß, and Nikolai Wyderka. The manuscript was finalized with input from all authors. The project was supervised by Hermann Kampermann, Otfried Gühne, Dagmar Bruß, and Nikolai Wyderka.

No quantum advantage without classical communication: fundamental limitations of quantum networks

Justus Neumann,[1] Tulja Varun Kondra,[1] Kiara Hansenne,[2,3] Lisa T. Weinbrenner,[2]
Hermann Kampermann,[1] Otfried Gühne,[2] Dagmar Bruß,[1] and Nikolai Wyderka[1]

[1] *Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany*
[2] *Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Str. 3, 57068 Siegen, Germany*
[3] *Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191 Gif-sur-Yvette, France*

(Dated: March 13, 2025)

Quantum networks connect systems at separate locations via quantum links, enabling a wide range of quantum information tasks between distant parties. Large-scale networks have the potential to enable global secure communication, distributed quantum computation, enhanced clock synchronization, and high-precision multiparameter metrology. For the optimal development of these technologies, however, it is essential to identify the necessary resources and sub-routines that will lead to the quantum advantage, but this is demanding even for the simplest protocols in quantum information processing. Here we show that quantum networks relying on the long-distance distribution of bipartite entanglement, combined with local operations and shared randomness, cannot achieve a relevant quantum advantage. Specifically, we prove that these networks do not help in preparing resourceful quantum states such as Greenberger-Horne-Zeilinger states or cluster states, despite the free availability of long-distance entanglement. At an abstract level, our work points towards a fundamental difference between bipartite and multipartite entanglement. From a practical perspective, our results highlight the need for classical communication combined with quantum memories to fully harness the power of quantum networks.

arXiv:2503.09473v1 [quant-ph] 12 Mar 2025

I. INTRODUCTION

Quantum networks promise to provide platforms for long-distance quantum information processing, enabling global secure communication and distributed quantum computation [1–3]. Consequently, many experimental efforts aim towards an experimental realization of building blocks of network structures [4–6]. A critical requirement for many applications is the ability of a network to generate and distribute entangled states among many distant parties. Particularly relevant among these states are quantum graph states, such as the Greenberger-Horne-Zeilinger (GHZ) states and cluster states. Indeed, these states can then be used for applications like blind quantum computation [7], quantum metrology [8–10], quantum key distribution protocols [11] and clock synchronization [12]. Preparing and distributing such states in practice, however, presents significant challenges, as it requires precise control over high-dimensional quantum systems, a task that becomes increasingly complex with system size.

In general, distributed information processing can be modeled in different ways, see also Fig. 1(a). In the simplest scenario (Fig. 1(a) left), one considers different parties controlling quantum mechanical systems in their labs, where the parties can communicate classically. This scenario, however, does not allow to generate entanglement between the parties, so no quantum advantage can be expected. In the most advanced scenario (Fig. 1(a) right), the parties not only communicate and control their systems, they also share initial bipartite entanglement. In this scenario, protocols like teleportation between the nodes can be carried out, allowing the preparation of arbitrary global states as well as the execution of general information processing protocols. This, however, requires the experimental implementation of quantum memories, as well as performing quantum operations in one lab in dependence of the measurement results communicated by the other parties.

In order to take into account the current experimental constraints, the community has studied intermediate models of networks, which are closer to the actual realization. One central model are networks based on local operations and shared randomness (LOSR), where parties are connected via bipartite quantum sources and can only rely on local operations along with pre-shared classical correlations [13–17]. LOSR networks also start from distributed bipartite entanglement, but they do not rely on time-consuming classical communication that necessitates functioning quantum memories. These characteristics make LOSR networks experimentally accessible, and as a result their properties and limitations have been actively studied in recent years [18–24].

But are quantum networks in the LOSR scenario really useful tools to unleash the full power of distributed quantum information processing? The main result of this paper is a negative answer to this question. More precisely, we consider the task of generating multipartite highly entangled quantum states. We demonstrate that the maximal fidelity achievable by LOSR networks with a large class of resource states does not significantly exceed the values reachable by classical networks. In other words, the advantage provided by bipartite sources for preparing multipartite entangled states to be used by

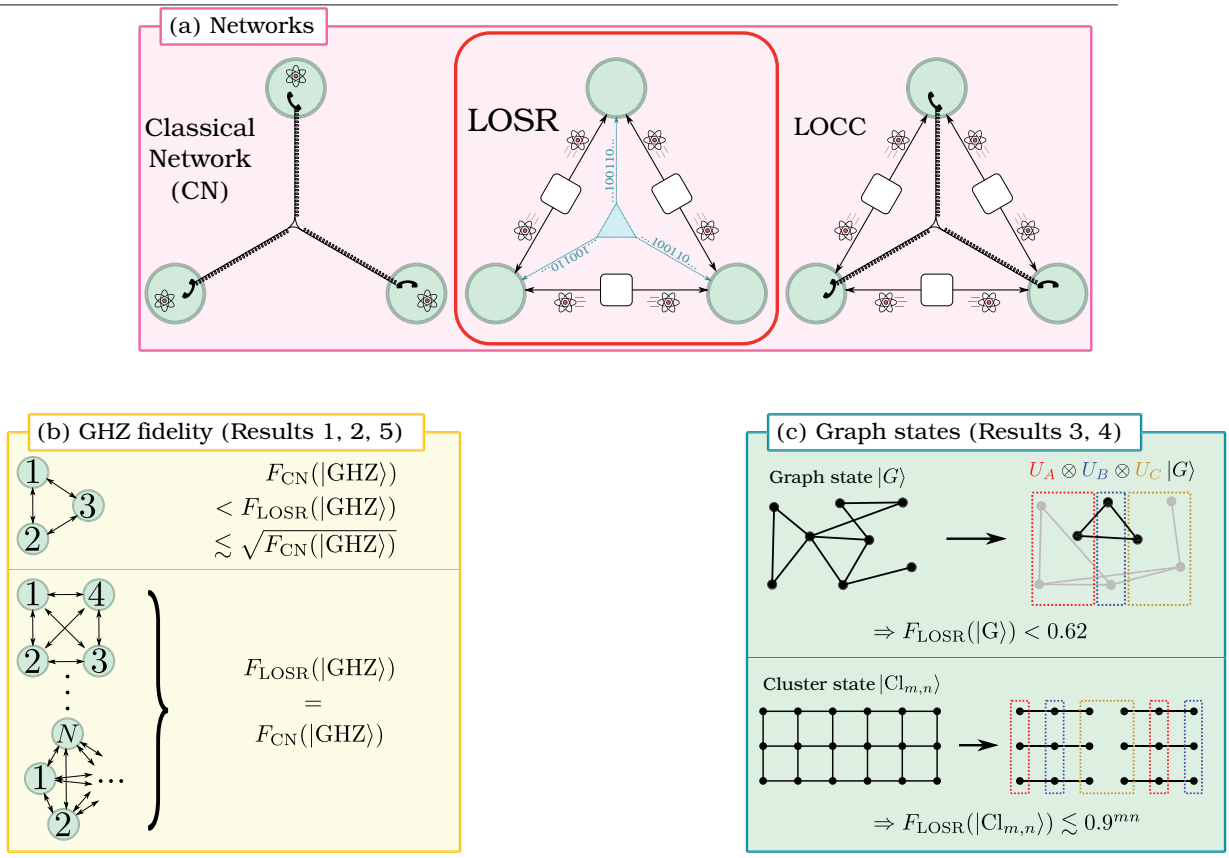


Figure 1. Summary of the setting and our results. (a) We consider quantum LOSR (local operations and shared randomness, center) networks, where distant parties are connected by bipartite entangled sources and have access to a source of shared randomness. We show that this scenario is, in terms of capabilities, much more similar to a completely classical network (CN, left) than to a quantum LOCC network (local operations and classical communications, right), where entangled sources are accompanied by classical communication, which allows for preparation of arbitrary quantum states. (b) In particular, we show that for the task of multipartite GHZ state preparation, a small advantage of LOSR networks over the classical network scenario is present only in tripartite networks, whereas it offers no advantage at all in four- and larger-partite networks. (c) More generally, we show that no connected graph state can be prepared with high fidelity in LOSR networks. Some relevant families of states such as cluster states, being resource states for measurement-based quantum computation, even have exponentially decreasing fidelity bounds in terms of the number of parties.

distant parties is minimal, and additional resources — such as quantum memories, classical communication, or direct distribution of multipartite entangled states — are essential. Our discoveries resemble an observation made in Ref. [21] where it was shown that for the special case of output states in the symmetric subspace only, LOSR networks cannot produce anything else than fully separable states.

Consequently, this limitation should not be seen as a merely negative result. In fact, no-go theorems have often served as starting points for major advancements, by forcing the research community to look for different routes. For example, the well-known constraints of linear optics in performing Bell state measurements motivated the development of alternative approaches, such as hyperentanglement [25–28] or the usage of ancilla photons combined with photon-number resolving detectors [29, 30]. Similarly, early recognized limitations in entanglement distillation with Gaussian states [31, 32] ultimately led to the study of non-Gaussian quantum operations, culminating in the experimental implementation of entanglement distillation with non-gaussian operations [33]. Similarly, our results highlight the need to explore alternative network architectures, such as hybrid models incorporating classical communication together with quantum channels and memories, to fully utilize the potential of quantum networks.

II. PREPARING MULTI-PARTY QUANTUM STATES

If quantum states shall be prepared in a network, the N-qubit GHZ state

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}) \tag{1}$$

is a desirable candidate, since it yields a quantum advantage in metrology and conference key agreement [11, 34]. On the other hand, generating a two-dimensional cluster state allows us to implement schemes for measurement-based quantum computation [35] or the establishment of a data bus [36]. Both families of states are part of the family of graph states [37], which will therefore be the main interest of our work.

None of the above-mentioned tasks can be successfully performed without the ability to generate these states with high fidelity. In particular, uncorrelated product states (that can arise in classical networks) do not provide any quantum advantage for these applications, making their use ineffective. Thus, the relevant question is: how well can graph states be generated in quantum networks? Do LOSR networks provide any advantage beyond classical networks?

To assess the suitability of the LOSR paradigm for large-scale quantum state preparation, we consider the fidelity as a popular and physically relevant measure of the distinguishability of quantum states [38]. First, we consider the simplest triangle scenario, see also Fig. 2 and the creation of tripartite GHZ states. We present optimized protocols for GHZ generation, but also derive rigorous upper bounds on the achievable fidelities. Subsequently, we show that the bounds derived in the triangular scenario can be lifted to fidelity constraints in arbitrarily large networks, thereby strictly limiting the amount of multipartite entanglement within such networks. Interestingly, besides having an impact on quantum network design, this also may shed light on some discussions on notions of multipartite entanglement in the literature (see e.g. Ref. [18] and Ref. [39] sections VI. E–F).

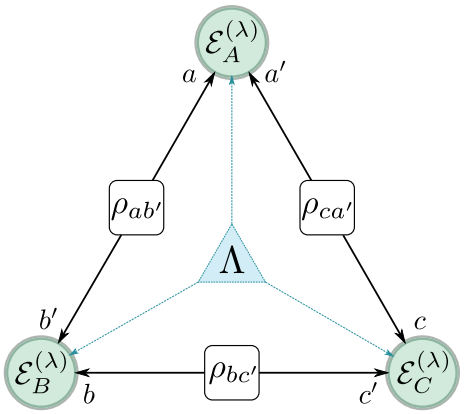


Figure 2. The LOSR (local operations and shared randomness) scenario of three-partite networks. The three parties A, B and C are receiving particles from bipartite sources ρ_{ij} and are allowed to perform local operations $\mathcal{E}_A^{(\lambda)}, \mathcal{E}_B^{(\lambda)}, \mathcal{E}_C^{(\lambda)}$, based on a shared random variable λ, to produce a three-partite output state.

III. RESULTS

A. Triangle networks

We start with the simplest nontrivial quantum network of three parties, assuming the framework of local operations and shared randomness. In this scenario, three spatially separated participants, called Alice, Bob and Charlie (A, B and C), are connected by bipartite source states shared between each pair. The parties apply local quantum operations on their subsystems, assisted by a shared classical random variable. More formally, states that can be prepared in a triangle LOSR network are of the form

$$\rho = \sum_{\lambda} p(\lambda) \mathcal{E}_A^{\lambda} \otimes \mathcal{E}_B^{\lambda} \otimes \mathcal{E}_C^{\lambda} [\rho_{ab'} \otimes \rho_{bc'} \otimes \rho_{ca'}], \quad (2)$$

where $\mathcal{E}_A^{\lambda}$, $\mathcal{E}_B^{\lambda}$, $\mathcal{E}_C^{\lambda}$ are local (trace-preserving) operations, $\rho_{ab'}$, $\rho_{bc'}$, $\rho_{ca'}$ are the source states and $p(\lambda)$ is a classical probability distribution (see Fig. 2 and Refs. [18, 21] for some technical details). This definition can be extended to an arbitrary number of parties by considering quantum networks where all participants are connected by bipartite source states. In the following, we call states that can be brought into the form of Eq. (2) LOSR states. Note that we do not limit the dimension of the bipartite source states ρ_{ij}.

To analyze the amount of multipartite entanglement one can generate we consider the maximal fidelity of an LOSR network state ρ with strongly entangled multipartite states, such as the multipartite qudit GHZ state $|\mathrm{GHZ}_{N,d}\rangle$, given by

$$F_{\mathrm{LOSR}}(|\mathrm{GHZ}_{N,d}\rangle) = \max_{\rho \in \mathrm{LOSR}} \langle \mathrm{GHZ}_{N,d}|\rho|\mathrm{GHZ}_{N,d}\rangle \,, \quad (3)$$

where $|\mathrm{GHZ}_{N,d}\rangle = (\sum_{i=0}^{d-1} |i\rangle^{\otimes N})/\sqrt{d}$, is the d-level GHZ state of N parties (if $d = 2$, we omit the dimension and write $|\mathrm{GHZ}_N\rangle$ instead). Of course, this is a specific target state, but we will later show that much larger classes of target states can be reduced to the GHZ case. In the case of the GHZ state, a fidelity value of $F = 1/d$ can directly be achieved by preparing the product state $|0\rangle^{\otimes N}$. In contrast, any value above $1/d$ already indicates the presence of genuine multipartite entanglement [40], and a value of $F_{\mathrm{LOSR}}(|\mathrm{GHZ}_{N,d}\rangle) = 1$ would indicate that the GHZ state can be prepared perfectly.

Let us start our discussion with the three-qubit case. For this, using numerical semidefinite programming techniques together with so-called inflation arguments, Ref. [18] showed that $F_{\mathrm{LOSR}}(|\mathrm{GHZ}_3\rangle) \leq (1 + \sqrt{3})/4 < 0.684$. This raises the question of whether LOSR quantum networks can reach this bound. In fact, the authors of Ref. [18] also report that they numerically obtained a LOSR state with a fidelity of approximately 0.517. On

the one hand, this is remarkable, as it shows that genuine multipartite entanglement can be prepared in the LOSR scenario, on the other hand this begs for improvement and the construction of explicit network protocols.

So, we designed constructive protocols for the preparation of three-qubit GHZ states in LOSR networks, see the Appendix A for details. For the case of two-qubit source states ρ_{ij} we find the optimal protocol, giving a GHZ fidelity of $F = [5+4\cos(2\pi/7)]/[12+4\cos(2\pi/7)] \approx 0.517$, confirming the reported numerical value. Surprisingly, however, the fidelity can be systematically increased if higher-dimensional resource states are used. Studying our optimized protocols for up to ten-dimensional source states, the achievable fidelities converge to $F \approx 0.548$. The fact that the reached fidelities increase monotonically with the source dimension suggests that the fidelity can act as a dimensionality witness for the sources.

On the other hand, we developed a novel approach for obtaining upper bounds on the achievable fidelities. This is based on an interpretation of the fidelity as an optimization over generalized measurements [41], combined with the Finner inequality [42] (see also Appendices C and D) which for the qubit case leads to $F < 0.618$. This allows us to summarize our first main result:

Result 1

In LOSR networks of three nodes the maximal achievable fidelity with the three-qubit GHZ state is bounded by

$$0.548 < F_{LOSR}(|GHZ_3\rangle) < 0.618. \tag{4}$$

Before discussing more general classes of quantum states and larger networks, let us formulate what our methods can teach about the generation of higher-dimensional GHZ states in triangle networks. In fact, as outlined in the Appendices, the methods can, with some modifications, also be applied to these cases. In our optimized network protocols for generating the states, however, it is relevant whether the dimension is odd or even. All our results can be summarized as follows:

Result 2

In LOSR networks of three nodes the maximal achievable fidelity with the three-qudit GHZ state for $d \geq 3$ is bounded by

$$\frac{1}{d}\left(\frac{3}{2} - \frac{\lfloor d/2 \rfloor}{d(d-1)}\right) \leq F_{LOSR}(|GHZ_{3,d}\rangle) \leq \frac{1}{\sqrt{d}}, \tag{5}$$

where $\lfloor \cdots \rfloor$ indicates the floor function.

Note that Result 2 also applies to $d = 2$, but we have stronger bounds in this case with Result 1. Since the fidelities of the constructed states scale like $3/(2d)$ and exceed the value of $1/d$, our constructive protocols show that the preparation of genuine multipartite entanglement is possible for all output dimensions. In contrast, the difference between the upper bound and the threshold $1/d$ is not large and vanishes in the asymptotic limit.

B. Networks of arbitrary size

In the following, we introduce a method to treat networks of arbitrary size. The basic idea is the following (see also Fig. 3 (a)): consider a network of N nodes with bipartite sources, which is able to prepare a quantum state ρ_N. We can group the N nodes into three groups, A, B, and C, take local transformations $\mathcal{E}_A$, $\mathcal{E}_B$, and $\mathcal{E}_C$ acting locally on these groups and then consider the state

$$\mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\rho_N) = \rho_\triangle. \tag{6}$$

Clearly, since ρ_N can be generated in the network, the state $\rho_\triangle$ can be prepared in the triangle network formed by the three groups A, B, and C. Conversely, if $\rho_\triangle$ is not feasible, e.g., due to our results from the previous section, any state ρ_M which can be reduced to $\rho_\triangle$ via some maps $\mathcal{E}_A$, $\mathcal{E}_B$, and $\mathcal{E}_C$, cannot be prepared in the full network of N nodes with bipartite sources.

To make this idea a powerful tool, we use three specifications. First, we focus on pure states and consider unitary transformations as maps. More precisely, for a given N particle state $|\psi_N\rangle$ we aim to find three groups and unitaries such that

$$U_A \otimes U_B \otimes U_C \, |\psi_N\rangle = |\phi_\triangle\rangle_{abc} \otimes |\tau\rangle \,, \tag{7}$$

where $a \subseteq A$, $b \subseteq B$, and $c \subseteq C$ are subsets of the groups and $|\tau\rangle$ is a residual state on the remaining nodes. By tracing out these nodes, the state $|\phi_\triangle\rangle_{abc}$ can be prepared in the triangle network, if $|\psi_N\rangle$ can be prepared in the large network. Importantly, this ansatz gives a direct relation between reachable fidelities in networks. If a state ρ_N can be prepared in the large network, having a fidelity F with the state $|\psi_N\rangle$, then one can prepare a state $\rho_\triangle$ in the triangle scenario, having at least the same fidelity F with $|\phi_\triangle\rangle_{abc}$.

Second, we want to use our fidelity bounds on the GHZ state in triangle networks to derive limitations for general networks. Third, we can employ a specific property of GHZ states: multiple copies of a three-qubit GHZ state are unitarily equivalent to a single GHZ state in higher dimensions [43]

$$|\mathrm{GHZ}_3\rangle^{\otimes k} \cong |\mathrm{GHZ}_{3,2^k}\rangle \,. \tag{8}$$

Consequently, if several copies of GHZ states can be prepared in the tripartitioned network, one can apply the exponentially decaying fidelity bounds for high-dimensional GHZ states from Result 2.

All that remains to be done to understand the general limitations of large quantum networks is to identify families of quantum states, which can be transformed into

three-partite GHZ states using the local transformation on three groups of nodes as outlined above. Here, the family of quantum graph states comes into play. Graph states form a family of multi-qubit quantum states, comprising multipartite GHZ states, as well as cluster states [37, 44, 45]. For defining graph states one considers a graph, consisting of nodes which are linked with some edges. Then, one associates each node with a qubit, while edges correspond to entangling two-qubit gates carried out between two nodes, to arrive at a pure quantum state corresponding to the graph (the formal definitions are given in Appendix B 2). Graph states are particularly relevant in the context of quantum networks: protocols such as measurement-based quantum computation [35], blind quantum computation [46], or entanglement routing [36] require the distribution of graph states to distant parties. Naturally, graph states have previously been studied in the context of LOSR networks [21–23], but the only known general fidelity bound states that arbitrary graph states cannot be prepared in networks using bipartite sources with fidelities exceeding 0.9 [22].

Remarkably, for graph states the number of extractable GHZ states for a fixed tripartition has been studied and is known as an entanglement quantifier [47, 48]. In these works, however, it remained unclear whether every graph state admits a tripartition that yields at least one GHZ state, but in Appendix B 2 we demonstrate that this is indeed the case. This directly leads to:

Result 3

No graph state corresponding to a graph with at least three connected nodes can be prepared in an LOSR network with bipartite sources with a fidelity larger than $F_{LOSR}(|GHZ_3\rangle) < 0.618$.

To strengthen this result we note that many graph states admit partitions that can produce more than one GHZ state. This includes the family of two-dimensional cluster states $|\mathrm{Cl}_{m,n}\rangle$, which correspond to a $N = m \times n$ grid as a graph, see Fig. 3 (b). These are known to be resource states for measurement-based quantum computation [35]. For such states, it is always possible to find a tripartition yielding the maximal number of $k = \lfloor mn/3 \rfloor$ GHZ states. Moreover, a lower bound on the achievable fidelity in LOSR networks can be obtained from the knowledge of the maximal fidelity of fully separable product states with the cluster state [49]. Together, we obtain

Result 4

The maximal fidelity of the $m \cdot n$*-partite cluster state* $|Cl_{m,n}\rangle$ *in LOSR networks of* N *parties and bipartite sources is bounded by*

$$\frac{1}{2^{\lfloor \frac{mn}{2} \rfloor}} \leq F_{LOSR}(|Cl_{m,n}\rangle) \leq \frac{1}{2^{\frac{1}{2}\lfloor \frac{mn}{3} \rfloor}}. \tag{9}$$

The fact that the maximal achievable fidelity is suppressed exponentially with the number of qubits suggests that LOSR networks do not provide any advantage compared to classical networks for tasks based on cluster states.

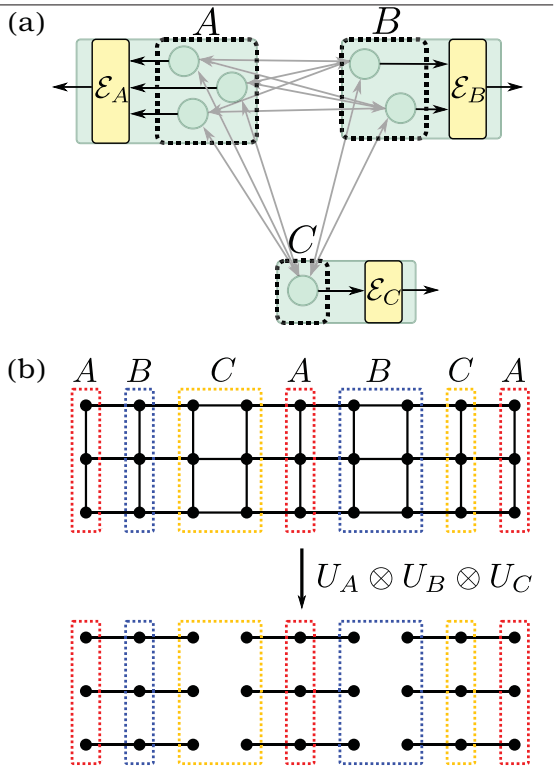


Figure 3. (a) Visualization of the reduction of an N-partite network (here, $N = 6$) to a triangle network by combining several nodes into one. If a state ρ_N is generated by the N-partite network, then $\rho_\triangle = \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\rho_N)$ must be generable in a tripartite network. (b) Example of GHZ extraction from a cluster state. The initial 27-qubit cluster state $|\mathrm{Cl}_{3,9}\rangle$ can be transformed into $|\mathrm{GHZ}_3\rangle^{\otimes 9}$ using a tripartition of the parties into three sets A (indicated red), B (blue) and C (orange). Within the sets, the unitaries U_A, U_B and U_C are chosen such that they remove links, leaving decoupled graph states of three connected parties which are known to be equivalent to $|\mathrm{GHZ}_3\rangle$.

C. Multipartite GHZ states

Our previous results prompt two immediate questions. First, we focused so far on the ability to extract three-partite states, but one could ask for the extraction of more-partite states, e.g. $|\mathrm{GHZ}_4\rangle$ instead, if better fidelity bounds are known for these states. Although it is often the case, it is, however, not always possible to find tetrapartitions that extract $|\mathrm{GHZ}_4\rangle$ from connected graph states [50]. A second question asks for direct fidelity bounds for $|\mathrm{GHZ}_{N,d}\rangle$ for $N > 3$ without resorting to any GHZ extraction procedure. For $N \geq 4$, stronger bounds than the ones for the triangle scenario can be established. They imply that in these LOSR networks the

fidelity of GHZ states cannot exceed the fidelity that can be obtained without distributing bipartite entanglement at all.

Result 5

In quantum networks of $N \geq 4$ nodes with bipartite sources, the maximal fidelity with $|GHZ_{N,d}\rangle$ is bounded by $1/d$. The same fidelity can be reached by a fully separable state in the classical network.

The proof of the statement can be found in Appendix D. Note that this fidelity bound allows to construct novel extraction scenarios, aiming at the extraction of four qubit GHZ states. In this sense, the results of Ref. [50] may be used to provide more bounds for general graph states.

IV. DISCUSSION

Our results demonstrate a fundamental limit in the state preparation capabilities of LOSR quantum networks with bipartite sources. Specifically, we have shown that these networks are inherently unable to generate entangled multipartite states with fidelities that significantly exceed those of fully separable states. To do so, we also provided insights into GHZ state extraction from graphs states that are along the lines of Refs. [50, 51]. We believe these results are of independent interest.

Our results enforce a reassessment of the potential of the LOSR paradigm for distributed quantum information processing and raise the need to explore alternative network architectures that rely on classical communication. Since the usage of classical communication typically introduces time delays, adding quantum memories may be required. To deal with this, a crucial next step is to determine the minimal amount of classical communication required for preparing highly entangled states in networks. This would allow us to derive concrete estimates on memory usage times and waiting times [52–54], setting requirements for practical and scalable experimental implementations. Moreover, this may pave the way towards more efficient schemes for entanglement distillation [55, 56]. In fact, understanding the minimal resources required for reaching the full power of quantum networks may guide the ultimate development of the quantum internet.

Note added.— While finishing this work we learned that related but complementary results have been obtained by Xiang Zhou et al.

ACKNOWLEDGMENTS

We thank Ghislaine Coulter-de Wit, Mariami Gachechiladze, Tristan Kraft, Julia Kunzelmann, Nikolai Miklin, Anton Trushechkin and Lina Vandré for discussions.

This work has been supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, project numbers 447948357 and 440958198), the Sino-German Center for Research Promotion (Project M-0294), the German Ministry of Education and Research (Projects QuKuK, BMBF Grant No. 16KIS1618K and QSolid, BMBF Grant No. 13N16163). K.H. and L.T.W. acknowledge support by the House of Young Talents of the University of Siegen.

[1] H. J. Kimble, Nature **453**, 1023 (2008).
[2] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, 303 (2018).
[3] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, Rev. Mod. Phys. **95**, 045006 (2023).
[4] S. Hermans, M. Pompili, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, Nature **605**, 663 (2022).
[5] J.-L. Liu, X.-Y. Luo, Y. Yu, C.-Y. Wang, B. Wang, Y. Hu, J. Li, M.-Y. Zheng, B. Yao, Z. Yan, *et al.*, arXiv preprint arXiv:2309.00221 (2023).
[6] L. Hartung, M. Seubert, S. Welte, E. Distante, and G. Rempe, Science **385**, 179 (2024).
[7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[8] P. Sekatski, S. Wölk, and W. Dür, Phys. Rev. Res. **2**, 023052 (2020).
[9] T. J. Proctor, P. A. Knott, and J. A. Dunningham, Phys. Rev. Lett. **120**, 080501 (2018).
[10] X. Guo, C. R. Breum, J. Borregaard, S. Izumi, M. V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U. L. Andersen, Nat. Phys. **16**, 281 (2020).
[11] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Adv. Quantum Technol. **3**, 2000025 (2020).
[12] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, Nat. Phys. **10**, 582 (2014).
[13] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[14] D. Schmid, T. C. Fraser, R. Kunjwal, A. B. Sainz, E. Wolfe, and R. W. Spekkens, Quantum **7**, 1194 (2023).
[15] J. I. de Vicente, J. Phys. A: Math. Theor. **47**, 424017 (2014).
[16] M. Forster, S. Winkler, and S. Wolf, Phys. Rev. Lett. **102**, 120401 (2009).
[17] G. Gutoski, Quantum Inf. Comput. **9**, 739 (2009).
[18] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens, Phys. Rev. Lett. **125**, 240505 (2020).
[19] M.-X. Luo, Adv. Quantum Technol. **4**, 2000123 (2021).
[20] T. Kraft, S. Designolle, C. Ritz, N. Brunner, O. Gühne, and M. Huber, Phys. Rev. A **103**, L060401 (2021).
[21] K. Hansenne, Z.-P. Xu, T. Kraft, and O. Gühne, Nat. Commun. **13**, 496 (2022).
[22] Y.-X. Wang, Z.-P. Xu, and O. Gühne, npj Quantum Inf. **10**, 11 (2024).
[23] O. Makuta, L. T. Ligthart, and R. Augusiak, npj Quantum Inf. **9**, 117 (2023).
[24] Y. Yang, B. Yadin, and Z.-P. Xu, Phys. Rev. Lett. **132**,

210801 (2024).
[25] Y.-B. Sheng, F.-G. Deng, and G. L. Long, Phys. Rev. A **82**, 032318 (2010).
[26] T.-C. Wei, J. T. Barreiro, and P. G. Kwiat, Phys. Rev. A **75**, 060305 (2007).
[27] S. P. Walborn, S. Pádua, and C. H. Monken, Phys. Rev. A **68**, 042313 (2003).
[28] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **96**, 190501 (2006).
[29] F. Ewert and P. van Loock, Phys. Rev. Lett. **113**, 140403 (2014).
[30] M. J. Bayerbach, S. E. D'Aurelio, P. van Loock, and S. Barz, Sci. Adv. **9**, eadf4080 (2023).
[31] J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).
[32] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).
[33] H. Takahashi, J. S. Neergaard-Nielsen, M. Takeuchi, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, Nat. Photonics **4**, 178 (2010).
[34] V. Giovannetti, S. Lloyd, and L. Maccone, Nat. Photonics **5**, 222 (2011).
[35] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nat. Phys. **5**, 19 (2009).
[36] J. Freund, A. Pirker, and W. Dür, Phys. Rev. Res. **6**, 033267 (2024).
[37] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
[38] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2010).
[39] A. Tavakoli, A. Pozas-Kerstjens, M.-X. Luo, and M.-O. Renou, Rep. Prog. Phys. **85**, 056001 (2022).
[40] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
[41] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: an introduction to quantum entanglement* (Cambridge University Press, 2017).
[42] M.-O. Renou, Y. Wang, S. Boreiri, S. Beigi, N. Gisin, and N. Brunner, Phys. Rev. Lett. **123**, 070403 (2019).
[43] T. Kraft, C. Ritz, N. Brunner, M. Huber, and O. Gühne, Phys. Rev. Lett. **120**, 060502 (2018).
[44] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).
[45] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[46] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *2009 50th annual IEEE symposium on foundations of computer science* (IEEE, 2009) pp. 517–526.
[47] S. Bravyi, D. Fattal, and D. Gottesman, J. Math. Phys. **47** (2006).
[48] N. Linden, S. Popescu, and W. Wootters, Phys. Rev. Lett. **89**, 207901 (2002).
[49] D. Markham, A. Miyake, and S. Virmani, New J. Phys. **9**, 194 (2007).
[50] M. Englbrecht, T. Kraft, and B. Kraus, Quantum **6**, 846 (2022).
[51] J. de Jong, F. Hahn, N. Tcholtchev, M. Hauswirth, and A. Pappa, Phys. Rev. Res. **6**, 013330 (2024).
[52] O. Collins, S. Jenkins, A. Kuzmich, and T. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).
[53] E. Shchukin, F. Schmidt, and P. van Loock, Phys. Rev. A **100**, 032322 (2019).
[54] L. T. Weinbrenner, L. Vandré, T. Coopmans, and O. Gühne, Phys. Rev. A **109**, 052611 (2024).
[55] W. Dür and H. J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).
[56] F. Rozpędek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, Phys. Rev. A **97**, 062333 (2018).
[57] J. Lockhart, O. Gühne, and S. Severini, Phys. Rev. A **97**, 062340 (2018).
[58] B. Ghimire, T. Wagner, H. Kampermann, and D. Bruß, Phys. Rev. A **107**, 042425 (2023).
[59] R. Krebs and M. Gachechiladze, Phys. Rev. Lett. **132**, 220203 (2024).
[60] C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, and G.-C. Guo, Phys. Rev. A **93**, 062329 (2016).
[61] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).
[62] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **70**, 034302 (2004).
[63] I. D. Smith, E. Wolfe, and R. W. Spekkens, arXiv preprint arXiv:2501.12320 (2025).
[64] N. Gisin, J.-D. Bancal, Y. Cai, P. Remy, A. Tavakoli, E. Zambrini Cruzeiro, S. Popescu, and N. Brunner, Nat. Commun. **11**, 2378 (2020).
[65] T. Nuradha, H. K. Mishra, F. Leditzky, and M. M. Wilde, arXiv preprint arXiv:2404.16101 (2024).

Appendix A: Protocols to achieve high GHZ fidelity

In this section, we present our construction for specific channels $\mathcal{E}_A$, $\mathcal{E}_B$, $\mathcal{E}_C$ and distributed states $\rho_{ab'}$, $\rho_{bc'}$, $\rho_{ca'}$ that yield network states ρ according to Eq. (2) with large $|\mathrm{GHZ}_3\rangle$-fidelities. Throughout this section, we denote the local dimension of the distributed states by d_{in} and the dimension of the output of the channels by d_{out}. As the target state is pure, the fidelity is a linear function and the maximal fidelity can be reached by a network state that does not make use of shared randomness. Therefore, we only have to find single channels and source states.

Using the Choi-Jamiołkowski isomorphism, the action of a channel $\mathcal{E}_A$ from input systems aa' to an output α can be written as

$$\mathcal{E}_A(\rho_{aa'}) = \mathrm{Tr}_{aa'}[\eta_A(\rho_{aa'}^T \otimes \mathbb{1}_\alpha)], \tag{A1}$$

where

$$\eta_A = \sum_{i,j,k,l=0}^{d_{\mathrm{in}}-1} |ij\rangle\langle kl|_{aa'} \otimes \mathcal{E}_A(|ij\rangle\langle kl|)_\alpha \tag{A2}$$

where η_A is the so called Choi matrix. The fact that $\mathcal{E}_A$ is a completely positive, trace preserving map translates into constraints on the Choi matrix η_A, namely

$$\eta_A \geq 0, \tag{A3}$$
$$\mathrm{Tr}_\alpha(\eta_A) = \mathbb{1}_{aa'}, \tag{A4}$$

thus, $\mathrm{Tr}(\eta_A) = d_{\mathrm{in}}^2$.

Using the Choi matrices, we can write the output state $\rho_{\alpha\beta\gamma}$ of the network as

$$\begin{aligned}\rho_{\alpha\beta\gamma} &= \mathcal{E}_A \otimes \mathcal{E}_B \otimes \mathcal{E}_C(\rho_{ab'} \otimes \rho_{bc'} \otimes \rho_{ca'}) \\ &= \mathrm{Tr}_{\substack{aa'\\bb'\\cc'}}[(\eta_A \otimes \eta_B \otimes \eta_C)(\rho_{ab'}^T \otimes \rho_{bc'}^T \otimes \rho_{ca'}^T \otimes \mathbb{1}_{\alpha\beta\gamma})].\end{aligned} \tag{A5}$$

Note that the order of systems in $\eta_A \otimes \eta_B \otimes \eta_C$ is different from the order of systems in $\rho_{ab'}^T \otimes \rho_{bc'}^T \otimes \rho_{ca'}^T \otimes \mathbb{1}_{\alpha\beta\gamma}$.

1. Grid channels

Let us introduce a framework to represent the constructed Choi matrices in a graphical way using a grid. We call the resulting maps of this construction *grid channels*, as their definition shares some similarities with the notion of grid states [57–59].

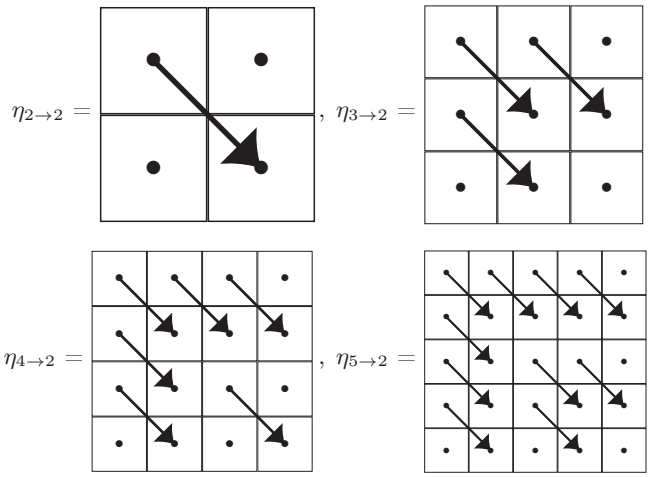


Figure 4. Visual grid representations of the Choi matrices $\eta_{d_{\mathrm{in}}\to 2}$ defined in Eqs. (A8) and (A9) that yield the fidelities with $|\mathrm{GHZ}_3\rangle$ reported in Table I. Each arrow connecting cell (i,j) to cell (k,l) corresponds to a term $\tau_{(i,j),(k,l)}$ as defined in Eq. (A6), whereas a single dot in an unconnected cell (m,n) corresponds to a term $\tau_{(m,n)}$. Note that every cell has to be covered by exactly one arrow or dot in order to obtain a trace preserving channel.

In order to form a grid channel, we represent its Choi matrix by a $d_{\text{in}} \times d_{\text{in}}$-dimensional grid as visualized in Fig. 4. We then connect the cells of the grid by arrows of different length. Each arrow of length k connecting cells $(i_0, j_0), \ldots, (i_{k-1}, j_{k-1})$ translates into a contribution of

$$\tau_{(i_0,j_0),\ldots,(i_{k-1},j_{k-1})} \coloneqq |T_{(i_0,j_0),\ldots,(i_{k-1},j_{k-1})}\rangle\langle T_{(i_0,j_0),\ldots,(i_{k-1},j_{k-1})}| \tag{A6}$$

to the Choi matrix, where

$$|T_{(i_0,j_0),\ldots,(i_{k-1},j_{k-1})}\rangle \coloneqq \sum_{l=0}^{k-1} |i_l, j_l, l\rangle\,. \tag{A7}$$

Here, the first two systems correspond to the input, whereas the third system corresponds to the output of the channel. This indicates that the maximal length of an arrow is given by the output dimension d_{out}. We do allow for arrows of length one, which are represented by a single dot. This construction inherently yields a positive semidefinite Choi matrix, fulfilling constraint (A3). The second constraint (A4), i.e. trace preservation, is ensured by covering each cell on the grid by exactly one arrow.

As an example, consider the grid in Fig. 4 for $d_{\text{in}} = d_{\text{out}} = 2$. It represents the Choi matrix

$$\eta_{2\to 2} = (|000\rangle + |111\rangle)(\langle 000| + \langle 111|) + |010\rangle\langle 010| + |100\rangle\langle 100|\,. \tag{A8}$$

2. Constructions for $d_{\text{out}} = 2$

Let us provide a construction of channels for arbitrary input dimensions and fixed output dimension $d_{\text{out}} = 2$. In Fig. 4, we show the grid representation of these channels for $d_{\text{in}} = 2, 3, 4$ and 5. However, we can generalize the construction to arbitrary input dimension via

$$\eta_{d_{\text{in}}\to 2} = \sum_{r=0}^{\lfloor \frac{d_{\text{in}}}{2} \rfloor - 1} \left[\tau_{(2r,2r),(2r+1,2r+1)} + \sum_{k=1}^{d_{\text{in}}-2-2r} \left(\tau_{(2r+k,2r),(2r+k+1,2r+1)} + \tau_{(2r,2r+k),(2r+1,2r+k+1)}\right)\right] \tag{A9}$$

In the next Appendix A 3, we analytically calculate the GHZ-fidelity that is achieved by choosing these grid-type channels as a function of the Schmidt coefficients of the input states. Here, we summarize the results of this calculation. To that end, we use Eq. (A5) to express the fidelity for a specific choice of $\eta_A = \eta_B = \eta_C \equiv \eta$ as

$$F_\eta \coloneqq \text{Tr}[\eta^{\otimes 3}(\rho^T_{ab'} \otimes \rho^T_{bc'} \otimes \rho^T_{ca'} \otimes |\text{GHZ}_3\rangle\langle \text{GHZ}_3|_{\alpha\beta\gamma})]. \tag{A10}$$

It turns out that F_η can be calculated by counting cycles of length 3 in a graph induced by the choice of grid for the Choi matrix. In fact, a guiding principle in choosing specifically the grids presented in Fig. 4 is to maximize this number of cycles, as each cycle contributes to the total fidelity.

We present a recursive expression for all input dimensions and input states $|\psi\rangle_{ab'} = |\psi\rangle_{bc'} = |\psi\rangle_{ca'} = \sum_{i=0}^{d_{\text{in}}-1} \lambda_i |ii\rangle$ in Theorem 2 in Appendix A 3 b. For $d_{\text{in}} = 2$, the fidelity reads

$$F_{\eta_{2\to 2}} = \frac{1}{2}\left(\lambda_0^6 + \lambda_1^6 + 3\lambda_0^4\lambda_1^2 + 2\lambda_0^3\lambda_1^3\right). \tag{A11}$$

Its maximal value is achieved for $\lambda_0^2 = 19/39 + 7/39(1/z^{1/3} + z^{1/3}) \approx 0.8346811596$ with $z = 71/98 + 39\sqrt{3}/98 \cdot i$ and evaluates to $[5 + 4\cos(2\pi/7)]/[12 + 4\cos(2\pi/7)] \approx 0.5170401751$. This matches the reported value in Ref. [18]. Furthermore, we checked its optimality by using a seesaw-based optimization technique using semidefinite programming, as simultaneous optimization over states and channels is not convex and thus inefficient. We thus fix five of the six matrices (three input states and three Choi matrices) and optimize only one at a time. This allows us to obtain quickly converging achievable fidelities for small input and output dimensions and confirms that our construction is likely optimal.

It is quite remarkable that in order to achieve the above-mentioned value one has to distribute weakly entangled states. In fact, fixing the input states to maximally entangled Bell pairs, we could not find any channel achieving a $|\text{GHZ}_3\rangle$-fidelity larger than 1/2 (recall that only fidelities larger than 1/2 are non-trivial, as the product state $|000\rangle$ yields already a fidelity of 1/2). This vaguely resembles effects observed in preparation schemes for four-partite cluster states, where less entangled bipartite resource states lead to higher success probabilities [60].

Also, using larger input dimensions yields an advantage: In Table I, we list the achievable $|\mathrm{GHZ}_3\rangle$-fidelity for different input dimensions. It is apparent that each additional input dimension yields an advantage. However, the fidelity quickly converges to a value slightly larger than 0.548047, thereby providing a proof of the lower bound stated in Result 1.

We give the explicit form of the resulting three-qubit state achieving this fidelity in Eq. (A25) in Appendix A 3 b. We conjecture that this is the highest $|\mathrm{GHZ}_3\rangle$-fidelity achievable in triangle LOSR networks with two-dimensional output. Furthermore, the reported values in Table I are matched by our numerical seesaw method up to input dimension $d_{\mathrm{in}} = 5$ (we could not check larger dimensions).

3. General fidelity expression for $d_{\mathrm{out}} = 2$

Let us complete the above argument by calculating an analytical expression for the obtained $|\mathrm{GHZ}_3\rangle$-fidelity with $|\mathrm{GHZ}_3\rangle$ in the triangle network with $d_{\mathrm{out}} = 2$ using the channels presented in Eq. (A9). This then provides a proof for the lower bound reported in Result 1 from the main text.

a. *Fidelity for $d_{in} = 2$*

It is illustrative to start with the simplest case of $d_{\mathrm{in}} = 2$ where

$$\eta_{2\to 2} = (|000\rangle + |111\rangle)(\langle 000| + \langle 111|) + |010\rangle\langle 010| + |100\rangle\langle 100|\,. \tag{A12}$$

Note that in this expression, the first two systems correspond to the inputs a and a', whereas the last system corresponds to the output α. We start by rearranging the expression by pulling the output system to the front and stacking the input system on top of each other, i.e., $|{}^{i}_{j}\rangle\langle{}^{k}_{l}|^{a'}_{a} := |i\rangle\langle k|_{a'} \otimes |j\rangle\langle l|_{a}$. Thus, for system A we get

$$\eta_{2\to 2} = |0\rangle\langle 0|_\alpha \otimes \left(|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{a'}_{a} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{a'}_{a} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{a'}_{a}\right) + |0\rangle\langle 1|_\alpha \otimes |{}^{0}_{0}\rangle\langle{}^{1}_{1}|^{a'}_{a} + |1\rangle\langle 0|_\alpha \otimes |{}^{1}_{1}\rangle\langle{}^{0}_{0}|^{a'}_{a} + |1\rangle\langle 1|_\alpha \otimes |{}^{1}_{1}\rangle\langle{}^{1}_{1}|^{a'}_{a}\,. \tag{A13}$$

Likewise expanding systems B and C yields

$$\begin{aligned}\eta^{\otimes 3}_{2\to 2} =& \big[\,|0\rangle\langle 0|_\alpha \otimes (|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{a'}_{a} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{a'}_{a} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{a'}_{a}) + |0\rangle\langle 1|_\alpha \otimes |{}^{0}_{0}\rangle\langle{}^{1}_{1}|^{a'}_{a} + |1\rangle\langle 0|_\alpha \otimes |{}^{1}_{1}\rangle\langle{}^{0}_{0}|^{a'}_{a} + |1\rangle\langle 1|_\alpha \otimes |{}^{1}_{1}\rangle\langle{}^{1}_{1}|^{a'}_{a}\,\big]\\ &\otimes\big[\,|0\rangle\langle 0|_\beta \otimes (|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{b'}_{b} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{b'}_{b} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{b'}_{b}) + |0\rangle\langle 1|_\beta \otimes |{}^{0}_{0}\rangle\langle{}^{1}_{1}|^{b'}_{b} + |1\rangle\langle 0|_\beta \otimes |{}^{1}_{1}\rangle\langle{}^{0}_{0}|^{b'}_{b} + |1\rangle\langle 1|_\beta \otimes |{}^{1}_{1}\rangle\langle{}^{1}_{1}|^{b'}_{b}\,\big]\\ &\otimes\big[\,|0\rangle\langle 0|_\gamma \otimes (|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{c'}_{c} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{c'}_{c} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{c'}_{c}) + |0\rangle\langle 1|_\gamma \otimes |{}^{0}_{0}\rangle\langle{}^{1}_{1}|^{c'}_{c} + |1\rangle\langle 0|_\gamma \otimes |{}^{1}_{1}\rangle\langle{}^{0}_{0}|^{c'}_{c} + |1\rangle\langle 1|_\gamma \otimes |{}^{1}_{1}\rangle\langle{}^{1}_{1}|^{c'}_{c}\,\big].\end{aligned} \tag{A14}$$

The input states are chosen to be given in the Schmidt diagonal form

$$|\psi\rangle\langle\psi|^{\otimes 3} = |\psi\rangle\langle\psi|^{a}_{b'} \otimes |\psi\rangle\langle\psi|^{b}_{c'} \otimes |\psi\rangle\langle\psi|^{c}_{a'} \tag{A15}$$

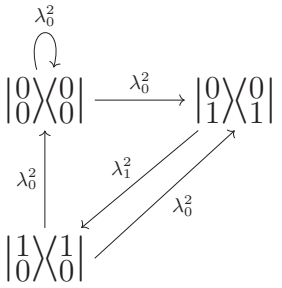
with $|\psi\rangle^{a}_{b'} = \lambda_0\,|0\rangle^{a}_{b'} + \lambda_1\,|1\rangle^{a}_{b'}$, where the Schmidt coefficients λ_i are real valued, and we will be taking the expectation value of the output with the GHZ state $|\mathrm{GHZ}_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{\alpha\beta\gamma} + |111\rangle_{\alpha\beta\gamma})$ to form the fidelity

$$F_{\eta_{2\to 2}} = \langle \mathrm{GHZ}_3|\,\eta^{\otimes 3}_{2\to 2}\,|\psi\rangle\langle\psi|^{\otimes 3}\,|\mathrm{GHZ}_3\rangle\,. \tag{A16}$$

Note that we can omit the transposition of the input states as they are chosen to be real-valued. Due to the symmetries of the GHZ state, when considering the expansion of the expression in Eq. (A14), only terms survive which have matching entries in the α, β and γ components. In other words, we are only allowed to expand along the four columns in that expression.

We will consider the four contributions to the fidelity individually, starting with

$$\langle 000|_{\alpha\beta\gamma}\,\eta^{\otimes 3}_{2\to 2}\,|\psi\rangle\langle\psi|^{\otimes 3}\,|000\rangle_{\alpha\beta\gamma} = \begin{matrix}\langle\psi|^{a}_{b'}\\ \otimes\\ \langle\psi|^{b}_{c'}\\ \otimes\\ \langle\psi|^{c}_{a'}\end{matrix}\begin{pmatrix}(|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{a'}_{a} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{a'}_{a} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{a'}_{a})\\ \otimes\\ (|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{b'}_{b} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{b'}_{b} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{b'}_{b})\\ \otimes\\ (|{}^{0}_{0}\rangle\langle{}^{0}_{0}|^{c'}_{c} + |{}^{0}_{1}\rangle\langle{}^{0}_{1}|^{c'}_{c} + |{}^{1}_{0}\rangle\langle{}^{1}_{0}|^{c'}_{c})\end{pmatrix}\begin{matrix}|\psi\rangle^{a}_{b'}\\ \otimes\\ |\psi\rangle^{b}_{c'}\\ \otimes\\ |\psi\rangle^{c}_{a'}\end{matrix}. \tag{A17}$$



Cycle	Multiplicity	Contribution
$\|0\rangle\langle 0\|_0 \to \|0\rangle\langle 0\|_0 \to \|0\rangle\langle 0\|_0$	1	λ_0^6
$\|0\rangle\langle 0\|_0 \to \|0\rangle\langle 0\|_1 \to \|1\rangle\langle 1\|_0$	3	$\lambda_0^4\lambda_1^2$

Figure 5. Left: The directed graph used to compute the contribution in Eq. (A18) to the $|\mathrm{GHZ}_3\rangle$-fidelity yielded by the construction using the Choi matrices from Eq. (A12). Right: The cycles of size three of the graph on the left. The contribution to the $|\mathrm{GHZ}_3\rangle$-fidelity is determined by those cycles, where each of them contributes the product of its edge labels.

We have offset the contraction with the input states to indicate that they connect between the rows of the expansion of the Choi matrices. Now, due to the symmetries of the Schmidt diagonal $|\psi\rangle = \lambda_0 |0\rangle_0^0 + \lambda_1 |1\rangle_1^1$, when expanding Eq. (A17), only terms survive where we select terms from the Choi matrix where the entries of the a input and the b' input match, and likewise for b and c', and c and a'. This can be represented as a directed graph indicating allowed contractions as displayed in Fig. 5, where we label the edges with the corresponding λ_i factor. Now, the complete contribution of $\langle 000|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |000\rangle_{\alpha\beta\gamma}$ corresponds to the sum of products of edge labels of all cycles of length three in that graph. For the graph at hand, the three-cycles and the corresponding factors are indicated in the table on the right-hand side of Fig. 5. Note that the second cycle comes with a factor of three as it can be started at any of its nodes. Counting these contributions, we get

$$\langle 000|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |000\rangle_{\alpha\beta\gamma} = \lambda_0^6 + 3\lambda_0^4\lambda_1^2. \tag{A18}$$

Next, we consider the contribution

$$\langle 111|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |111\rangle_{\alpha\beta\gamma} = \begin{matrix} \langle\psi|_{b'}^{a} \\ \otimes \\ \langle\psi|_{c'}^{b} \\ \otimes \\ \langle\psi|_{a'}^{c} \end{matrix} \begin{pmatrix} |1\rangle\langle 1|_a^{a'} \\ \otimes \\ |1\rangle\langle 1|_b^{b'} \\ \otimes \\ |1\rangle\langle 1|_c^{c'} \end{pmatrix} \begin{matrix} |\psi\rangle_{b'}^{a} \\ \otimes \\ |\psi\rangle_{c'}^{b} \\ \otimes \\ |\psi\rangle_{a'}^{c} \end{matrix} . \tag{A19}$$

The corresponding trivial graph consists of only one node connected to itself, yielding the contribution of

$$\langle 111|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |111\rangle_{\alpha\beta\gamma} = \lambda_1^6. \tag{A20}$$

Likewise, for $\langle 000|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |111\rangle_{\alpha\beta\gamma}$ and $\langle 111|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |000\rangle_{\alpha\beta\gamma}$, we get a contribution of $\lambda_0^3\lambda_1^3$ each. Summing all contributions to form the fidelity, we get the expression reported in Eq. (A11):

$$\begin{aligned} F_{\eta_{2\to 2}} &= \frac{1}{2}(\langle 000|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |000\rangle_{\alpha\beta\gamma} + \langle 000|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |111\rangle_{\alpha\beta\gamma} \\ &\quad + \langle 111|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |000\rangle_{\alpha\beta\gamma} + \langle 111|_{\alpha\beta\gamma} \eta_{2\to 2}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |111\rangle_{\alpha\beta\gamma}) \\ &= \frac{1}{2}\left(\lambda_0^6 + \lambda_1^6 + 3\lambda_0^4\lambda_1^2 + 2\lambda_0^3\lambda_1^3\right). \end{aligned} \tag{A21}$$

This expression can be maximized under the normalization constraint of $\lambda_0^2 + \lambda_1^2 = 1$, yielding a value of $F_{\eta_{2\to 2}} = [5 + 4\cos(2\pi/7)]/[12 + 4\cos(2\pi/7)] \approx 0.5170401751642$, achieved by input states with Schmidt coefficients $\lambda_0 \approx 0.913608866$ and $\lambda_1 \approx 0.406594196$.

b. *Fidelities for $d_{in} > 2$*

Let us now generalize the argument to higher dimensional input states using the Choi maps displayed in Fig. 4 and defined by Eq. (A9), which we repeat here for convenience:

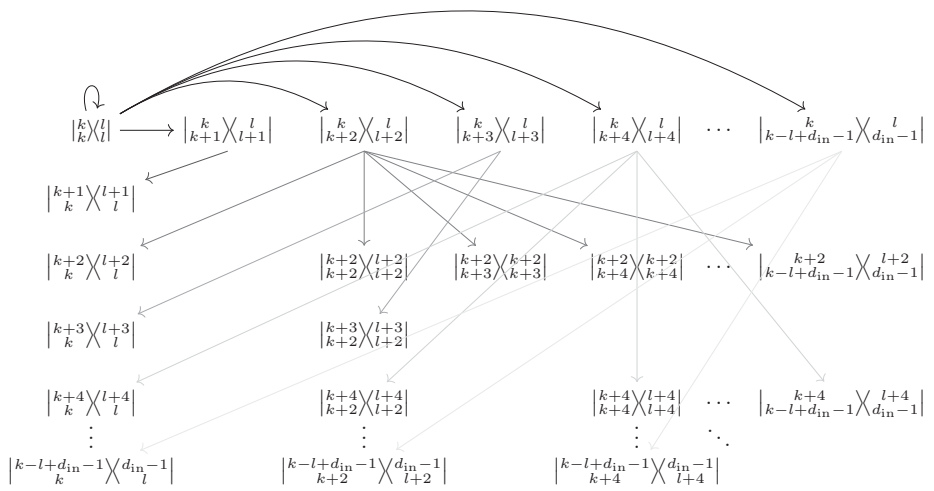


Figure 6. Part of the directed graph used to determine the $|\mathrm{GHZ}_3\rangle$-fidelity contribution $\langle kkk|_{\alpha\beta\gamma}\,\eta_{d_{\mathrm{in}}\to 2}^{\otimes 3}\,|\psi\rangle\langle\psi|^{\otimes 3}\,|lll\rangle_{\alpha\beta\gamma}$ using the Choi matrices from Eq. (A22) for fixed $k \leq l \in \{0,1\}$. The contribution is given by all three-cycles in this graph. For clarity, we only display the edges from the first line of nodes. In general, a node in the r'th column is connected to each node in the r'th row. The form of three-cycles in a graph with this structure is given by Eq. (A23).

$$\eta_{d_{\mathrm{in}}\to 2} = \sum_{r=0}^{\lfloor \frac{d_{\mathrm{in}}}{2} \rfloor - 1} \left[\tau_{(2r,2r),(2r+1,2r+1)} + \sum_{k=1}^{d_{\mathrm{in}}-2-2r} \left(\tau_{(2r+k,2r),(2r+k+1,2r+1)} + \tau_{(2r,2r+k),(2r+1,2r+k+1)} \right) \right]. \tag{A22}$$

Expanding the threefold tensor product of this Choi map and taking the expectation value with $|\mathrm{GHZ}_3\rangle$, we can again separate four contributions which can be translated into directed graphs that represent the selection rules due to the Schmidt diagonality of the input states $|\psi\rangle = \sum_{i=0}^{d-1} \lambda_i\,|ii\rangle$. We display the corresponding graph for the contribution $\langle kkk|_{\alpha\beta\gamma}\,\eta_{d_{\mathrm{in}}\to 2}^{\otimes 3}\,|\psi\rangle\langle\psi|^{\otimes 3}\,|lll\rangle_{\alpha\beta\gamma}$ for fixed $k \leq l \in \{0,1\}$ in Fig. 6, where we only display the edges from the nodes in the first row for clarity. In fact, it is helpful to notice that a node in the r'th column can connect to any node in the r'th row. This demands that any three-cycle is of the form

$$\left|{}^{k+r}_{k+s}\right\rangle\!\!\left\langle{}^{l+r}_{l+s}\right| \to \left|{}^{k+s}_{k+t}\right\rangle\!\!\left\langle{}^{l+s}_{l+t}\right| \to \left|{}^{k+t}_{k+r}\right\rangle\!\!\left\langle{}^{l+t}_{l+r}\right| \tag{A23}$$

for suitable choices of r, s, t.

Carefully counting all such cycles that connect the nodes in the last column and row, i.e., where one of the entries equals $d_{\mathrm{in}} - 1$, allows us to relate the corresponding fidelity contributions for dimension d_{in} to that of $d_{\mathrm{in}} - 1$. Doing so for all choices of k and l, we obtain:

Theorem 2. *For symmetric pure input states $|\psi\rangle_{ab'} = |\psi\rangle_{bc'} = |\psi\rangle_{ca'} = \sum_{i=0}^{d_{in}-1} \lambda_i\,|ii\rangle$ and local channels $\mathcal{E}_A = \mathcal{E}_B = \mathcal{E}_C$ represented by the Choi matrix $\eta_{d_{in}\to 2}$ in Eq. (A9), the fidelity with $|GHZ_3\rangle$ is given by the recursive rule*

$$F_{\eta_{d_{in}\to 2}} = F_{\eta_{d_{in-1}\to 2}} + \frac{1}{2} \begin{cases} \lambda_{d_{in}-1}^6 + 2\lambda_{d_{in}-1}^3\lambda_{d_{in}-2}^3 + 3\lambda_{d_{in}-1}^2\Big(\sum\limits_{r,s=0,2,\ldots}^{d_{in}-2} \lambda_r^2\lambda_s^2 + \sum\limits_{r=1,3,\ldots}^{d_{in}-3}\sum\limits_{s=1,3,\ldots}^{d_{in}-1} \lambda_r^2\lambda_s^2\Big) + \\ \qquad +6\lambda_{d_{in}-1}\lambda_{d_{in}-2} \sum\limits_{r=1,3,\ldots}^{d_{in}-3}\sum\limits_{s=1,3,\ldots}^{d_{in}-1} \lambda_r\lambda_{r-1}\lambda_s\lambda_{s-1} \quad \textit{if } d_{in} \textit{ even}, \\ \lambda_{d_{in}-1}^6 + 3\lambda_{d_{in}-1}^2\Big(\sum\limits_{r=0,2,\ldots}^{d_{in}-3}\sum\limits_{s=0,2,\ldots}^{d_{in}-1} \lambda_r^2\lambda_s^2 + \sum\limits_{r,s=1,3,\ldots}^{d_{in}-2} \lambda_r^2\lambda_s^2\Big) + \\ \qquad +6\lambda_{d_{in}-1}\lambda_{d_{in}-2} \sum\limits_{r,s=1,3,\ldots}^{d_{in}-2} \lambda_r\lambda_{r-1}\lambda_s\lambda_{s-1} \quad \textit{if } d_{in} \textit{ odd} \end{cases} \tag{A24}$$

d_{in}	max. $F_{\eta_{d_{\text{in}}\to 2}}$	max. Schmidt coefficients
2	0.51704017	(0.91361, 0.40659)
3	0.54009112	(0.82466, 0.52659, 0.20646)
4	0.54595881	(0.79959, 0.54155, 0.24057, 0.09750)
5	0.54749297	(0.79038, 0.54384, 0.24871, 0.12321, 0.04991)
6	0.54790031	(0.78708, 0.54412, 0.25072, 0.13021, 0.06302, 0.02561)
7	0.54800887	(0.78595, 0.54411, 0.25121, 0.13214, 0.06655, 0.03247, 0.01320)
8	0.54803772	(0.78559, 0.54408, 0.25133, 0.13268, 0.06750, 0.03430, 0.01671, 0.00680)
9	0.54804537	(0.78547, 0.54407, 0.25136, 0.13282, 0.06775, 0.03480, 0.01764, 0.00860, 0.00350)
10	0.54804739	(0.78544, 0.54407, 0.25136, 0.13286, 0.06782, 0.03492, 0.01789, 0.00908, 0.00442, 0.00180)

Table I. Optimal Schmidt coefficients of the bipartite input states and associated obtained $|\text{GHZ}_3\rangle$-fidelities for different input dimensions d_{in} when using the construction based on the Choi matrices in Eq. (A22).

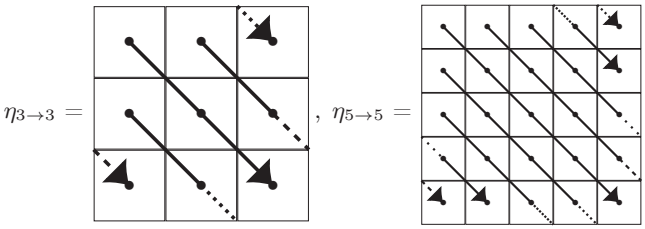


Figure 7. The grid representation of the Choi matrices $\eta_{d_{\text{out}}\to d_{\text{out}}}$ for $d_{\text{out}} = 3$ and $d_{\text{out}} = 5$ of the grid channels defined in Eq. (A26). Note that this construction only works for odd dimensions and yields the fidelities with $|\text{GHZ}_{3,d_{\text{out}}}\rangle$ reported in Eq. (A28).

and the fidelity $F_{\eta_{2\to 2}}$ *is given by Eq.* (A11).

Maximizing these polynomials under the normalization condition of the Schmidt coefficients λ, we obtain the fidelity values and maximizing squared Schmidt coefficients given in Table I.

Finally, let us explicitly state the output of the constructed channels, i.e., the state that achieves the reported fidelities for $d_{\text{in}} = 10$ up to four digits of precision:

$$\rho_{\alpha\beta\gamma}^{d_{\text{in}}=10} = \begin{pmatrix} 0.6858 & 0 & 0 & 0 & 0 & 0 & 0 & 0.1805 \\ 0 & 0.0862 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.0862 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.0021 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.0862 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.0021 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.0021 & 0 \\ 0.1805 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0493 \end{pmatrix} \tag{A25}$$

4. Constructions for odd $d_{\text{out}} > 2$

Let us shift our attention to higher-dimensional outputs of three-partite networks. For a general output dimension of d_{out}, an output fidelity of more than $1/d_{\text{out}}$ with $|\text{GHZ}_{3,d_{\text{out}}}\rangle$ indicates genuine multipartite entanglement [40].

We first consider the case of odd d_{out} and the same input dimension, as numerical search indicates that curiously, in contrast to the case of $d_{\text{out}} = 2$, in case of $d_{\text{out}} = 3$, the fidelity seems to saturate as soon as $d_{\text{in}} = d_{\text{out}}$. For this case, we can produce probably highest fidelities by choosing the grid-type Choi matrices presented in Fig. 7, and for general odd dimension d_{out} given explicitly by

$$\begin{aligned} \eta_{d_{\text{out}}\to d_{\text{out}}} = {} & \tau_{(0,0),(1,1),\ldots,(d_{\text{out}}-1,d_{\text{out}}-1)} + \\ & \sum_{r=1}^{\frac{d_{\text{out}}-1}{2}} \big(\tau_{(0,r),(1,r\oplus 1),\ldots(d_{\text{out}}-1,r\oplus(d_{\text{out}}-1))} + \\ & \tau_{(r,0),(r\oplus 1,1),\ldots(r\oplus(d_{\text{out}}-1),d_{\text{out}}-1)}\big), \end{aligned} \tag{A26}$$

where $\oplus$ denotes addition modulo d_{out}.

In the subsequent Appendix A 5, we calculate the fidelity (as a function of the Schmidt coefficients of the input states) for this construction by counting again cycles in an induced graph, yielding

$$F_{\eta_{d_{\text{out}}\to d_{\text{out}}}} = \frac{1}{d_{\text{out}}} \sum_{k,l=0}^{d_{\text{out}}-1} \left(\lambda_k^3 \lambda_l^3 + 3\lambda_k^2 \lambda_l^2 \sum_{i=1}^{\frac{d_{\text{out}}-1}{2}} \lambda_{k\oplus i} \lambda_{l\oplus i} \right). \tag{A27}$$

In contrast to $d_{\text{out}} = 2$, in this case the optimal values for the Schmidt coefficients is given by $\lambda_i = 1/\sqrt{d_{\text{out}}}$, i.e., maximally entangled input states. From the calculation in Appendix A 5, we get an achievable fidelity of

$$F_{\eta_{d_{\text{out}}\to d_{\text{out}}}} = \frac{3d_{\text{out}} - 1}{2d_{\text{out}}^2} = \frac{1}{d_{\text{out}}} \left(\frac{3}{2} - \frac{1}{2d_{\text{out}}} \right) \tag{A28}$$

by using the channels in Eq. (A26) and maximally entangled bipartite inputs of dimension $d_{\text{in}} = d_{\text{out}}$.

These fidelities numbers are matched by numerical seesaw search for $d_{\text{out}} = 3$. Interestingly, for $d_{\text{out}} = 5$, there seem to exist better channels which slightly exceed the fidelity of 0.28 that is reached by our construction.

Note that the achieved fidelity exceeds the bound of $1/d_{\text{out}}$ (and approaches a value of $3/(2d_{\text{out}})$ for large dimensions), therefore demonstrating genuine multipartite entanglement for all dimensions. Interestingly, choosing $\lambda_0 = \sqrt{1-\epsilon^2}, \lambda_1 = \epsilon$ and $\lambda_{i>1} = 0$ yields already a fidelity value exceeding the GME bound, thus, even very weakly entangled input states can be mapped to a GME state.

While this construction does not work for even output dimensions d_{out}, we can lift the construction in dimension $d_{\text{out}} - 1$ to dimension d_{out} by simply dismissing the extra dimension. Denoting the constructed $d_{\text{out}} - 1$ dimensional network state by ρ, we get

$$\langle \text{GHZ}_{3,d_{\text{out}}} | \rho | \text{GHZ}_{3,d_{\text{out}}} \rangle = \frac{d_{\text{out}} - 1}{d_{\text{out}}} \langle \text{GHZ}_{3,d_{\text{out}}-1} | \rho | \text{GHZ}_{3,d_{\text{out}}-1} \rangle = \frac{1}{d_{\text{out}}} \left(\frac{3}{2} - \frac{1}{2(d_{\text{out}} - 1)} \right) \tag{A29}$$

for even d_{out}.

Together with the value presented in Eq. (A28), this proves the lower bound reported in Result 2 in the main text.

5. General fidelity expression for $d_{\text{out}} > 2$

Here we derive Eq. (A27) from the previous section by calculating the reachable fidelity with $|\text{GHZ}_{3,d_{\text{out}}}\rangle$ using the construction specified in Fig. 7 and Eq. (A26), which reads

$$\eta_{d_{\text{out}}\to d_{\text{out}}} = \tau_{(0,0),(1,1),\ldots,(d_{\text{out}}-1,d_{\text{out}}-1)} + \sum_{r=1}^{\frac{d_{\text{out}}-1}{2}} \left(\tau_{(0,r),(1,r\oplus 1),\ldots(d_{\text{out}}-1,r\oplus(d_{\text{out}}-1))} + \tau_{(r,0),(r\oplus 1,1),\ldots(r\oplus(d_{\text{out}}-1),d_{\text{out}}-1)} \right). \tag{A30}$$

Just as in the case of the analysis of $d_{\text{out}} = 2$, we can split the fidelity with $|\text{GHZ}_{3,d_{\text{out}}}\rangle$ into d_{out}^2 terms of the form $\langle kkk|_{\alpha\beta\gamma} \eta_{d_{\text{out}}\to d_{\text{out}}}^{\otimes 3} |\psi\rangle\langle\psi|^{\otimes 3} |lll\rangle_{\alpha\beta\gamma}$ for $k, l = 0, \ldots, d_{\text{out}} - 1$ and some input state $|\psi\rangle = \sum_{i=0}^{d_{\text{out}}-1} \lambda_i |ii\rangle$.

Expanding the contribution for some fixed choice of k and l leads to the graph shown in Fig. 8. Its three-cycles are of the form

$$\left|\begin{smallmatrix} k \\ k \end{smallmatrix}\right\rangle\!\left\langle\begin{smallmatrix} l \\ l \end{smallmatrix}\right| \to \left|\begin{smallmatrix} k \\ k\oplus i \end{smallmatrix}\right\rangle\!\left\langle\begin{smallmatrix} l \\ l\oplus i \end{smallmatrix}\right| \to \left|\begin{smallmatrix} k\oplus i \\ k \end{smallmatrix}\right\rangle\!\left\langle\begin{smallmatrix} l\oplus i \\ l \end{smallmatrix}\right| \tag{A31}$$

for $i = 0, \ldots, \delta := (d_{\text{out}} - 1)/2$. Note that whenever $i \neq 0$, we have to count the cycle three times as it may start at any of its nodes, and each cycle contributes $\lambda_k^2 \lambda_l^2 \lambda_{k\oplus i} \lambda_{l\oplus i}$ to the total fidelity.

Summing the contributions of all three-cycles for all k and l and taking into account the normalization of the GHZ state, we obtain the result reported in Eq. (A27):

$$F_{\eta_{d_{\text{out}}\to d_{\text{out}}}} = \frac{1}{d_{\text{out}}} \sum_{k,l=0}^{d_{\text{out}}-1} \left(\lambda_k^3 \lambda_l^3 + 3\lambda_k^2 \lambda_l^2 \sum_{i=1}^{\frac{d_{\text{out}}-1}{2}} \lambda_{k\oplus i} \lambda_{l\oplus i} \right). \tag{A32}$$

In contrast to the case of $d_{\text{out}} = 2$, in this case, the optimum seems to be achieved for $\lambda_i = 1/\sqrt{d_{\text{out}}}$ for all i, for which the fidelity reaches the value reported in Eq. (A28) of

$$F_{\eta_{d_{\text{out}}\to d_{\text{out}}}} = \frac{3d_{\text{out}} - 1}{2d_{\text{out}}^2}. \tag{A33}$$

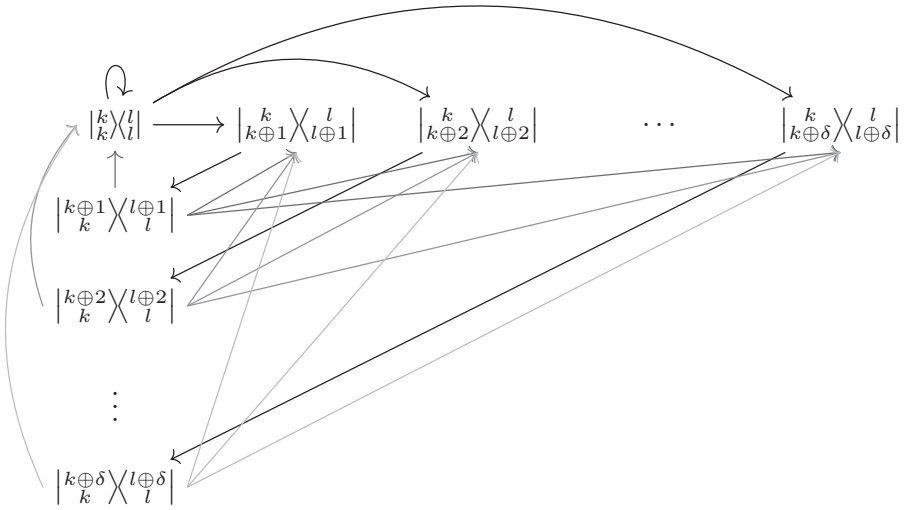


Figure 8. The directed graph used to determine the $|\mathrm{GHZ}_{3,d_{\mathrm{out}}}\rangle$-fidelity of the construction using Choi matrices in Eq. (A30) for odd d_{out}, where $\delta = (d_{\mathrm{out}} - 1)/2$ and $k, l = 0, \ldots, d_{\mathrm{out}} - 1$. As before, the fidelity is determined by three-cycles in this graph, which are of the form in Eq. (A31).

Appendix B: Fidelity bounds in larger networks from bounds in triangular networks

1. Reducing fidelity bounds in large networks to smaller ones

In order to find fidelity bounds for states in LOSR with N nodes, bipartite sources, it is often possible to reduce this task to finding bounds in smaller networks. Intuitively, the idea is to group nodes in the N-partite network and allow them to perform a unitary post-processing, followed by tracing out all but one node per group. This procedure can only lead to higher fidelities with the target state while at the same time producing a network state of fewer parties. We formally prove this argument in the following lemma.

Lemma 3 (State extraction)**.** *Let $|\psi_N\rangle$ be an N-partite quantum state of local dimension d. Let the N parties be partitioned into $n \geq 3$ sets $A_1, \ldots, A_n$.*

If there exist unitary operators U_{A_i} acting only on the parties in A_i for $i = 1, \ldots, n$ such that

$$U_{A_1} \otimes \ldots \otimes U_{A_n} |\psi_N\rangle = |\varphi_n\rangle_{a_1,\ldots a_n} \otimes |\tau\rangle_R \,, \tag{B1}$$

where $|\varphi_n\rangle$ is an n-partite state of parties $a_1 \in A_1, \ldots, a_n \in A_n$, and where $|\tau\rangle_R$ is a residual state on the parties in $R = \{1, \ldots, N\} \setminus \{a_1, \ldots a_n\}$, then the maximal fidelity of LOSR-states in N-partite networks with $|\psi_N\rangle$ cannot be larger than that of LOSR-states in n-partite networks with $|\varphi_n\rangle$, i.e.,

$$F_{LOSR}(|\psi_N\rangle) \leq F_{LOSR}(|\varphi_n\rangle). \tag{B2}$$

Proof. For clarity, we prove the statement for N parties, partitioned into three sets $A_1 = A$, $A_2 = B$, $A_3 = C$. The argument can then directly be extended to larger n.

To prove the statement, we consider the larger class of N-partite LOSR networks with bipartite sources between all parties, where now the parties in A, B and C are allowed to apply set-local unitaries U_A, U_B and U_C, respectively, to their outputs (see Fig. 9). Let us denote this class by $\underline{\mathrm{LOSR}}_d^N$. Clearly, the maximal fidelity achievable in the usual N-partite LOSR network cannot exceed the one obtainable in the $\underline{\mathrm{LOSR}}$ network. Let ρ denote a state in LOSR.

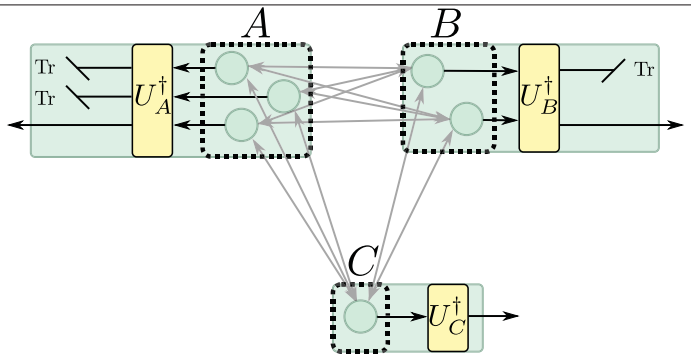


Figure 9. Visualization of the proof of Lemma 3 for the tripartition $A = \{1, 2, 3\}$, $B = \{4, 5\}$, $C = \{6\}$. The 6-partite network can be used to create a tripartite network by applying local unitaries U_A, U_B and U_C and then tracing out all but one party per set. If a 6-partite state $|\psi_6\rangle$ can be transformed using the unitaries U_A, U_B and U_C into a 3-partite state $|\varphi_3\rangle$ between some parties in A, B and C (and some residual state), then the fidelity with $|\psi_6\rangle$ in the full network is upper bounded by the fidelity with $|\varphi_3\rangle$ in the tripartite network.

Then its fidelity with $|\psi_N\rangle$ is given by

$$
\begin{aligned}
F' &= \langle\psi_N|\rho|\psi_N\rangle && \text{(B3)}\\
&\leq \max_{\rho'\in\underline{\text{LOSR}}} \langle\psi_N|\rho'|\psi_N\rangle && \text{(B4)}\\
&= \max_{\rho'\in\underline{\text{LOSR}}} \langle\psi_N|\big(U_A^\dagger\otimes U_B^\dagger\otimes U_C^\dagger\big)\rho'\big(U_A\otimes U_B\otimes U_C\big)|\psi_N\rangle && \text{(B5)}\\
&= \max_{\rho'\in\underline{\text{LOSR}}} \langle\varphi_3|\otimes\langle\tau|\,\rho'\,|\varphi_3\rangle\otimes|\tau\rangle && \text{(B6)}\\
&\leq \max_{\rho'\in\underline{\text{LOSR}}} \langle\varphi_3|\,\mathrm{Tr}_R(\rho')|\varphi_3\rangle && \text{(B7)}\\
&\leq F_{\text{LOSR}}(|\varphi_3\rangle). && \text{(B8)}
\end{aligned}
$$

The second-last inequality follows from the fact that the fidelity between two states can only increase under the partial trace. Finally, the last inequality follows from the fact that the state $\mathrm{Tr}_R(\rho')$ is preparable in a tripartite LOSR network. To see this, we combine the nodes in A (and likewise for B and C) into a single node. The channels of these nodes are then given by first applying the original parties' channels, followed by the unitary post-processing and the subsequent partial trace. Additionally, the bipartite sources connecting the parties in A and B are combined into a single (larger-dimensional) bipartite source between A and B, and likewise for the other two pairs. □

Let us stress that this proof also bounds the fidelities for a larger class of networks, where instead of having bipartite sources between all parties, we allow even for multipartite sources connecting the parties in each pair of sets A_i and A_j for $1 \leq i < j \leq n$.

An immediate application of Lemma 3 concerns the fidelity LOSR-states with GHZ states:

Corollary 4. *For all* $3 \leq n < N$,

$$
F_{LOSR}(|GHZ_{N,d}\rangle) \leq F_{LOSR}(|GHZ_{n,d}\rangle) \tag{B9}
$$

Proof. We use Lemma 3 and choose $|\psi_N\rangle = |\mathrm{GHZ}_{N,d}\rangle$ and $|\varphi_n\rangle = |\mathrm{GHZ}_{N,d}\rangle$. We further choose $A_1 = \{1\}, A_2 = \{2\}, \ldots, A_{n-1} = \{n-1\}$ and $A_n = \{n, n+1, \ldots, N\}$, such that $|A_n| = N - n + 1$.

Finally, we set $U_i = \mathbb{1}$ for $1 \leq i \leq n-1$ and U_n such that $U_n\,|i\rangle^{\otimes(N-n+1)} = |i\rangle\otimes|0\rangle^{\otimes(N-n)}$ for $0 \leq i < d$. This yields

$$
U_1\otimes\ldots\otimes U_n\,|\mathrm{GHZ}_{N,d}\rangle = |\mathrm{GHZ}_{n,d}\rangle\otimes|0\rangle^{\otimes(N-n)}\,. \tag{B10}
$$

The claim then follows from Lemma 3. □

2. Bounding fidelities of graph states

We now shift our attention to graph states [37, 44, 45]. This family of multipartite states has found ubiquitous applications in quantum information theory and quantum computing and includes prominent examples of states like the multipartite GHZ state, as well as cluster states, which are resource states for measurement based quantum computation [45]. Furthermore, each stabilizer state is locally equivalent to a graph state [61], which makes the results of this section applicable to them as well.

Previous results have shown that no connected graph state can be prepared in LOSR networks with arbitrary bipartite sources with fidelities exceeding 9/10 [22, 23]. Here, we improve this result for all graph states. For a comprehensive introduction to the graph state formalism, see, for example, Ref. [37]. Here, we just state the basic facts required for our argument.

a. Graph state preliminaries

Let us now consider the case of graph states, for which we start by stating the basic definitions and proving some useful Lemmas.

A graph state $|G\rangle$ of N qubits is defined via a graph $G = (V, E)$ of N vertices $V = \{1, \ldots, N\}$ and edges $E \subset V \times V$ between them via

$$|G\rangle = \prod_{(i,j)\in E} \mathrm{CZ}_{i,j} \, |+\rangle^{\otimes N} , \tag{B11}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and

$$\mathrm{CZ}_{i,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}_{i,j} \otimes \mathbb{1}_{\{1,\ldots,N\}\setminus\{i,j\}} \tag{B12}$$

denotes the self-inverse controlled-Z operation on qubits i and j. Note that due to the one-to-one correspondence of graphs and graph states, we sometimes use G and $|G\rangle$ interchangeably.

Of general interest is the question of when two graph states $|G\rangle$ and $|G'\rangle$ are locally equivalent, i.e., whether there exists a (local) unitary transformation $U = U_1 \otimes U_2 \otimes \ldots \otimes U_N$, such that $U\,|G\rangle = |G'\rangle$. In many cases, this can be checked by considering local complementations of the associated graph G. Denoting the neighborhood of an vertex v in G by $\boldsymbol{N}(v, G) = \{i \in V \,:\, (i, v) \in E\}$, the local complementation τ_v with respect to v can be graphically interpreted as inverting every edge in the neighborhood of v. If two vertices in the neighborhood of v are connected in G, this edge will be removed in $\tau_v(G)$, and vice versa. Mathematically, a local complementation τ_v w.r.t. a vertex $v \in V$ transforms the graph $G = (V, E)$ into the graph $G' = (V, E')$, where $E' = (E \setminus \{(i, j) \,:\, i, j \in \boldsymbol{N}(v, G) \wedge (i, j) \in E\}) \cup \{(i, j) \,:\, i, j \in \boldsymbol{N}(v, G) \wedge (i, j) \notin E\}$.

We note here that applying the controlled-Z operation $\mathrm{CZ}_{i,j}$ to the graph state $|G\rangle$ gives a graph state $|G'\rangle$, where G' has the same vertices and edges as G, except for the edge between the vertices i and j. If the edge (i, j) is present in G, it will be absent in G' and vice versa. Thus, the action of a local complementation on a graph state $|G\rangle$ can be written equivalently in terms of controlled-Z operations as

$$\tau_v(|G\rangle) = \prod_{k,l\in\boldsymbol{N}(v,G),k<l} \mathrm{CZ}_{k,l} \, |G\rangle \, . \tag{B13}$$

The relevance of local complementations is then given by the following result:

Theorem 5 ([37, 62])**.** *If a sequence of local complementations $\tau_{v_1} \ldots \tau_{v_k}$ transforms the graph G into G', then the corresponding graph states $|G\rangle$ and $|G'\rangle$ are locally equivalent.*

In the next section, we make use of a special case of the commutation relation between the local complementation operations and the controlled-Z operations. In the following, we will use the notion of removing a vertex v of a graph G, which can be seen as deleting all edges to v in the graph G. Using the notation

$$\mathrm{CZ}_{M,v} \coloneqq \prod_{j\in M} \mathrm{CZ}_{j,v} \tag{B14}$$

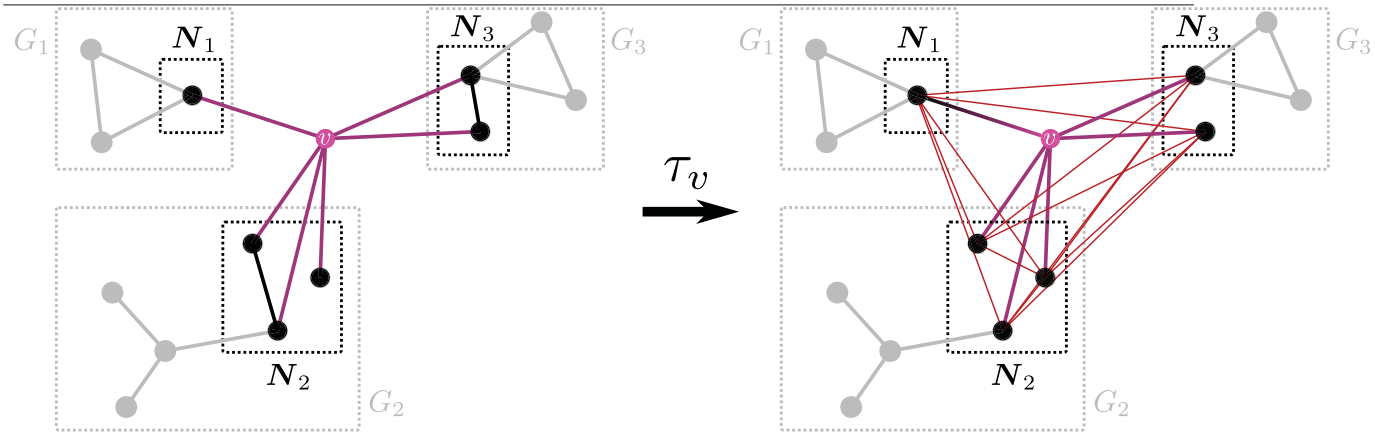


Figure 10. Left: visualization of an articulation point v in a graph which connects the three components G_1, G_2 and G_3. The neighborhood of v inside G_i is denoted by $\boldsymbol{N}_i$. Right: the same graph after a local complementation of v. Even though some edges within the neighborhood are removed, all vertices remain connected after v is removed. Thus, v is not an articulation point anymore.

for any subset M of the vertices, the deletion of all edges to the vertex v in the graph G leads to the graph state $\mathrm{CZ}_{\boldsymbol{N}(v,G),v}\,|G\rangle$. Interestingly, this action commutes with local complementations on vertices unequal to v. Since a local complementation τ_j may only create and delete edges to v, it is clear that first deleting all edges to v in the graph G and then applying the local complementation τ_j has the same effect as deleting all edges to v in the graph $\tau_j(G)$ obtained by applying the local complementation first. Since also all controlled-Z operations commute, we arrive at the following lemma:

Lemma 6. *For any graph state $|G\rangle$, one of its vertices v and a sequence U of controlled-Z gates and local complementations of vertices unequal to v, it holds that*

$$U\,\mathrm{CZ}_{\boldsymbol{N}(v,G),v}\,|G\rangle = \mathrm{CZ}_{\boldsymbol{N}(v,UG),v}\,U\,|G\rangle\,. \tag{B15}$$

As a final ingredient, we need the following observation regarding articulation points of a graph, which are vertices such that their removal increases the number of components of the graph:

Lemma 7. *Let $G=(V,E)$ be a connected graph and $v\in V$ be an articulation point of G. Then v is not an articulation point in the graph $\tau_v(G)$.*

Proof. We have to show that there exists a path between any pair of vertices $x\neq v, y\neq v$ in $G' \coloneqq \tau_v(G)\setminus\{v\}$.

As v is an articulation point, its removal splits G into $k\geq 2$ components $G_1,\ldots,G_k$ which are not connected to each other. Denote the neighborhood of v in G as before by $\boldsymbol{N}(v,G)$ and define $\boldsymbol{N}_j \coloneqq G_j\cap\boldsymbol{N}(v,G)$ for $1\leq j\leq k$ as the part of G_j that is connected to v (see Fig. 10). Note that in G', for all $1\leq i<j\leq k$, all vertices in $\boldsymbol{N}_i$ are connected to all vertices in $\boldsymbol{N}_j$ due to the local complementation.

Now we consider different cases for x and y.

Case 1 ($x\in G_i\ni y$)**:** Then x and y are connected in G via a path within G_i. This path might contain edges within $\boldsymbol{N}_i$ which got removed due to the local complementation. However, since all vertices in $\boldsymbol{N}_i$ are connected to all vertices in $\boldsymbol{N}_j$ for any $j\neq i$, we can replace the missing edge in the path by a detour via some vertex in $\boldsymbol{N}_j$. Thus, x and y are still connected.

Case 2 ($x\in G_i, y\in G_j$)**:** In this case, x and y would not be connected in $G\setminus\{v\}$, as any path from x to y would contain the sequence $n-v-m$ where $n\in\boldsymbol{N}_i$ and $m\in\boldsymbol{N}_j$, and possibly edges within $\boldsymbol{N}_i$ and edges within $\boldsymbol{N}_j$. However, noting that the first vertex in the path that belongs to $\boldsymbol{N}_i$ is directly connected to the last vertex in the path that belongs to $\boldsymbol{N}_j$ yields a path connecting x and y in G'.

□

b. GHZ extraction

Here, we show that an extraction of a three-partite GHZ state from arbitrary connected graph states is always possible.

Theorem 8 (Graph state GHZ extraction)**.** *For all connected graph states $|G\rangle$ of $N \geq 3$ qubits and any choice of three of its parties a, b and c, there exists a proper tripartition $A \cup B \cup C = \{1, \ldots, N\}$ with $a \in A$, $b \in B$ and $c \in C$ and set-local unitary operations U_A, U_B and U_C acting on A, B and C, respectively, such that*

$$U_A \otimes U_B \otimes U_C \, |G\rangle = |GHZ_3\rangle_{abc} \otimes |G'\rangle \,, \tag{B16}$$

where $|G'\rangle$ is a graph state of $N-3$ vertices.

Proof. It is sufficient to prove the same statement where we replace $|\mathrm{GHZ}_3\rangle$ by the local unitary equivalent three-partite fully connected graph state $|\triangle\rangle$. We prove the theorem by induction over N.

Let $N = 3$ and $|G\rangle$ be a connected graph state of three vertices and w.l.o.g. $a = 1$, $b = 2$, $c = 3$. The only possible choice of sets is given by $A = \{1\}$, $B = \{2\}$, $C = \{3\}$. As $|G\rangle$ is connected, it either already equals $|\triangle\rangle$, or it is missing one edge. By local complementation of the opposite vertex, this edge is created, thereby transforming $|G\rangle$ into $|\triangle\rangle$.

Now, let the claim be true for some fixed $N - 1 \geq 3$. We consider the N-partite graph $|G_N\rangle$ and three arbitrary vertices $\{a, b, c\}$. We choose an arbitrary vertex $v \notin \{a, b, c\}$, such that we can write

$$|G_N\rangle = \prod_{j \in \boldsymbol{N}(v, G_N)} \mathrm{CZ}_{j,v} \, |G_{N-1}\rangle \otimes |+\rangle_v \,, \tag{B17}$$

where $|G_{N-1}\rangle$ is a graph state of $N-1$ vertices, including a, b and c. The goal is now to use the assumption of induction on $|G_{N-1}\rangle$, but it might be that $|G_{N-1}\rangle$ is not connected. This happens if v is an articulation point of the graph G_N, in which case we make use of Lemma 7 and first apply a local complementation w.r.t. v. To keep track of this, we define

$$|\tilde{G}_N\rangle = \begin{cases} \tau_v(|G_N\rangle) & \text{if } v \text{ is an articulation point of } G_N \\ |G_N\rangle & \text{otherwise.} \end{cases} \tag{B18}$$

and decompose

$$|\tilde{G}_N\rangle = \prod_{j \in \boldsymbol{N}(v, \tilde{G}_N)} \mathrm{CZ}_{j,v} \, |\tilde{G}_{N-1}\rangle \otimes |+\rangle_v \,, \tag{B19}$$

now with a certainly connected $N-1$-partite graph state $|\tilde{G}_{N-1}\rangle$. By assumption of induction, there exists a tripartition $A \cup B \cup C = \{1, \ldots, N-1\}$ of the vertices of $|\tilde{G}_{N-1}\rangle$ and set-local unitaries U_A, U_B and U_C, such that

$$U_A \otimes U_B \otimes U_C \, |\tilde{G}_{N-1}\rangle = |\triangle\rangle_{abc} \otimes |G'\rangle \,, \tag{B20}$$

where $|G'\rangle$ is some graph state of $N-4$ vertices. Note that we construct $U_A \otimes U_B \otimes U_C$ further below such that it is not only a set-local unitary, but it consists in fact only of products of CZ gates within the sets A, B and C, respectively, and local complementations. Thus, combining Eq. (B20) and Eq. (B19) we find

$$U_A \otimes U_B \otimes U_C \prod_{j \in \boldsymbol{N}(v, \tilde{G}_N)} \mathrm{CZ}_{j,v} \, |\tilde{G}_N\rangle = |\triangle\rangle_{abc} \otimes |G'\rangle \otimes |+\rangle_v \,. \tag{B21}$$

Using the definition in Eq. (B14), we can shorten the left-hand side of this equation and apply Lemma 6:

$$U_A \otimes U_B \otimes U_C \prod_{j \in \boldsymbol{N}(v, \tilde{G}_N)} \mathrm{CZ}_{j,v} \, |\tilde{G}_N\rangle = U_A \otimes U_B \otimes U_C \, \mathrm{CZ}_{\boldsymbol{N}(v, \tilde{G}_N), v} \, |\tilde{G}_N\rangle \tag{B22}$$

$$= \mathrm{CZ}_{\boldsymbol{N}(v, U_A \otimes U_B \otimes U_C \tilde{G}_N), v} \, U_A \otimes U_B \otimes U_C \, |\tilde{G}_N\rangle \,. \tag{B23}$$

Applying the controlled-Z operations on the right-hand side of Eq. (B19) again, we get

$$U_A \otimes U_B \otimes U_C \, |\tilde{G}_N\rangle = \mathrm{CZ}_{\boldsymbol{N}(v, U_A \otimes U_B \otimes U_C \tilde{G}_N), v} \, |\triangle\rangle_{abc} \otimes |G'\rangle \otimes |+\rangle_v \,. \tag{B24}$$

Now, depending on the connections of v to a, b and c in $U_A \otimes U_B \otimes U_C \, |\tilde{G}_N\rangle$, we can decide to which of the sets A, B or C we add the vertex v and how to modify U_A, U_B and U_C such that they stay set-local and disconnect $|\triangle\rangle_{abc}$ from v. We consider each case individually. To that end, set $\boldsymbol{N} \coloneqq \boldsymbol{N}(v, U_A \otimes U_B \otimes U_C \tilde{G}_N)$.

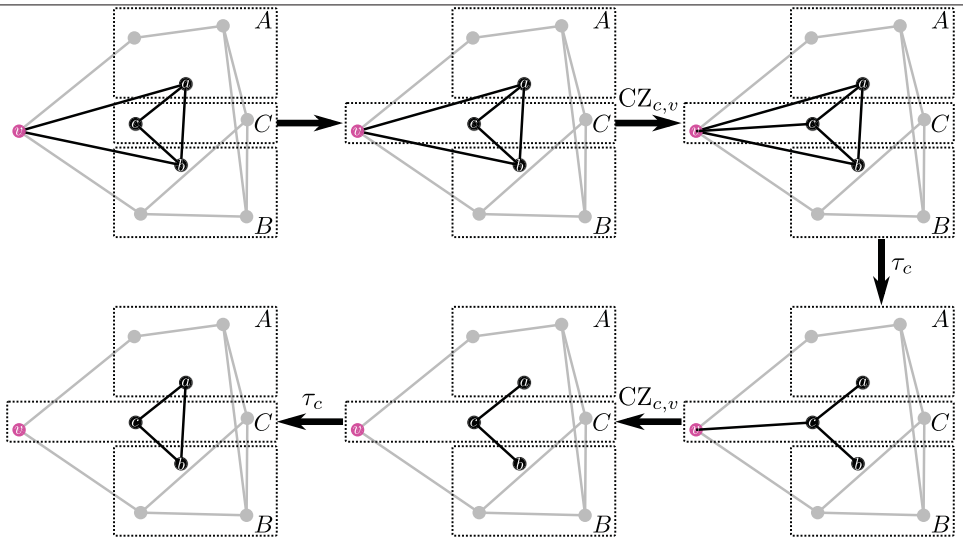


Figure 11. Visualization of case 3 of the proof: If the new vertex v is connected to vertices a and b of the extracted triangle graph state, we add it to set C and perform the C-local operations $\mathrm{CZ}_{c,v}$, τ_c, $\mathrm{CZ}_{c,v}$, τ_c to disconnect the vertices a, b, c from the new vertex v.

Case 1, $a, b, c \notin \boldsymbol{N}$**:**
In this case, $\mathrm{CZ}_{\boldsymbol{N},v} |\triangle\rangle_{abc} \otimes |G'\rangle \otimes |+\rangle_v = |\triangle\rangle_{abc} \otimes \mathrm{CZ}_{\boldsymbol{N},v} |G'\rangle \otimes |+\rangle_v$, where the triangle state is disconnected from the rest. Thus, we do not have to modify the local unitary and we can add the new vertex v to any of the sets A, B or C in order to obtain a proper tripartition of the vertices.

Case 2, $a \in \boldsymbol{N}$**,** $b, c \notin \boldsymbol{N}$**:**
In this case (and analogously in cases where b or c instead of a are connected to v), we commute all controlled-Z gates but $\mathrm{CZ}_{a,v}$ past $|\triangle\rangle_{abc}$:

$$U_A \otimes U_B \otimes U_C |\tilde{G}_N\rangle = \mathrm{CZ}_{a,v} |\triangle\rangle_{abc} \otimes \mathrm{CZ}_{\boldsymbol{N}\setminus\{a\},v} |G'\rangle \otimes |+\rangle_v . \tag{B25}$$

We add the new vertex v to the set A such that we can absorb $\mathrm{CZ}_{a,v}$ into U_A on the left-hand side to yield the claim.

Case 3, $a, b \in \boldsymbol{N}$**,** $c \notin \boldsymbol{N}$**:** In this case (and analogously in cases where a or b instead of c are not connected to v), we write

$$U_A \otimes U_B \otimes U_C |\tilde{G}_N\rangle = \mathrm{CZ}_{a,v}\, \mathrm{CZ}_{b,v} |\triangle\rangle_{abc} \otimes \mathrm{CZ}_{\boldsymbol{N}\setminus\{a,b\},v} |G'\rangle \otimes |+\rangle_v . \tag{B26}$$

We add v to C and multiply both sides from the left by the set-local sequence $\tau_c\, \mathrm{CZ}_{c,v}\, \tau_c\, \mathrm{CZ}_{c,v}$ (such that $\mathrm{CZ}_{c,v}$ is applied first). As visualized in Fig. 11, this sequence disconnects the triangle again from the rest. Thus,

$$\tau_c\, \mathrm{CZ}_{c,v}\, \tau_c\, \mathrm{CZ}_{c,v}\, U_A \otimes U_B \otimes U_C |\tilde{G}_N\rangle = |\triangle\rangle_{abc} \otimes \mathrm{CZ}_{\boldsymbol{N}\setminus\{a,b\},v} |G'\rangle \otimes |+\rangle_v . \tag{B27}$$

Case 4, $a, b, c \in \boldsymbol{N}$**:**
In this case, add v to C, and, analogously to case 3, we skip the first application of $\mathrm{CZ}_{c,v}$ and just apply $\tau_c\, \mathrm{CZ}_{c,v}\, \tau_c$, yielding the claim.

Finally, we absorb the potential local complementation of v from the definition of $|\tilde{G}_N\rangle$ into $U_A \otimes U_B \otimes U_C$ to yield the claim. Therefore, in any case we are able to recover the structure of an isolated triangle graph that is locally equivalent to $|\mathrm{GHZ}_3\rangle$. □

We are now in position to put all ingredients together: Knowing from Theorem 8 that we can extract a $|\mathrm{GHZ}_3\rangle$-state from every connected graph state of 3 or more parties, we can apply Lemma 3, which immediately yields the claim of Result 3 from the main text:

Theorem 2. *No connected qubit graph state of $N \geq 3$ parties can be prepared in an N-partite LOSR network with bipartite sources with a fidelity larger than $F_{LOSR}(|GHZ_3\rangle)$.*

Let us stress that the task of GHZ state extraction from graph states with a fixed tripartition of the vertices has been considered before [47]. In fact, the number of extractable GHZ states for a fixed tripartition has been shown to be an entanglement measure [48] and is equal to the difference of the dimension of the stabilizer group S of a stabilizer state (which is equal to the number of parties N) and the dimension of the group that is generated by the union of the local subgroups S_{AB}, S_{AC} and S_{BC}. Thus, the result of Theorem 8 sheds additional light on the structure of qubit stabilizer groups:

Corollary 9. *For every N-partite qubit stabilizer group S of size 2^N (i.e., dimension N) and every choice of three of its parties a, b and c, there exists a tripartition A, B, C of the parties with $a \in A$, $b \in B$ and $c \in C$ such that $\dim(\langle S_{AB}, S_{AC}, S_{BC}\rangle) < \dim(S) = N$.*

This, in turn, has an interesting consequence in terms of whether a stabilizer state is uniquely determined by its marginals:

Corollary 10. *For every N-partite qubit stabilizer state $|\psi\rangle$ and every choice of three of its parties a, b and c, there exists a tripartition A, B, C of the parties with $a \in A$, $b \in B$ and $c \in C$ such that $|\psi\rangle$ is not uniquely determined by the reduced states $\rho_{AB} = \mathrm{Tr}_C(|\psi\rangle\langle\psi|)$, ρ_{AC} and ρ_{BC}.*

Appendix C: Analytical upper bounds on the two-dimensional GHZ state fidelity

Here, we prove the upper bound of $F_{\mathrm{LOSR}}(|\mathrm{GHZ}_3\rangle) < 0.618$ from Result 1 for tripartite networks with qubit outputs, which improves upon the previously known bound of $F_{\mathrm{LOSR}} \leq (1+\sqrt{3})/4 < 0.684$ [18]. Note that in Refs. [18] and [63], the numerical value is incorrectly reported as 0.6803.

We prove the statement for tripartite network states without shared randomness (i.e, LO states, which are sometimes called independent triangle (ITN) states). For such states, stricter inequalities are known. Since the fidelity is linear if at least one of the states is pure, the bounds obtained for LO-states will then also be valid for LOSR-states.

We start with an alternative formulation for the fidelity between two quantum states ρ and σ [41]:

$$F(\rho,\sigma) = \left(\min_{\{E_k\}_k} \sum_k \sqrt{\mathrm{Tr}\left[E_k\rho\right]}\sqrt{\mathrm{Tr}\left[E_k\sigma\right]}\right)^2, \tag{C1}$$

where the minimization ranges over all positive operator valued measures (POVMs), i.e., sets of positive semidefinite, hermitian operators E_k with $\sum_k E_k = \mathbb{1}$. Thus, for any fixed choice of a POVM $\{E_k\}_k$, the fidelity is bounded by

$$F(\rho,\sigma) \leq \left(\sum_k \sqrt{\mathrm{Tr}\left[E_k\rho\right]}\sqrt{\mathrm{Tr}\left[E_k\sigma\right]}\right)^2. \tag{C2}$$

We choose $\sigma = |\mathrm{GHZ}_3\rangle\langle\mathrm{GHZ}_3|$ to be the target state, ρ to be preparable in a triangle network without shared randomness and the POVM to be the projective measurement in the computational basis, i.e. $\{|ijk\rangle\langle ijk|\}_{i,j,k\in\{0,1\}}$. Then, inequality (C2) reduces to

$$F(\rho,\sigma) \leq \frac{1}{2}\left(\sqrt{\mathrm{Tr}\left[|000\rangle\langle 000|\,\rho\right]} + \sqrt{\mathrm{Tr}\left[|111\rangle\langle 111|\,\rho\right]}\right)^2. \tag{C3}$$

We write $|000\rangle\langle 000| = (\mathbb{1}+Z)^{\otimes 3}/8$ and $|111\rangle\langle 111| = (\mathbb{1}-Z)^{\otimes 3}/8$ to rewrite the r.h.s. of (C3) in terms of the expectation values of the Pauli-Z matrices w.r.t. ρ, i.e.,

$$F(\rho,\sigma) \leq \frac{1}{16}\left(\sqrt{1+3z_1+3z_2+z_3} + \sqrt{1-3z_1+3z_2-z_3}\right)^2, \tag{C4}$$

where $z_1 \equiv (\langle Z_A\rangle + \langle Z_B\rangle + \langle Z_C\rangle)/3$, $z_2 \equiv (\langle Z_AZ_B\rangle + \langle Z_AZ_C\rangle + \langle Z_BZ_C\rangle)/3$ and $z_3 \equiv \langle Z_AZ_BZ_C\rangle$.

Before proving the statement, let us establish a fidelity bound involving z_2 only. To that end, notice that we can express the fidelity in terms of the stabilizers of the GHZ state via

$$F(\rho,\sigma) = \frac{1}{8}(1+3z_2+\langle X_AX_BX_C\rangle - \langle X_AY_BY_C\rangle - \langle Y_AX_BY_C\rangle - \langle Y_AY_BX_C\rangle). \tag{C5}$$

Furthermore, we can write the fidelity with the orthogonal state $|\overline{\mathrm{GHZ}}_3\rangle \coloneqq \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ as

$$0 \leq F(\rho, |\overline{\mathrm{GHZ}}_3\rangle\langle\overline{\mathrm{GHZ}}_3|) = \frac{1}{8}(1 + 3z_2 - \langle X_A X_B X_C\rangle + \langle X_A Y_B Y_C\rangle + \langle Y_A X_B Y_C\rangle + \langle Y_A Y_B X_C\rangle). \tag{C6}$$

Thus,

$$F(\rho, \sigma) \leq F(\rho, \sigma) + F(\rho, |\overline{\mathrm{GHZ}}_3\rangle\langle\overline{\mathrm{GHZ}}_3|) = \frac{1}{4}(1 + 3z_2). \tag{C7}$$

Let us now consider the constituents of z_1. W.l.o.g., we can assume that $\langle Z_A\rangle \geq 0$ and $\langle Z_B\rangle \geq 0$, because otherwise we could consider a permutation of the state $X_A X_B X_C \rho X_A X_B X_C$, which can be prepared in the triangle network without shared randomness as well, has the same fidelity with the GHZ state and negated (and possibly permuted) local Z-correlations. As only $\langle Z_C\rangle$ might be negative, we have that $z_1 \in [-1/3, 1]$. Let us consider the two cases of positive or negative $\langle Z_C\rangle$ individually.

Case 1, $\langle Z_C\rangle < 0$**:** In this case, we know from Eq. (44) in the Supplemental Material of Ref. [64] that the following inequality holds for triangle network states without shared randomness:

$$\begin{aligned}(1 + \langle Z_A\rangle + \langle Z_B\rangle + \langle Z_A Z_B\rangle)^2 + (1 + \langle Z_A\rangle - \langle Z_C\rangle + \langle Z_A Z_C\rangle)^2 + (1 + \langle Z_B\rangle - \langle Z_C\rangle + \langle Z_B Z_C\rangle)^2 \\ \leq 6(1 + \langle Z_A\rangle)(1 + \langle Z_B\rangle)(1 - \langle Z_C\rangle) + 8\langle Z_C\rangle(\langle Z_A\rangle + \langle Z_B\rangle + \langle Z_A\rangle\langle Z_B\rangle).\end{aligned} \tag{C8}$$

Furthermore, positivity demands

$$1 - \langle Z_A\rangle - \langle Z_B\rangle + \langle Z_C\rangle + \langle Z_A Z_B\rangle - \langle Z_A Z_C\rangle - \langle Z_B Z_C\rangle + \langle Z_A Z_B Z_C\rangle \geq 0 \tag{C9}$$

$$\Rightarrow \quad 1 - \langle Z_A\rangle - \langle Z_B\rangle + \langle Z_C\rangle + \langle Z_A Z_B\rangle - \langle Z_A Z_C\rangle - \langle Z_B Z_C\rangle + 1 \geq 0, \tag{C10}$$

as the first line corresponds to the non-negative probability of obtaining outcomes $1, 1, 0$ when measuring in the computational basis. The second line follows from bounding the tripartite correlation $\langle Z_A Z_B Z_C\rangle$, by its maximal value of 1.

We can now consider the constrained optimization problem

$$z_2^* = \max_{\langle Z_i\rangle, \langle Z_k Z_l\rangle} z_2 \tag{C11}$$

$$\text{s. t.} \qquad 0 \leq \langle Z_A\rangle \leq 1, \tag{C12}$$

$$0 \leq \langle Z_B\rangle \leq 1, \tag{C13}$$

$$-1 \leq \langle Z_C\rangle < 0, \tag{C14}$$

$$\text{Eq. (C8) holds}, \tag{C15}$$

$$\text{Eq. (C10) holds}. \tag{C16}$$

Let us simplify this optimization problem by showing that $\langle Z_A\rangle = \langle Z_B\rangle$ and $\langle Z_A Z_C\rangle = \langle Z_B Z_C\rangle$ can be assumed at the maximum. We show this by demonstrating that, given a solution to the optimization problem, symmetrizing these expectations values leads to another valid solution. To see this, we restrict ourselves to an optimization on the planes corresponding to constant sums $\langle Z_A\rangle + \langle Z_B\rangle$ and $\langle Z_A Z_C\rangle + \langle Z_B Z_C\rangle$ by setting $\langle Z_B\rangle = \bar{z}_1 - \langle Z_A\rangle$ and $\langle Z_B Z_C\rangle = \bar{z}_2 - \langle Z_A Z_C\rangle$ for fixed $\bar{z}_1$, $\bar{z}_2$. Note that the optimization function z_2, as well as the left-hand side of Eq. (C10) are independent of the single expectation values and only depend on the constant sums $\bar{z}_1$ and $\bar{z}_2$, whereas Eq. (C8) becomes

$$\begin{aligned}(1 + \bar{z}_1 + \langle Z_A Z_B\rangle)^2 + (1 + \langle Z_A\rangle - \langle Z_C\rangle + \langle Z_A Z_C\rangle)^2 + (1 + \bar{z}_1 + \bar{z}_2 - \langle Z_A\rangle - \langle Z_C\rangle - \langle Z_A Z_C\rangle)^2 \\ - 6(1 + \langle Z_A\rangle)(1 + \bar{z}_1 - \langle Z_A\rangle)(1 - \langle Z_C\rangle) - 8\langle Z_C\rangle(\bar{z}_1 + (\bar{z}_1 - \langle Z_A\rangle)\langle Z_A\rangle) \leq 0.\end{aligned} \tag{C17}$$

While this might not look appealing, it becomes least restrictive, i.e., the left-hand side becomes minimal, for the symmetric case. To see this, consider the Hesse matrix w.r.t. the variables $\langle Z_A\rangle$ and $\langle Z_A Z_C\rangle$, the eigenvalues of which read

$$\lambda_\pm = 2\left(5 + \langle Z_C\rangle \pm \sqrt{\langle Z_C\rangle^2 + 6\langle Z_C\rangle + 13}\right), \tag{C18}$$

which are strictly positive for $-1 \leq \langle Z_C \rangle < 0$. Thus, the left-hand side is convex w.r.t. these two variables. Furthermore, its partial derivatives w.r.t. the two variables vanish at $\langle Z_A \rangle = \bar{z}_1/2$, $\langle Z_A Z_C \rangle = \bar{z}_2/2$, showing that the global minimum of the left-hand side is assumed for the choice of $\langle Z_A \rangle = \langle Z_B \rangle$ and $\langle Z_A Z_C \rangle = \langle Z_B Z_C \rangle$. Inserting this into the optimization problem allows us to analytically solve it using the computer algebra system Mathematica and obtain $z_2^* = \left(42 - 5\sqrt{42}\right)/21$. Inserting this into the fidelity bound of Eq. (C7) yields

$$F \leq \frac{1}{28}\left(49 - 5\sqrt{42}\right) \approx 0.593. \tag{C19}$$

As we will see below, we will obtain a larger bound in the other case, such that we can dismiss this one.

Case 2, $\langle Z_C \rangle \geq 0$: In this case, we use two inequalities valid for triangle network states without shared randomness: First, we use Gisin's inequality from Ref. [64] for the case of positive local correlators, which reads

$$\begin{aligned}(1 + \langle Z_A \rangle + \langle Z_B \rangle + \langle Z_A Z_B \rangle)^2 + (1 + \langle Z_A \rangle + \langle Z_C \rangle + \langle Z_A Z_C \rangle)^2 + (1 + \langle Z_B \rangle + \langle Z_C \rangle + \langle Z_B Z_C \rangle)^2 \\ \leq 6(1 + \langle Z_A \rangle)(1 + \langle Z_B \rangle)(1 + \langle Z_C \rangle)\end{aligned} \tag{C20}$$

Second, we make use of a variant of the classical Finner inequality, established in Ref. [42].[1] It states that for each local projective measurement $\{P_i\}_{i=0}^{d-1}$ and all triangle network states without shared randomness,

$$\mathrm{Tr}(\rho P_i \otimes P_j \otimes P_k) \leq \sqrt{\mathrm{Tr}(\rho P_i \otimes \mathbb{1} \otimes \mathbb{1})\,\mathrm{Tr}(\rho \mathbb{1} \otimes P_j \otimes \mathbb{1})\,\mathrm{Tr}(\rho \mathbb{1} \otimes \mathbb{1} \otimes P_k)} \tag{C21}$$

holds. If we choose the dichotomic measurement in the Z basis, i.e., $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$, and consider $i = j = k = 1$, this yields similar to the step from Eq. (C3) to Eq. (C4),

$$1 - 3z_1 + 3z_2 - z_3 \leq \sqrt{8}\sqrt{(1 - \langle Z_A \rangle)(1 - \langle Z_B \rangle)(1 - \langle Z_C \rangle)}. \tag{C22}$$

We now maximize the right-hand side of Eq. (C4), i.e.,

$$F \leq \max_{\langle Z_i \rangle, \langle Z_k Z_l \rangle, \langle Z_A Z_B Z_C \rangle} \frac{1}{16}\left(\sqrt{1 + 3z_1 + 3z_2 + z_3} + \sqrt{1 - 3z_1 + 3z_2 - z_3}\right)^2 \tag{C23}$$

$$\text{s. t.} \qquad 0 \leq \langle Z_A \rangle, \langle Z_B \rangle, \langle Z_C \rangle \leq 1, \tag{C24}$$

$$\text{Eq. (C20) holds,} \tag{C25}$$

$$\text{Eq. (C22) holds.} \tag{C26}$$

Let us argue again that in order to maximize the expression, we can assume symmetric choices $\langle Z_A \rangle = \langle Z_B \rangle = \langle Z_C \rangle$ as well as $\langle Z_A Z_B \rangle = \langle Z_A Z_C \rangle = \langle Z_B Z_C \rangle$. To that end, we consider the planes of fixed z_1 and z_2 and set $\langle Z_C \rangle = 3z_1 - \langle Z_A \rangle - \langle Z_B \rangle$, $\langle Z_A Z_B \rangle = 3z_2 - \langle Z_A Z_C \rangle - \langle Z_B Z_C \rangle$. Note that the objective function is independent of the single expectation values and only depends on the constant sums z_1 and z_2. While the left-hand side of Inequality (C22) remains independent as well, its right-hand side is clearly maximized (and therefore least restrictive) for the symmetric choice. However, the inequality (C20) becomes

$$\begin{aligned}(1 + 3z_2 + \langle Z_A \rangle + \langle Z_B \rangle - \langle Z_A Z_C \rangle - \langle Z_B Z_C \rangle)^2 + (1 + 3z_1 - \langle Z_B \rangle + \langle Z_A Z_C \rangle)^2 + (1 + 3z_1 - \langle Z_A \rangle + \langle Z_B Z_C \rangle)^2 \\ - 6(1 + \langle Z_A \rangle)(1 + \langle Z_B \rangle)(1 + 3z_1 - \langle Z_A \rangle - \langle Z_B \rangle) \leq 0.\end{aligned} \tag{C27}$$

We again minimize the left-hand side of this inequality to obtain the least restrictive one. To that end, we calculate its 4×4-dimensional Hesse matrix w.r.t. the variables $\langle Z_A \rangle, \langle Z_B \rangle, \langle Z_A Z_C \rangle, \langle Z_B Z_C \rangle$. Its characteristic polynomial reads

$$x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0, \tag{C28}$$

[1] Note, however, that the proof in that reference is not complete.

where

$$\begin{aligned}
a_0 &= 432[&& -9z_1^2 + 6z_1 + 3 && +12z_1(\langle Z_A\rangle + \langle Z_B\rangle) - 4(\langle Z_A\rangle^2 + \langle Z_A\rangle\langle Z_B\rangle + \langle Z_B\rangle^2)],\\
a_1 &= 288[&& 9z_1^2 - 6z_1 - 5 && -(12z_1+1)(\langle Z_A\rangle + \langle Z_B\rangle) + 4(\langle Z_A\rangle^2 + \langle Z_A\rangle\langle Z_B\rangle + \langle Z_B\rangle^2)],\\
a_2 &= 12[&& -27z_1^2 + 24z_1 + 35 && +(36z_1+8)(\langle Z_A\rangle + \langle Z_B\rangle) - 12(\langle Z_A\rangle^2 + \langle Z_A\rangle\langle Z_B\rangle + \langle Z_B\rangle^2)],\\
a_3 &= && -40 && -12(\langle Z_A\rangle + \langle Z_B\rangle) .
\end{aligned}$$

We can trivially maximize the prefactors of x^3 and x, as well as minimize those of x^2 and x^0 over $\langle Z_A\rangle$, $\langle Z_B\rangle$ and z_1 under the constraints $0 \leq \langle Z_A\rangle, \langle Z_B\rangle \leq 1$ and $\langle Z_A\rangle + \langle Z_B\rangle \leq 3z_1 \leq 3$ using the computer algebra system Mathematica to show that the signs of the prefactors alternate. Thus, by Descartes' rule of signs, the Hesse matrix is positive and therefore the left-hand side of (C27) is convex. Setting the first derivatives equal zero yields a single solution in the optimization region, namely $\langle Z_A\rangle = \langle Z_B\rangle = \langle Z_C\rangle$ and $\langle Z_A Z_B\rangle = \langle Z_A Z_C\rangle = \langle Z_B Z_C\rangle$, which is therefore the global minimum and thus the least restrictive choice for the optimization.

Finally, we can thus consider the symmetrized optimization problem where each occurrence of $\langle Z_A\rangle$, $\langle Z_B\rangle$ and $\langle Z_C\rangle$ is replaced by z_1 (and likewise $\langle Z_A Z_B\rangle = \ldots = z_2$), yielding

$$\begin{aligned}
F \leq \max_{z_1,z_2,z_3} \frac{1}{16}\left(\sqrt{1+3z_1+3z_2+z_3} + \sqrt{1-3z_1+3z_2-z_3}\right)^2 && \text{(C29)}\\
\text{s. t.} \quad 0 \leq z_1 \leq 1, && \text{(C30)}\\
3(1+2z_1+z_2)^2 \leq 6(1+z_1)^3 && \text{(C31)}\\
0 \leq 1-3z_1+3z_2-z_3 \leq \sqrt{8}\sqrt{(1-z_1)^3}. && \text{(C32)}
\end{aligned}$$

This optimization can be solved using the computer algebra system Mathematica and yields a maximum in terms of the largest real root of the polynomial

$$832000x^6 + 114944x^5 - 2964416x^4 + 4210624x^3 - 2743640x^2 + 889800x - 120125, \tag{C33}$$

which is approximately given by

$$F \leq 0.618, \tag{C34}$$

where we rounded up the last digit. This proves the claim.

The derivation of the analytical bound in Result 1 makes use of a couple of inequalities and estimates which raises the question of how wasteful they are. To answer this question, we resort to convex optimization. However, both the Gisin inequality in Eq. (C20) as well as the Finner inequality in Eq. (C22) are not convex. Thus, we apply the following trick: Instead of optimizing the fidelity over general output states, we fix the values of $\langle Z_A\rangle \equiv z_A$ and $\langle Z_B\rangle \equiv z_B$ and treat z_A and z_B as parameters between 0 and 1. In order to get rid of the absolute values around $\langle Z_C\rangle$, we treat its sign as an additional dichotomic input parameter $c \in \{-1, 1\}$. When maximizing the inequality, we then consider individually the cases of $\langle Z_C\rangle \geq 0$ (i.e., $c = 1$) and $\langle Z_C\rangle < 0$ (i.e., $c = -1$) and take the maximum of both optimizations. We therefore consider the parameterized optimization problem

$$\begin{aligned}
B(z_A, z_B, c) = \max_{\rho} \ \langle \mathrm{GHZ}_3|\rho|\mathrm{GHZ}_3\rangle && \text{(C35)}\\
\text{s. t.} \quad \rho \geq 0, && \text{(C36)}\\
\mathrm{Tr}(\rho) = 1, && \text{(C37)}\\
\langle Z_A\rangle = z_A, && \text{(C38)}\\
\langle Z_B\rangle = z_B, && \text{(C39)}\\
c\langle Z_C\rangle \geq 0, && \text{(C40)}\\
\text{Eq. (C20) (if } c = 1) \text{ or Eq. (C8) (if } c = -1) \text{ holds}, && \text{(C41)}\\
\text{Eq. (C22) holds.} && \text{(C42)}
\end{aligned}$$

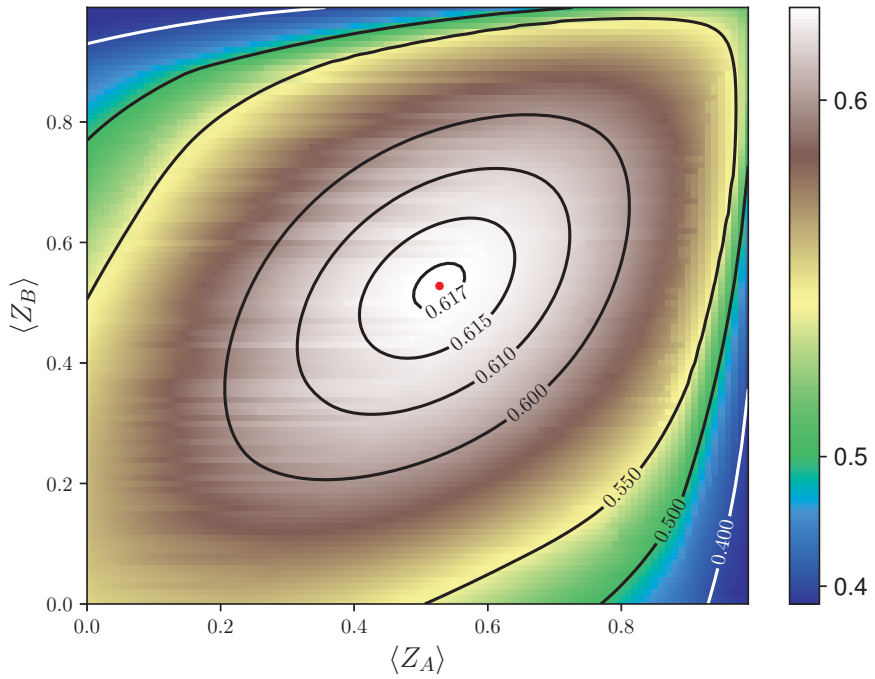


Figure 12. The maximal GHZ-fidelities in triangle LOSR networks $B(z_A, z_B)$ from Eq. (C46) for fixed values of $z_A = \langle Z_A \rangle$ and $z_B = \langle Z_B \rangle$. The optimization takes into account Gisin's inequality (C20) and the Finner inequality (C22). The image is obtained by rasterization of the parameters in steps of 10^{-2}. The global optimum (marked with a red dot) reaches the bound from Result 1, indicating that no further improvement of the upper bound is possible if only Gisin's inequality and the Finner inequality are taken into account.

We can turn this optimization into the form of a semidefinite program by noticing that for $c = 1$, the constraint (C20) can be cast into the form of a positivity constraint of a symmetric matrix, namely

$$\begin{pmatrix} 6(1+z_A)(1+z_B)(1+\langle Z_C\rangle) & \dots & \dots & \dots \\ 1+z_A+z_B+\langle Z_A Z_B\rangle & 1 & \dots & \dots \\ 1+z_A+\langle Z_C\rangle+\langle Z_A Z_C\rangle & 0 & 1 & \dots \\ 1+z_B+\langle Z_C\rangle+\langle Z_B Z_C\rangle & 0 & 0 & 1 \end{pmatrix} \geq 0 \tag{C43}$$

(the entries filled with ... are fixed by choosing the matrix symmetric). Likewise, if $c = -1$, (C8) can be written as positivity of the matrix

$$\begin{pmatrix} 6(1+z_A)(1+z_B)(1-\langle Z_C\rangle)+8\langle Z_C\rangle(z_A+z_B+z_A z_B) & \dots & \dots & \dots \\ 1+z_A+z_B+\langle Z_A Z_B\rangle & 1 & \dots & \dots \\ 1+z_A-\langle Z_C\rangle+\langle Z_A Z_C\rangle & 0 & 1 & \dots \\ 1+z_B-\langle Z_C\rangle+\langle Z_B Z_C\rangle & 0 & 0 & 1 \end{pmatrix} \geq 0. \tag{C44}$$

Finally, the Finner inequality from Eq. (C22) can be written as

$$\begin{pmatrix} (1-z_A)(1-z_B)(1-\langle Z_C\rangle) & \dots \\ 1-z_A-z_B-\langle Z_C\rangle+\langle Z_A Z_B\rangle+\langle Z_A Z_C\rangle+\langle Z_B Z_C\rangle-\langle Z_A Z_B Z_C\rangle & 8 \end{pmatrix} \geq 0 \tag{C45}$$

The virtue of formulating a semidefinite program lies in the fact that we can obtain robust numerical solutions with guaranteed optimality for each choice of z_A, z_B, c. We plot the resulting function

$$B(z_A, z_B) := \max_{c\in\{-1,1\}} B(z_A, z_B, c) \tag{C46}$$

in Fig. 12 by sampling the space of $z_A, z_B \in [0, 1]$ in steps of 10^{-2}. It is apparent from the figure that the maximum occurs at $z_A = z_B \approx 0.528$ and reaches indeed the fidelity of $F \approx 0.618$, implying that the result from Result 1 cannot

be improved, if only Gisin's inequality and the Finner inequality are considered (we also added the Finner inequality for different choices of outcomes i, j, k, but it did not improve the result). Additionally, we combined our SDP method with the SDP inflation technique that was used in Ref. [18]. However, it did not improve the result.

Note that the numerical result also allows us to explicitly state the putative state which reaches this fidelity, namely

$$\rho_{\text{opt}} = \begin{pmatrix} 0.597 & 0 & 0 & 0 & 0 & 0 & 0 & 0.262 \\ 0 & 0.071 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.071 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.025 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.071 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.025 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.025 & 0 \\ 0.262 & 0 & 0 & 0 & 0 & 0 & 0 & 0.115 \end{pmatrix}. \tag{C47}$$

By design, it neither violates Gisin's inequality nor the Finner inequality, however, given the fact that its fidelity deviates from the fidelity reached by our constructions in Appendix A by about 0.07, we assume that it is not preparable in an LOSR network. One would need tools beyond Gisin's inequality, the Finner inequality and the SDP inflation technique from Ref. [18] to exclude it.

Appendix D: Fidelity bounds with the GHZ state for arbitrary dimension and number of parties

In this section we prove the statements of Results 2 and 5 from the main text by deriving upper bounds for the fidelity of quantum network states with the GHZ state for any dimension and number of parties, i.e., $F_{\text{LOSR}}(|\text{GHZ}_{N,d}\rangle)$.

First, for $N = 3$, we use Eq. (C1) to bound the fidelity of a state ρ with the GHZ state in terms of joint probability distributions by choosing as POVM the projective measurements in the computational basis, i.e. $\{|ijk\rangle\langle ijk|\}_{i,j,k\in\{0,d-1\}}$, which yields

$$F(\rho, |\text{GHZ}_{3,d}\rangle\langle\text{GHZ}_{3,d}|) \leq \frac{1}{d}\left(\sum_{i=0}^{d-1}\sqrt{\langle iii|\,\rho\,|iii\rangle}\right)^2 = \frac{1}{d}\left(\sum_{i=0}^{d-1}\sqrt{p(i,i,i)}\right)^2. \tag{D1}$$

We make use of Eq. (C21), the quantum variant of the classical Finner inequality for quantum network states without shared randomness [42]. Note again that due to the fact that the fidelity with a pure state is a linear function, the derived fidelity bound will also hold for proper LOSR states with shared randomness. Using for the Finner inequality the same measurement in the computational basis, i.e. $P_i = |i\rangle\langle i|$, we get

$$p(i,j,k) \leq \sqrt{p_A(i)p_B(j)p_C(k)} \tag{D2}$$

where $p(i,j,k) = \text{Tr}(\rho\,|ijk\rangle\langle ijk|)$, $p_A(i) = \text{Tr}(\rho\,|i\rangle\langle i|\otimes\mathbb{1}\otimes\mathbb{1})$, $p_B(j) = \text{Tr}(\rho\mathbb{1}\otimes|j\rangle\langle j|\otimes\mathbb{1})$ and $p_C(k) = \text{Tr}(\rho\mathbb{1}\otimes\mathbb{1}\otimes|k\rangle\langle k|)$ for $i,\ j,\ k \in \{0,1,\ldots,d-1\}$.

Thus, for any state ρ from a triangle network without shared randomness, we have that

$$F(\rho, |\text{GHZ}_{3,d}\rangle\langle\text{GHZ}_{3,d}|) \leq \frac{1}{d}\left(\sum_{i=0}^{d-1}(p_A(i)p_B(i)p_C(i))^{1/4}\right)^2 \tag{D3}$$

$$= \frac{1}{d}\left(d^{1/4}\sum_{i=0}^{d-1}\left(p_A(i)p_B(i)p_C(i)\frac{1}{d}\right)^{1/4}\right)^2 \tag{D4}$$

$$\leq \frac{1}{\sqrt{d}}, \tag{D5}$$

where in the last step we used that the Matusita fidelity is upper bounded by 1 (see, e.g., [65]). The Matusita fidelity is defined as follows: For $r \in \mathbb{N}$, let $\{p_1, p_2, \ldots, p_r\}$ be a set of probability distributions on a finite set $\mathcal{X}$, then $\mathcal{F}_r(p_1, p_2, \ldots, p_r) \coloneqq \sum_{x\in\mathcal{X}}(p_1(x)\ldots p_r(x))^{1/r}$ is called their Matusita fidelity. Note that here we have $r = 4$, and the fourth probability distribution $p_4(i) = 1/d$ is the uniform distribution on the set $\{0,\ldots,d-1\}$.

Next we consider network states of four parties with bipartite source states without shared randomness. Note that the constraint in Eq. (D2) is extendible to an arbitrary number of parties [42]:

$$p(a_1, a_2, \ldots a_N) \leq \sqrt{p_{A_1}(a_1)p_{A_2}(a_2)\ldots p_{A_N}(a_N)}. \tag{D6}$$

Thus,

$$F(\rho, |\mathrm{GHZ}_{4,d}\rangle\langle\mathrm{GHZ}_{4,d}|) \leq \frac{1}{d}\left(\sum_{i=0}^{d-1}\sqrt{\langle iiii|\,\rho\,|iiii\rangle}\right)^2 = \frac{1}{d}\left(\sum_{i=0}^{d-1}\sqrt{p(i,i,i,i)}\right)^2 \tag{D7}$$

$$\leq \frac{1}{d}\left(\sum_{i=0}^{d-1}(p_A(i)p_B(i)p_C(i)p_D(i))^{1/4}\right)^2 \tag{D8}$$

$$= \frac{1}{d}\mathcal{F}_4(p_A, p_B, p_C, p_D)^2 \leq \frac{1}{d}. \tag{D9}$$

In the first line, we again estimate the fidelity by choosing the projective measurement in the computational basis. In the second line, we use Eq. (D6) and in the last step we use the property that the Matusita fidelity cannot be greater than 1. Together with Corollary 4, it follows that this bound also holds for quantum network states with $N \geq 4$ parties and bipartite source states, i.e.,

$$F(\rho, |\mathrm{GHZ}_{N,d}\rangle\langle\mathrm{GHZ}_{N,d}|) \leq \frac{1}{d} \tag{D10}$$

for all $N \geq 4$. We also remark that this is a tight bound which can be achieved by the product state $\rho = |i\rangle\langle i|^{\otimes N}$ with $i \in \{0, \ldots, d-1\}$.

Paper B

Bounds on quantum conference key agreement in pair-entangled networks

The following text is reproduced from the preprint

Justus Neumann, Hermann Kampermann, Dagmar Bruß, and Anton Trushechkin
Bounds on quantum conference key agreement in pair-entangled networks arXiv preprint, 2026. 2605.18399 [quant-ph]

Statement of contribution

My main contribution to this work consisted of deriving upper bounds on conference key agreement in pair-entangled quantum networks. In particular, I derived Theorems 1 and 2. Anton Trushechkin derived Theorems 3, 4, and 5. The proof strategies, interpretation of the results, and their relation to the general problem of conference key agreement in quantum networks were discussed jointly. Hermann Kampermann and Dagmar Bruß contributed to discussions and provided feedback on the presentation of the work. The manuscript was finalized with input from all authors. The project was supervised by Hermann Kampermann, Dagmar Bruß, and Anton Trushechkin.

arXiv:2605.18399v1 [quant-ph] 18 May 2026

Bounds on quantum conference key agreement in pair-entangled networks

Justus Neumann,[1] Hermann Kampermann,[1] Dagmar Bruß,[1] and Anton Trushechkin[1,2,*]

[1] *Heinrich Heine University Düsseldorf, Faculty of Mathematics and Natural Sciences, Institute for Theoretical Physics III, Universitätsstr. 1, Düsseldorf 40225, Germany*
[2] *Technical University of Braunschweig, Faculty of Electrical Engineering, Information Technology, and Physics, Institute for Communications Technology, Schleinitzstr. 22, Braunschweig 38106, Germany*

(Dated: May 19, 2026)

We investigate the task of conference key agreement in near-term quantum networks, where the nodes are connected by sources of bipartite entangled states, under the class of local operations not requiring quantum memory. We derive upper bounds on the distillable conference key depending on the network topology and degree of entanglement of the sources, and prove tightness of these bounds for some particular cases. In these cases, we show that pairwise bipartite key distillation followed by merging the bipartite keys into the conference key is optimal.

I. INTRODUCTION

Quantum networks and even the "quantum internet" are believed to be a part of future quantum communication infrastructure [1–8]. Secure distribution of cryptographic keys is supposed to be one of the earliest applications of quantum networks.

An important network cryptographic task is conference key agreement (CKA), i.e., establishing a common secret key for all participants in the network or a subset of them. Quantum conference key agreement (QCKA) has recently attracted attention [9–13]. One way of doing QCKA is distributing multipartite entangled states, e.g., GHZ states. It has been shown that directly utilizing multipartite entangled states (e.g. GHZ states) can improve the rate of conference key generation compared to pairwise schemes [11, 12, 14]. However, the generation of multipartite GHZ states remains technologically challenging. Near-term quantum networks will likely be limited to pairwise entanglement, e.g. Bell states, between nodes. In such pair-entangled networks (PENs) [15], the global resource state is composed solely of bipartite entangled states shared among various parties (nodes).

In this paper, we do not consider full QCKA protocols, which assume that the adversary can replace a source of entangled states (or a quantum channel) by their own, but consider the simplified task of *conference key distillation* [16–19], where the quantum state is given and known. The role of the adversary is that they hold the purification of this state (if it is mixed) and listen to the public classical communication.

We assume that users at their respective nodes can perform collective measurements on the subsystems coming from different sources. In the case of photons, this can be achieved using suitable interferometers. But we assume that the users cannot perform general local operations and classical communications (LOCC), which would require quantum memories. In our scenario, users are not required to store their quantum systems after receiving the distributed quantum states. However, they are supposed to have preshared randomness, which gives rise to the "local operations and shared randomness" (LOSR) scenario. The LOSR network setting, i.e., PEN states followed by LOSR operations, is actively studied [20–24]. Additionally, we allow postprocessing with arbitrary classical communication.

Although LOSR networks are severely restricted operationally, they can nevertheless generate nontrivial multipartite correlations. In particular, while the global resource consists only of bipartite states distributed along the edges of a network, the resulting network state may exhibit genuine multipartite entanglement [21, 24]. This observation suggests that there might exist multipartite strategies for QCKA which outperform strategies restricted to biseparable source states [25, 26]. In this work, we show that this is not the case for this type of network.

The central question we address are upper bounds on the distillable conference key originating from the network topology and their tightness. Some general upper bounds are known [19, 27]. We apply them to PEN networks and show that they reduce to the "weakest cut" bound. Roughly speaking, this means that, if the network is decomposed into two weakly connected parts, then the conference key agreement cannot exceed the capacity of this link. This bound is often not tight. We then derive bounds taking into account more general network topologies and bottleneck structures, which are based on arbitrary partitions of the corresponding graph, not just bipartitions.

We show that the protocol based on the spanning-tree packing [28–30] allows us to achieve upper bounds for some particular cases, proving the tightness of these bounds in these cases. In contrast to Ref. [30], here we focus on upper bounds rather than on explicit protocols. Furthermore, in Ref. [30] only the scenario where the participants have already established a bipartite secret key is considered. Here we consider a more general situation of a network of bipartite entangled states.

This work is organized as follows. In Section II, we give the definitions of the distillable conference key for an ar-

* anton.trushechkin@hhu.de

bitrary multipartite resource state and the definition of the PEN states. In Section III, we study conference key distillation protocols in which a single party serves as the reference party. This setting naturally gives rise to the tripartite generalization of the Devetak–Winter formula [11, 31, 32]. We derive a general upper bound for the multipartite Devetak-Winter conference key generation rate in the LOSR setting and an upper bound for the tripartite generalization of the BB84 quantum key distribution (QKD) protocol [33].

It is known that genuine multipartite entanglement is not a necessary condition for QCKA [25, 26], but upper bounds on the distillable conference key under restricted classes of multipartite states like LOSR preparable states from bipartite sources are unknown.

Starting from Section IV, we analyze the general conference key distillation. We discuss the bound based on vertex bipartitions ("weakest cut") and also prove that the bound from Ref. [19] applied to PEN states reduces to this bound. Section V contains general upper bounds. Our conclusions are given in Section VI.

II. PRELIMINARIES

A. Distillable conference key

Throughout the paper we fix the following conventions: We work with N honest parties $1, 2, ..., N$. We denote the corresponding quantum systems as $A_1, A_2, \ldots, A_N$ and write $\vec{A} = (A_1, \ldots, A_N)$. At the start of every protocol round a source distributes a multipartite state $\rho_{A_1 \ldots A_N} \equiv \rho_{\vec{A}}$, i.e., a density operator in a Hilbert space $\mathcal{H}_{A_1} \otimes \ldots \otimes \mathcal{H}_{A_N} \equiv \mathcal{H}_{\vec{A}}$. For every non-empty subset $I \subset \{1, \ldots, N\} \equiv [N]$ we abbreviate $A_I = (A_i)_{i \in I}$, $\overline{I} = [N] \backslash I$, $\mathcal{H}_I = \bigotimes_{i \in I} \mathcal{H}_{A_i}$, and

$$\rho_{A_I} = \mathrm{Tr}_{A_{\overline{I}}} \rho_{\vec{A}}, \qquad \rho_{A_I E} = \mathrm{Tr}_{A_{\overline{I}}} \rho_{\vec{A}E}. \tag{1}$$

Here $\rho_{A_I E}$ is a purification of state ρ_{A_I}, i.e., a projector onto a vector in the Hilbert space $\mathcal{H}_{\vec{A}} \otimes \mathcal{H}_E$. The additional party E is called Eve. We consider the following scenario. First, the participants perform measurements from the LOSR (local operations and shared randomness) class, i.e., measurements of the form

$$\Big\{ \sum_{\lambda \in \mathcal{L}} p_\lambda M_{x_1}^{(1),(\lambda)} \otimes M_{x_2}^{(2),(\lambda)} \otimes \ldots \otimes M_{x_N}^{(N),(\lambda)} \Big| \, x_i \in \mathcal{X}_i \Big\}, \tag{2}$$

where $\{M_{x_i}^{(i),(\lambda)}\}_{x_i \in \mathcal{X}_i}$, $i \in \{1, \ldots, N\}$, $\lambda \in \mathcal{L}$ are local positive operator-valued measures (POVM) depending on the parameter λ randomly chosen from a finite set $\mathcal{L}$ according to the probability distribution $\{p_\lambda\}$ (public shared randomness). Here $\mathcal{X}_i$ are arbitrary finite sets of the outcomes. Then, the participants perform classical postprocessing. We denote this class of quantum channels (CPTP maps) as LOSR+PP.

The distillable conference key for the parties I (following Ref. [29], we call them "secrecy-seeking parties", while $[N]\backslash I$ are commonly referred to as "helpers") is defined as [17–19]

$$\overline{r}_{\mathrm{key}}(I) = \lim_{\varepsilon \to 0} \sup_{\substack{n,m, \\ \Lambda \in \mathrm{LOSR+PP}}} \Big\{ \frac{m}{n} \Big| \, \frac{1}{2} \big\| \Lambda(\rho_{\vec{A}E}^{\otimes n}) - \rho_{K_I E^n C}^{(m),\,\mathrm{ideal}} \big\|_1 \leq \varepsilon \Big\}, \tag{3}$$

where E^n is Eve's register originating from n copies of $\rho_{\vec{A}E}$, the channel Λ acts on the parties $\vec{A}$ (i.e., the action on E^n is trivial), C is the register for the classical communication in the postprocessing part of an LOSR+PP protocol (and also includes the public shared randomness λ), and

$$\begin{aligned} \rho_{K_I E^n C}^{(m),\,\mathrm{ideal}} &= 2^{-m} \sum_{k \in \{0,1\}^m} (|k\rangle \langle k|)^{\otimes |I|} \otimes \rho_{E^n C}, \\ \rho_{E^n C} &= \mathrm{Tr}_{K_I} \Lambda(\rho_{\vec{A}E}^{\otimes n}). \end{aligned} \tag{4}$$

Here K_i, $i \in I$, are registers containing the secret key and associated with the corresponding parties. Each of them corresponds to the 2^m-dimensional Hilbert space of key and $\{|k\rangle\}$ is an orthonormal basis in this space. That is, in the ideal state (4), the parties from I share a perfectly classically correlated state uncoupled from Eve and classical communication. In the definition of (3) we assume that the helpers are trusted: We do not require privacy with respect to them. In classical multiterminal information theory, both problem statements with trusted and untrusted helpers are considered [34]. We will return to this discussion in the end of the paper in Remark 2.

B. Network model

We consider a special class of multipartite states, namely the so called pair-entangled network (PEN) states [15]. Let a connected graph $([N], \mathcal{E})$ be given, where $[N] = \{1, \ldots, N\}$ is the set of vertices and $\mathcal{E}$ is the set of edges. A PEN state has the form

$$\rho_{\vec{A}} = \bigotimes_{e \in \mathcal{E}} \rho_e, \tag{5}$$

where ρ_e are (possibly different) bipartite states acting on Hilbert spaces $\mathcal{H}_e$ corresponding to the edges e. An example is depicted in Fig. 1.

A pure PEN state has the form

$$\rho_{\vec{A}} = \bigotimes_{e \in \mathcal{E}} |\psi_e\rangle \langle \psi_e| \tag{6}$$

If $\rho_{\vec{A}}$ is a mixed state, then, for each ρ_e in Eq. (5), there exists a purification $|\psi_{e,E_e}\rangle \langle \psi_{e,E_e}|$, with E_e being the purifying system. The purification $\rho_{\vec{A}E}$ of the state $\rho_{\vec{A}}$ is given by

$$\rho_{\vec{A}E} = \bigotimes_{e \in \mathcal{E}} |\psi_{e,E_e}\rangle \langle \psi_{e,E_e}| \, . \tag{7}$$

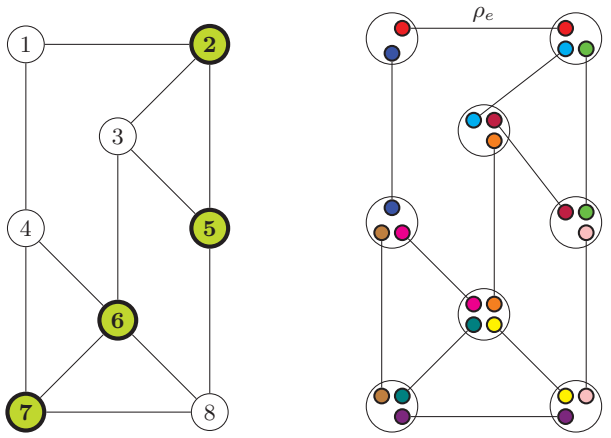


Figure 1. Left: Example for the graph of a network. The vertices (or nodes) correspond to participants and the edges correspond to bipartite entangled states between them. Vertices from the subset I of participants who want to establish a common conference key ("secrecy-seeking parties") are depicted in green. The other participants can assist them: Here the vertices 5 and 6 are connected only via the vertices outside I. Right: more detailed structure of the network and a PEN state. The "total" Hilbert space is the tensor product of the spaces corresponding to the participants. The Hilbert spaces of the participants are the tensor products of their corresponding parts of the bipartite states.

III. BOUNDS ON THE MULTIPARTITE DEVETAK-WINTER KEY RATE

Let us first explore a scenario when there is a distinguished party A_1 whose raw key is considered as the reference and the other participants try to fix discrepancies between their raw keys and that of A_1 (treated in this scenario as "errors"). A known achievable conference key rate for this case is the multipartite generalization of the Devetak-Winter formula [11, 31, 32]:

$$r_{\mathrm{DW}} = \max_{\substack{\mathrm{LOSR}\\ \mathrm{measurements}}} \{\min_{i=2,\ldots,N} I(X_1 : X_i) - I(X_1 : E)\} \tag{8}$$

where $I(X_1 : X_i)$ is the classical mutual information between the measurement outcomes X_1 and X_i of the parties A_1 and A_i, respectively, and $I(X_1 : E)$ is the quantum mutual information between X_1 and the eavesdropper Eve (E) [32]. Then the following bound holds for the multipartite Devetak-Winter key rate for PEN states.

Theorem 1. *Let ρ be a PEN state. Then the multipartite Devetak-Winter key rate (8) for N participants is upper bounded by*

$$r_{\mathrm{DW}}([N]) \leq \frac{S(A_1)}{N-1}, \tag{9}$$

where $S(A_1)$ is the von Neumann entropy of the reduced state of A_1. In the case of ρ being a pure state (see Eq. (6)) and A_1 connected to all other users, this bound can be reached by a bipartite QKD strategy.

The proof can be found in Appendix A. The theorem shows that no conference key agreement protocol should outperform the simple bipartite QKD protocol, where one party constructs a private key with each other party individually and merges them into a final mutual key shared by all parties.

As an example, consider the PEN state corresponding to the graph depicted in the left part of Fig. 3, where each edge corresponds to one Bell pair. Then $S(A_1) = 2$ and Theorem 1 gives $r_{\mathrm{DW}} \leq 1$. To see that the bound is tight let A_1 run a perfect bipartite QKD strategy separately with A_2 and A_3, producing one-bit keys K_{12} and K_{13}. If we take the conference key to be $K := K_{12}$ and let A_1 publicly announce $K_{12} \oplus K_{13}$, A_3 can reconstruct K_{12}, so all three parties share the same secret bit at rate 1, and the announcement reveals nothing about K to Eve.

Let us impose a further restriction on the scenario and consider the multipartite version of the BB84 protocol [11, 13]. Ideally, this protocol assumes a GHZ state (not a PEN state) distributed at each round. However, using PEN states and LOSR maps, states that can be interpreted as noisy versions of the GHZ state can be generated. Upper bounds on fidelities of such states with the GHZ state can be found in Ref. [24, 35]. First, the users map their systems into qubits using LOSR transformations and then measure them and postprocess measurements according to the multipartite BB84 protocol. We denote the corresponding rate as r_{BB84}.

Interestingly, in Ref. [25, 26], it was shown that even biseparable qubit states can lead to nonzero conference key rate, i.e., genuine multipartite entanglement is not a prerequisite for conference key agreement. On the other hand, LOSR transformations of PEN states lead to a strictly larger class of quantum states including genuinely multipartite entangled states with larger GHZ state fidelity.

In the following theorem, however, we show that r_{BB84} cannot outperform the conference key rate for biseparable states.

Theorem 2. *Let ρ be a tripartite qubit state which can be prepared in PEN with 3 nodes (see the left part of Fig. 3). Then the maximal rate for conference key agreement with a multipartite BB84 protocol is*

$$\max_{\rho\in\mathrm{PEN}} r_{\mathrm{BB84}}([N=3]) = 1 - h\left(\frac{1}{4}\right) \approx 0.188, \tag{10}$$

where h is the binary entropy function.

The proof can be found in Appendix B. The right-hand side of Eq. (10) can be achieved by biseparable states, which was shown in Ref. [25].

IV. BOUNDS ON THE DISTILLABLE CONFERENCE KEY BASED ON BIPARTITIONS

In the previous section we considered the multipartite Devetak-Winter key rate formula for many participants. We mentioned that this formula corresponds to the scenario with one distinguished participant. If the network is decentralized, this is too restrictive. More general key agreement protocols of conference key agreement by public discussion in decentralized networks were studied in classical information theory [28, 29, 34]. Consider the PEN state corresponding to the graph depicted in the left part of Fig. 1, where each edge corresponds to the generation of one Bell pair per round. We mentioned that the upper bound for the multipartite Devetak-Winter key rate is 1. In the following we will show that the actual distillable conference key here is 3/2.

We start with an obvious bound on the distillable conference key for pure PEN states (6). Recall that a cut of a graph is a set of edges whose removal breaks the graph into two disconnected parts (sides of the cut) [36]. We say that a cut is I-proper if each of its sides contains at least one vertex from the set $I \subset [N]$.

Proposition 1. *Consider a pure PEN state (6) and denote S_e the entanglement entropy of the edge bipartite states $|\psi_e\rangle$. Then*

$$\overline{r}_{\text{key}}(A_I) \leq \min_{I\text{-proper cut } C} \sum_{e\in C} S_e, \tag{11}$$

where the minimum is taken over all I-proper cuts C.

Thus, the distillable conference key is upper bounded by the total entanglement entropy of the "weakest" cut.

Proof. Consider the I-proper cut C. Consider the problem of bipartite secret key distillation between the two subsets in this partition, i.e., we treat all vertices from each set as one "aggregated" participant and we allow them to perform collective operations. If a conference key for the subset I is established, then, obviously, it can be viewed as a bipartite secret key between these two subsets. Hence, the distillable conference key cannot exceed this distillable bipartite key. As is well-known, the bipartite distillable key is upper bounded by the relative entropy of entanglement [17, 37], which, in turn, in the case of a pure state, is equal to the entanglement entropy. For a pure PEN-state (6) considered as a bipartite state between the two subsets in a bipartition of $[N]$, the entanglement entropy is the sum of the bipartite entanglement entropies S_e over the edges e from the cut (Fig. 2). Minimization over the I-proper cuts gives the right-hand side of Eq. (11). □

In Ref. [19], the following upper bound for the distillable conference key for the case $I = [N]$ (i.e., all participants want to have a conference key) was proved:

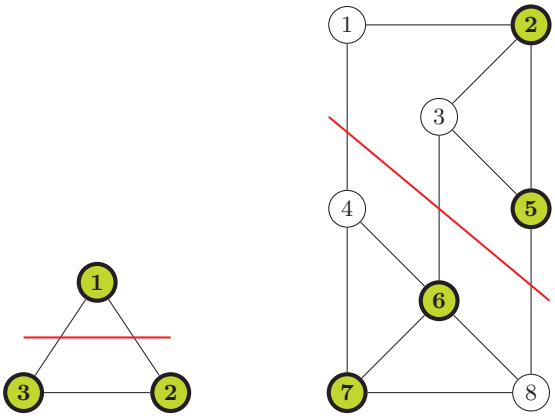


Figure 2. Illustration of Proposition 1. Here each edge corresponds to one Bell pair. A simple bound on the distillable conference rate is given by a "weakest" cut: If we find a cut of the graph such that both parts contain vertices from I (secrecy-seeking parties, depicted in green), then the distillable conference key cannot be larger than the distillable bipartite key corresponding to this bipartition, which is equal to the total entanglement entropy of the edges from the cut. The weakest cuts depicted in the figure give the bound $\overline{r} \leq 2$ for the network to the left and the bound $\overline{r} \leq 3$ for the network to the right. However, these bounds are not tight, see Fig. 3.

$$r_{\text{key}}(\vec{A}) \leq \lim_{n\to\infty} \frac{1}{n} \min_{\sigma\in\text{BISEP}} D(\rho_{\vec{A}}^{\otimes n} \| \sigma). \tag{12}$$

The quantity $\min_{\sigma\in\text{BISEP}} D(\rho\|\sigma)$ is called the relative entropy of genuine multipartite entanglement (GME) of ρ and the right-hand side of Ineq. (12) is its regularized version.

In the case of pure PEN states, the bound (12) is reduced to the bound (11). Namely, the following statement, which we prove in Appendix C, holds.

Theorem 3. *Given a pure PEN state $\rho_{\vec{A}}$,*

$$\min_{\sigma\in\text{BISEP}} D(\rho\|\sigma) = \min_{I\text{-proper cut } C} \sum_{e\in C} S_e. \tag{13}$$

Thus, for PEN states, the bound (12) reduces to the weakest cut (vertex bipartition). Fig. 2 illustrates the weakest-cut bound (11), but, as we will see in the next sections and in Fig. 3, these bounds are not tight. Namely, for the triangle graph the "weakest" cut gives an upper bound of 2 for the distillable conference key, while the actual distillable conference key is (as we will see) 3/2.

Let us also note that upper bounds on the distillable conference key based on multipartite generalizations of squashed entanglement were proposed [38, 39]. However, these bounds applied to the PEN states correspond to the "weakest" cut bound.

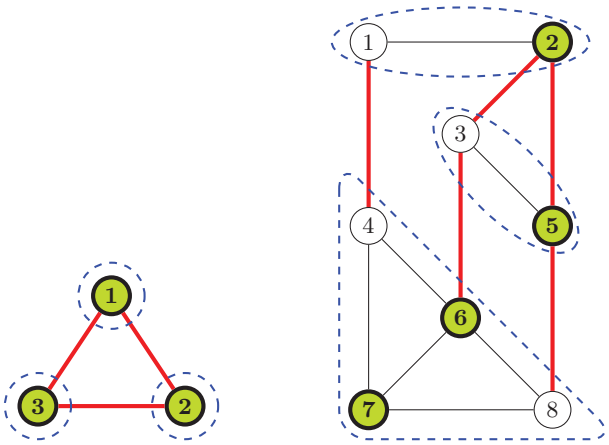


Figure 3. Illustration of Theorems 4 and 5. These theorems include the minimization over all vertex partitions such that each subset intersects with I (secrecy-seeking parties, depicted in green). We consider arbitrary vertex partitions of the graphs and the partition subsets are encircled by blue dashed curves. For PEN states, the total entanglement entropy (if the state is pure) or the total entanglement cost (if the state is mixed) of the cross edges (i.e., edges connecting different partition subsets, depicted in red) gives an upper bound for the distillable conference key (see Eq. (16)). If each edge corresponds to a Bell pair, then, according to Theorem 4, the partitions depicted here give stronger bounds than the estimates based on the weakest cuts (see Fig. 2): $\overline{r} \leq 3/2$ for the network to the left and the bound $\overline{r} \leq 5/2$ for the network to the right.

V. BOUNDS ON THE DISTILLABLE CONFERENCE KEY BASED ON ARBITRARY PARTITION

Consider a partition

$$\mathcal{P} = \{J_1, \ldots, J_p\} \tag{14}$$

of the set $[N]$ into disjoint subsets such that all $J_\alpha \cap I$, $\alpha = 1, \ldots, p$, are nonempty. We will refer to such partitions as *I-proper* partitions (thus generalizing the I-proper bipartition from Sec. IV). Also denote $|\mathcal{P}| = p$ the number of the partition sets.

Let us illustrate the condition on a proper partition. Let $N = 4$ and $I = 1, 2, 3$. Then the partition of the set $\{1, 2, 3, 4\}$ into the subsets $\{1, 2\}$ and $\{3, 4\}$ is I-proper, while the partition into the subsets $\{1, 2\}$, $\{3\}$, and $\{4\}$ is not proper because the last subset does not intersect with I. Examples of proper partitions are depicted in Fig. 3.

For a vertex partition $\mathcal{P}$, denote $\mathcal{E}(\mathcal{P})$ the set of edges connecting vertices from different subsets in the vertex partition $\mathcal{P}$.

Theorem 4. *Let*

$$\rho_{\vec{A}} = \bigotimes_{e \in \mathcal{E}} |\psi_e\rangle \langle\psi_e| \tag{15}$$

be a pure PEN state [cf. Eq. (5)]. Then

$$\overline{r}_{\text{key}}(A_I) \leq \min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_{e \in \mathcal{E}(\mathcal{P})} S_e, \tag{16}$$

where S_e is the entanglement entropy of the bipartite state $|\psi_e\rangle$ and the minimum is taken over I-proper partitions $\mathcal{P}$.

The upper bound (16) is depicted in Fig. 3. The proof is based on the estimation of the maximal total correlation (a multipartite generalization of the mutual information) of the outcomes of local measurements (see Appendix D).

Remark 1. If $|I| = N$, i.e., all participants are secrecy-seeking, then the bound (16) is tight and achieved by the optimal spanning-tree-packing protocol, see [30] and papers from classical information theory [28, 29]. Namely, for each edge e, the distillable bipartite secret key for the state $|\psi_e\rangle$ is equal to S_e. Then, to get a conference key from the resulting network of bipartite secret keys, we use the optimal secret key packing. This means that, in this case, collective measurements of states coming from different sources or collective postprocessing do not give advantage: Doing pairwise bipartite QKD and then merging the bipartite keys into a conference key is an optimal strategy in PEN networks.

We can generalize Theorem 4 to the case of arbitrary (mixed) PEN states as follows:

Theorem 5. *Let $\rho_{\vec{A}}$ be a PEN state (5). Then*

$$\overline{r}_{\text{key}}(A_I) \leq \min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_{e \in \mathcal{E}(\mathcal{P})} E_{\text{F}}^{\infty}(\rho_e), \tag{17}$$

where E_{F}^{∞} denotes the regularized entanglement of formation and the minimum is taken over I-proper partitions $\mathcal{P}$.

The proof can be found in Appendix E. Recall that the entanglement of formation $E_{\text{F}}(\rho_{AB})$ of the bipartite state ρ_{AB} is defined as

$$E_{\text{F}}(\rho_{AB}) = \inf \Big\{ \sum_{\alpha} p_\alpha S_{\text{ent}}(|\psi_\alpha\rangle_{AB}) \Big\}, \tag{18}$$

where the infimum is taken over decompositions

$$\rho_{AB} = \sum_{\alpha} p_\alpha |\psi_\alpha\rangle_{AB} \langle\psi_\alpha| \tag{19}$$

and $S_{\text{ent}}(|\psi_\alpha\rangle_{AB})$ denotes the entanglement entropy of the pure state $|\psi_\alpha\rangle_{AB}$. The regularized entropy of formation is defined as

$$E_{\text{F}}^{\infty}(\rho_{AB}) = \lim_{n \to \infty} \frac{1}{n} E_{\text{F}}(\rho_{AB}^{\otimes n}). \tag{20}$$

Note that, in the bipartite scenario, it is known that the entanglement cost (equal to the regularized entanglement of formation) is an upper bound for the distillable

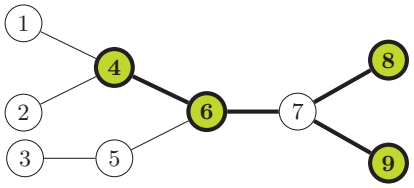


Figure 4. Tree network. The subgraph induced by the vertices 4 and 6–9 constitutes the minimal tree containing the picked vertices. Then the distillable conference key is equal to the minimal bipartite distillable key in this "shortened tree". Vertices 1, 2, 3, and 5 do not connect any picked vertices, hence, they cannot assist the distillation task and their edges are unimportant.

key [17, 40]. Appendix E contains another proof of this fact, which is based on typical sequences (sketched in Ref. [40]).

Finally, let us make the following simple observation about the distillable conference key for the case when the network graph is a tree, i.e., contains no cycles.

Proposition 2. *Let the network graph $(\mathcal{V},\mathcal{E})$ be a tree and r_e, $e\in\mathcal{E}$, be the bipartite distillable key for the (general) state ρ_e. Then, the distillable conference key $\overline{r}_{\text{key}}(A_I)$ is given by*

$$\overline{r}(A_I)=\min_{e\in\widetilde{\mathcal{E}}} r_e, \tag{21}$$

where $\widetilde{\mathcal{E}}$ is the set of edges in the minimal subtree $(\widetilde{\mathcal{V}},\widetilde{\mathcal{E}})$ of the tree graph $([N],\mathcal{E})$ for which $I\subset\widetilde{\mathcal{V}}$ (see Fig. 4).

Proof. From one side, we can repeat the proof of Proposition 1 that the distillable conference key cannot increase the bipartite distillable key for any vertex bipartition. Removal of any edge breaks a tree into two disconnected parts. I-proper bipartitions correspond to removal of the edges from $\widetilde{\mathcal{E}}$. Hence, $\overline{r}(A_I)\leq r_e$ for all e defining an I-proper bipartition.

From the other side, if r_{e^*} is the minimal bipartite distillable key among the edges from $\widetilde{\mathcal{E}}$, then all other bipartite links from $\widetilde{\mathcal{E}}$ can work at least with the same distillation rate providing the conference distillation rate r_{e^*}. □

Remark 2. Let us recall that we assumed the helpers to be trusted, i.e., they may also know the conference key or a part of it. Let us now consider the case of untrusted helpers who are not allowed to get any information about the conference key. Of course, the derived upper bounds are still valid in the case of increased restrictions. However, even in the networks like in Fig. 4, where the subsets $\{4,6\}$ and $\{8,9\}$ of the secrecy-seeking parties are separated by the helper node 7, generation of a conference key which is private also to helpers can be possible. In the classical case this is obviously impossible because any communication between these two subsets flows through the untrusted node 7. In the quantum case, the parties can distill a certain number of Bell pairs from all necessary bipartite links (under the condition that it is possible) and then the node 7 performs GHZ measurements creating GHZ correlations between the nodes 6, 8, and 9. This allows the secrecy-seeking parties to establish a conference key private also from the node 7. The node 6, 8 and 9 can verify the GHZ-type correlation such that node 7 cannot cheat.

Thus, in the presence of untrusted nodes, genuinely multipartite quantum conference key agreement protocols (rather than putting together the bipartite ones) might be necessary. This aligns with the example of the advantage from the use of genuinely multipartite protocols from Ref. [11]. A more detailed analysis of conference key agreement in pair-entangled networks with untrusted nodes is a subject for future research.

VI. CONCLUSIONS AND DISCUSSION

We have studied the task of conference key agreement in pair-entangled networks (PEN), where the global network state consists of bipartite entangled states shared along the edges of a network graph. Networks we considered are memory-free: Each node measures its incoming quantum systems immediately after possible local operations with shared randomness (LOSR) and uses public classical communication afterwards.

We derived an upper bound on the multipartite Devetak-Winter key rate implying that a simple pairwise QKD strategy saturates the bound on fully connected graphs. This aligns with broader evidence that highly resourceful multipartite states are hard to create in LOSR networks (see Theorem 1).

Next, we showed that for the multipartite BB84 protocol in a 3-node PEN, no LOSR state generated in the network outperforms the best biseparable resource (see Theorem 2). This already signals that straightforward GHZ-based approaches yield no rate advantage in PENs.

We then considered the most general conference key distillation protocols not requiring a central distinguished node and have derived upper bounds depending on the network topology and degree of entanglement of the source. Theorem 4 gives us an upper bound for pure PEN states and Theorem 5 generalizes this bound to the case of mixed PEN states. These bounds are based on simple partition structures of the network and they have been shown to be stronger than previously known cut-based bounds.

Moreover, in the case of pure states and all nodes being the secrecy-seeking parties (no helpers), we have shown that the obtained bounds are tight and can be achieved by individual measurements followed by the spanning-tree-packing algorithm of conference key propagation from previous work [30] and also known in classical network information theory [28, 29]. In particular, this means that collective measurements and collective postprocessing do not give an advantage in this case and,

although, in principle, many different multipartite strategies might be considered in a quantum network, the optimal approach is remarkably simple.

We have also provided a calculation of the relative entropy of genuine multipartite entanglement and showed that for pure pairwise entangled network states it is reduced to the minimal entanglement entropy of vertex bipartitions (Theorem 3). This result can be viewed as a multipartite generalization of the well-known fact that the relative entropy of (bipartite) entanglement of a pure bipartite state is equal to its entanglement entropy.

Two open questions can be suggested for the future. First, in the case of a pure PEN state, but in the presence of helpers, is the strategy of bipartite distillation protocols followed by merging the bipartite keys into a conference one still optimal? The second open question is whether the entropy of formation in Theorem 5 can be replaced by other upper bounds for bipartite distillable key, e.g., the (bipartite) relative entropy of entanglement or squashed entanglement.

ACKNOWLEDGMENTS

We thank Giacomo Carrara and Tulja Varun Kondra for helpful discussions. This work was funded by the Federal Ministry of Research, Technology and Space BMFTR (Project QuKuK, Grant No. 16KIS1618K). J.N., H.K., and D.B. also acknowledge support by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769. A.T. acknowledges support by BMFTR (Project QR.N, Grant No. 16KIS2196).

Appendix A: Proof of Theorem 1

Proof of Theorem 1. Consider a network with bipartite source states and local operations. Then

$$r_{DW} \leq \min_{i=2,\ldots,N}\{I(A_1:A_i)\} \tag{A1}$$

$$\leq \frac{\sum_{i=1}^{N-1} I(A_1:A_i)}{N-1} \tag{A2}$$

$$\leq \frac{H(A)}{N-1}, \tag{A3}$$

where in the last step we use the result from [41]. The tightness can be shown by performing a bipartite QKD strategy, where the party A_1 generates a perfect private key with the other parties separately and combines them into one single shared conference key. □

Appendix B: Proof of Theorem 2

The asymptotic key-rate in the BB84-protocol can be written as

$$r_{\mathrm{BB84}} = 1 - h\left(\frac{1-\langle X_A X_B X_C\rangle}{2}\right) - \max\left\{h\left(\frac{1-\langle Z_A Z_B\rangle}{2}\right), h\left(\frac{1-\langle Z_A Z_C\rangle}{2}\right)\right\}$$

where $h(x)$ is the binary entropy [33].
Here we use the shorthand notation for Pauli strings e.g. $X_A X_B X_C = \sigma_x \otimes \sigma_x \otimes \sigma_x$. To derive an upper bound for the asymptotic conference key-rate we can make use of the inflation technique, a tool that allows us to derive restrictions based on the network structure [42, 43]. It was shown in [42] that in a PEN with 3 nodes that the constraint

$$|\langle Z_A Z_B\rangle| + |\langle Z_A Z_C\rangle| \leq 1 + |\langle Z_B\rangle|\,|\langle Z_C\rangle|$$

has to be met. Together with the uncertainty relation (see [44]) $\langle X_A X_B X_C\rangle^2 + \langle Z_i\rangle\langle Z_j\rangle \leq 1$ with $i,j \in \{A,B,C\}$ we obtain

$$\langle X_A X_B X_C\rangle^2 + 2\min\{\langle Z_A Z_B\rangle, \langle Z_A Z_C\rangle\} \leq 2.$$

This is an improved condition of [23] for the preparability of a state in a network with bipartite source states. With that we get the following upper bound for the asymptotic key-rate

$$r_{\mathrm{BB84}} \leq 1 - h\left(\frac{1}{4}\right) \approx 0.188,$$

which turns out to be a tight bound. For instance, the state

$$\rho = \frac{1}{2}\left(|\phi^+\rangle\langle\phi^+|_{AB} \otimes |+\rangle\langle+|_C + |\phi^+\rangle\langle\phi^+|_{AC} \otimes |+\rangle\langle+|_B\right)$$

gives rise to a key-rate of $1 - h\left(\frac{1}{4}\right)$ (see [25]).

Appendix C: Proof of Theorem 3

The proof follows (generalizes) one of the proofs that the relative entropy of (bipartite) entanglement for pure states is equal to the entanglement entropy given in Ref. [45]. But a difference with respect to the bipartite case is that we need to consider different cuts of a multipartite entangled state into a product of two parts. Our generalization of the proof from Ref. [45] works only for the case when the bipartite pure states $|\psi_e\rangle$ in Eq. (6) are maximally entangled. So we start with this case and return to the general case later. The case of the general $|\psi_e\rangle$ can be reduced to the case of the maximally entangled $|\psi_e\rangle$ by the entanglement purification.

Lemma 1. *The statement of Theorem 3 is true if $|\psi_e\rangle$ in Eq. (6) are maximally entangled on the corresponding Hilbert spaces $\mathcal{H}_e$:*

$$|\psi_e\rangle = |\Phi_e\rangle := \frac{1}{\sqrt{d_e}} \sum_{n_e=1}^{d_e} |n_e\rangle\,|n_e\rangle \tag{C1}$$

for some bases $|n_e\rangle$ in the corresponding Hilbert spaces.

That is, the basis $|n_e\rangle$ in each Hilbert space is not the computational basis, but the basis specified by the Schmidt decomposition of $|\psi_e\rangle$. For short, we will also write $|n_e\rangle\,|n_e\rangle = |n_e n_e\rangle$.

Proof. Consider two arbitrary (generally mixed) states $\sigma_{\vec{A}}$ and $\sigma^*_{\vec{A}}$ and the function

$$f(x) = (\ln 2)\, D(\rho_{\vec{A}} \,\|\, (1-x)\sigma^*_{\vec{A}} + x\sigma_{\vec{A}}). \tag{C2}$$

Here $\sigma^*_{\vec{A}}$ will be our guess for the minimum of the relative entropy, i.e. is treated as a fixed biseparable state and $\sigma_{\vec{A}}$ is a variable biseparable function. We will be interested in $f'(0)$, which is thus the directional derivative of the quantum relative entropy (up to a constant factor or, equivalently, base of the logarithm) with respect to $\sigma_{\vec{A}}$ in the point $\sigma^*_{\vec{A}}$. For simplicity, we will drop the subindex $\vec{A}$.

Using the representation

$$\ln a = \int_0^\infty \frac{at-1}{a+t} \cdot \frac{dt}{1+t^2}, \tag{C3}$$

it can be shown [45, 46] that the derivative of the function $f(x)$ in the point $x = 0$ is

$$f'(0) = 1 - \int_0^\infty \mathrm{Tr}\left(\frac{1}{\sigma^*+t}\,\rho\,\frac{1}{\sigma^*+t}\,\sigma\right) dt \tag{C4}$$

for $x \in [0,1]$.

Set

$$\sigma^* = \bigotimes_{e\in C^*} \sigma^*_e \otimes \bigotimes_{e\notin C^*} |\psi_e\rangle\langle\psi_e| \tag{C5}$$

for some cut C^* (to be fixed later), where

$$\sigma^*_e = \frac{1}{d_e} \sum_{n_e=1}^{d_e} |n_e n_e\rangle\langle n_e n_e|\,. \tag{C6}$$

σ^* is our guess for minimum for a proper C^*. It is straightforward to calculate that

$$D(\rho\,\|\,\sigma^*) = \sum_{e\in C^*} S_e = \sum_{e\in C^*} \log d_e. \tag{C7}$$

Also,

$$\frac{1}{\sigma^*+t} = \frac{1}{\prod\limits_{e\in C^*} d_e^{-1} + t} \bigotimes_{e\in C^*} \left(\sum_{n_e=1}^{d_e} |n_e n_e\rangle\langle n_e n_e|\right) \otimes \bigotimes_{e\notin C^*} |\Phi_e\rangle\langle\Phi_e| \tag{C8}$$

and

$$\frac{1}{\sigma^*+t}\,\rho\,\frac{1}{\sigma^*+t} = \frac{\prod\limits_{e\in C^*} d_e^{-1}}{\left(\prod\limits_{e\in C^*} d_e^{-1} + t\right)^2} \times \bigotimes_{e\in C^*} \left(\sum_{n_e,m_e=1}^{d_e} |n_e n_e\rangle\langle m_e m_e|\right) \otimes \bigotimes_{e\notin C^*} |\Phi_e\rangle\langle\Phi_e| \tag{C9}$$

Let now $\sigma = |\varphi\rangle\langle\varphi|$ be a pure biseparable state. This means that it is separable with respect to a certain vertex partition. Denote the corresponding cut as C. Then $|\varphi\rangle$ can be written as

$$|\varphi\rangle = \bigotimes_{e\in C} |\alpha_e\rangle\,|\beta_e\rangle \otimes \bigotimes_{e\notin C} |\varphi_e\rangle\,, \tag{C10}$$

where $|\varphi_e\rangle$ are arbitrary (generally, entangled) bipartite states from the Hilbert spaces $\mathcal{H}_e$, and $|\alpha_e\rangle\,|\beta_e\rangle$ are pure separable states on $\mathcal{H}_e$:

$$|\alpha_e\rangle = \sum_{n_e=1}^{d_e} a^e_{n_e} |n_e\rangle\,, \qquad |\beta_e\rangle = \sum_{n_e=1}^{d_e} b^e_{n_e} |n_e\rangle\,. \tag{C11}$$

Substitution of Eqs. (C9), (C10), and (C11) into Eq. (C4) gives

$$\begin{aligned} 1 - f'(0) = {} & \bigotimes_{e\in C^*\cap C} \sum_{n_e,m_e=1}^{d_e} \overline{a^e_{n_e} b^e_{n_e}}\, a^e_{m_e} b^e_{m_e} \\ & \otimes \bigotimes_{e\in C^*\setminus C} \sum_{n_e,m_e=1}^{d_e} \langle m_e m_e|\varphi_e\rangle\langle\varphi_e|n_e n_e\rangle \\ & \otimes \bigotimes_{e\in C\setminus C^*} \frac{1}{d_e} \sum_{n_e,m_e=1}^{d_e} \overline{a^e_{n_e} b^e_{n_e}}\, a^e_{m_e} b^e_{m_e} \\ & \otimes \bigotimes_{e\notin C\cup C^*} |\langle\Phi_e|\varphi_e\rangle|^2, \end{aligned} \tag{C12}$$

where we have taken into account that $\int_0^\infty \frac{c\,dt}{(c+t)^2} = 1$.

Now estimate the absolute values of the all four groups of terms in Eq. (C12). For the fourth line we apply the bound $|\langle\Phi_e|\varphi_e\rangle| \le 1$. For the first and the third lines we apply the Cauchy-Bunyakovsky-Schwarz inequality:

$$\begin{aligned} \left|\sum_{n_e,m_e=1}^{d_e} \overline{a^e_{n_e} b^e_{n_e}}\, a^e_{m_e} b^e_{m_e}\right| &\le \left(\sum_{n_e=1}^{d_e} |a^e_{n_e} b^e_{n_e}|\right)^2 \\ &\le \left(\sum_{n_e=1}^{d_e} |a^e_{n_e}|^2\right)\left(\sum_{n_e=1}^{d_e} |b^e_{n_e}|^2\right) \\ &= 1. \end{aligned} \tag{C13}$$

For the second line of Eq. (C12), we consider the maximization problem

$$\sum_{n_e=1}^{d_e} |\langle n_e n_e|\varphi_e\rangle| \to \max \tag{C14}$$

such that

$$\sum_{n_e=1}^{d_e} |\langle n_e n_e|\varphi_e\rangle|^2 \leq 1. \tag{C15}$$

Its solution is $|\langle n_e n_e|\varphi_e\rangle| = 1/\sqrt{d_e}$ giving

$$\sum_{n_e,m_e=1}^{d_e} |\langle m_e m_e|\varphi_e\rangle\langle\varphi_e|n_e n_e\rangle| = \left(\sum_{n_e=1}^{d_e} |\langle n_e n_e|\varphi_e\rangle|\right)^2 \leq d_e. \tag{C16}$$

Putting it all together, we obtain

$$|1 - f'(0)| \leq \frac{\prod\limits_{e\in C^*\setminus C} d_e}{\prod\limits_{e\in C\setminus C^*} d_e} = \frac{\prod\limits_{e\in C^*} d_e}{\prod\limits_{e\in C} d_e}. \tag{C17}$$

Now let us choose C^* such that

$$\prod_{e\in C^*} d_e = \min_{\text{cuts } C} \prod_{e\in C} d_e, \tag{C18}$$

or, equivalently,

$$\sum_{e\in C^*} \log d_e = \min_{\text{cuts } C} \sum_{e\in C} \log d_e. \tag{C19}$$

Then $|1 - f'(0)| \leq 1$ and, hence, $f'(0) \geq 0$ for all pure biseparable σ. Since $f'(0)$ is linear in σ and every biseparable state is a convex combination of pure biseparable states, the inequality $f'(0) \geq 0$ holds for all biseparable σ. Together with the convexity of the quantum relative entropy in Eq. (C2), this means that σ^* provides minimum to the quantum relative entropy over all biseparable states. Together with Eq. (C7), this means that the statement of Proposition 3 is true if $|\psi_e\rangle$ are maximally entangled states (C1).

□

Consider now the case of a general $|\psi_e\rangle$. Consider again their Schmidt decomposition:

$$|\psi_e\rangle = \sum_{n_e=1}^{d_e} \sqrt{p^e_{n_e}}\, |n_e n_e\rangle\,. \tag{C20}$$

As a guess for the minimum of the relative entropy, we again consider the state σ^* (C5), where

$$\sigma^*_e = \sum_{n_e=1}^{d_e} \sqrt{p^e_{n_e}}\, |n_e n_e\rangle\langle n_e n_e| \tag{C21}$$

and C^* is chosen such that

$$\sum_{e\in C^*} S_e = \min_{\text{cuts } C} \sum_{e\in C} S_e. \tag{C22}$$

The direct calculation shows that

$$D(\rho_{\vec{A}} \| \sigma^*_{\vec{A}}) = \sum_{e\in C^*} S_e. \tag{C23}$$

So, we need to show that the relative entropy of entanglement does not exceed the right-hand side of Eq. (C23).

As is well-known [17, 37], the distillable (bipartite) entanglement of the pure state $|\psi_e\rangle$ is equal to its entanglement entropy S_e. This means that, for every $\varepsilon > 0$ and every $\delta > 0$, there exists a family of LOCC maps $\Lambda_e^{(n)}$ acting on n copies of $|\psi_e\rangle\langle\psi_e|$ such that

$$\|\Lambda_e^{(n)}(|\psi_e\rangle\langle\psi_e|^{\otimes n}) - |\Phi_e\rangle\langle\Phi_e|^{\otimes\lfloor n(S_e-\delta)\rfloor}\| \leq \frac{\varepsilon}{|\mathcal{E}|} \tag{C24}$$

for all sufficiently large n. Composition of $\Lambda_e^{(n)}$ for all e constitutes the map $\Lambda^{(n)}$ acting on n copies of the PEN state $\rho_{\vec{A}}$, see Eq. (6). Then

$$\|\Lambda(n)(\rho_{\vec{A}}^{\otimes n}) - \tau_{\vec{A}}^{(n)}\| \leq \varepsilon, \tag{C25}$$

where

$$\tau_{\vec{A}}^{(n)} = \bigotimes_{e\in\mathcal{E}} |\Phi_e\rangle\langle\Phi_e|^{\otimes\lfloor n(S_e-\delta)\rfloor}\,. \tag{C26}$$

We have the following chain:

$$\begin{aligned} E_{\text{GME}}(\rho_{\vec{A}}) &\geq \frac{1}{n} E_{\text{GME}}(\rho_{\vec{A}}^{\otimes n}) \\ &\geq \frac{1}{n} E_{\text{GME}}\big(\Lambda^{(n)}(\rho_{\vec{A}}^{\otimes n})\big) \\ &\geq \frac{1}{n}[E_{\text{GME}}(\tau_{\vec{A}}^{(n)}) - g(\varepsilon, n)] \\ &= \frac{1}{n}\left[\min_C \sum_{e\in C} \lfloor n(S_e - \delta)\rfloor - g(\varepsilon, n)\right] \\ &\geq \min_C \sum_{e\in C} \left(S_e - \delta - \frac{1}{n}\right) - \frac{g(\varepsilon, n)}{n}, \end{aligned} \tag{C27}$$

where

$$g(\varepsilon, n) = 2\varepsilon \log\left(\prod_{e\in\mathcal{E}} d_e^{\lfloor n(S_e-\delta)\rfloor}\right) - 2\varepsilon\log\varepsilon + 4\varepsilon. \tag{C28}$$

The first inequality in chain (C27) follows from the definition of the relative entropy of GME (it is the standard regularization procedure). In the second inequality, we have used the monotonicity of the relative entropy of GME E_{GME} under LOCC maps. The third inequality is the continuity bound for such kind of quantities (relative entropy with respect to a certain class of density operators) [47]. In the fourth line, we have used the proved statement (Lemma 1) about the relative entropy of GME for PEN states of form (C26) and the minimum is taken over cuts C. The last inequality is due to the rounding operation.

Since δ, ε, $g(\varepsilon,n)/n$, and $1/n$ can be made arbitrarily small, we conclude that

$$E_{\mathrm{GME}}(\rho_{\vec{A}}) \geq \min_{C} \sum_{e\in C} S_e. \tag{C29}$$

Together with Eq. (C23), this gives the required statement.

Appendix D: Proof of Theorem 4

Since we consider pure $\rho_{\vec{A}}$, there is now Eve's register E in Eq. (3); the only Eve's knowledge is classical communication (and shared randomness), i.e., register C. Consider first the case of no shared randomness, i.e., no λ. For an arbitrary partition $\mathcal{P}$ (14), denote the maximal total correlation of the outcomes of local measurements

$$\begin{aligned} I_{\mathrm{loc}}(\mathcal{P}) &\equiv I_{\mathrm{loc}}(A_{J_1} : A_{J_2} : \ldots : A_{J_p}) \\ &= \max I(X_{J_1} : X_{J_2} : \ldots : X_{J_p}), \end{aligned} \tag{D1}$$

where the maximum is taken over $\mathcal{P}$-local POVMs (i.e., collective measurements inside the subsets $J_\alpha \in \mathcal{P}$ are allowed) and X_{J_α}, $\alpha = 1,\ldots,p$, denote the random variables corresponding to the measurement outcomes. Here

$$I(X_{J_1} : \ldots : X_{J_p}) = \sum_{\alpha=1}^{p} H(X_{J_1}) - H(X_{J_1}\ldots X_{J_p}) \geq 0 \tag{D2}$$

is the total correlation (a multipartite generalization of the mutual information) and H denotes the Shannon entropy of a random variable.

If we include shared randomness λ, we will be interested in the corresponding conditional quantity conditioned on λ:

$$\begin{aligned} I_{\mathrm{loc}}(\mathcal{P}|L) &\equiv I_{\mathrm{loc}}(A_{J_1} : A_{J_2} : \ldots : A_{J_p}|L) \\ &= \max I(X_{J_1} : X_{J_2} : \ldots : X_{J_p}|L), \end{aligned} \tag{D3}$$

where the maximum is taken over all $\mathcal{P}$-local measurements with shared randomness and L is the shared randomness as a random variable (in contrast to λ, which denotes a concrete value of it). Here,

$$\begin{aligned} I(X_{J_1} : \ldots : X_{J_p}|C) &= \sum_{\alpha=1}^{p} H(X_{J_1}|C) - H(X_{J_1}\ldots X_{J_p}|C) \\ &= \sum_{c\in\mathcal{C}} P(C=c) I(X_{J_1} : \ldots : X_{J_p}|C=c) \end{aligned} \tag{D4}$$

is the conditional total correlation for an arbitrary random variable C taking values on the set $\mathcal{C}$. In our case this is classical communication, which includes the public randomness. Due to the last line in Eq. (D4), the maximization in Eq. (D3) is reduced to the maximization over $\mathcal{P}$-local POVMs without shared randomness. In other words, shared randomness does not give advantage for the maximization of information. So, in the following, we will consider the maximal total correlation (D1) without shared randomness.

Consider first the case of two parties $A_1 = A$ ("Alice") and $A_2 = B$ ("Bob") and a pure bipartite state $|\psi_{AB}\rangle$. Denote $\rho_A = \mathrm{Tr}_B |\psi_{AB}\rangle\langle\psi_{AB}|$ and $\rho_B = \mathrm{Tr}_A |\psi_{AB}\rangle\langle\psi_{AB}|$. Denote also $S(\varrho)$ the von Neumann entropy of an arbitrary density operator ϱ.

The fact from the following lemma is well-known since it is actually a reformulation of the statement that the accessible information for an ensemble of quantum states cannot be greater than the Holevo information of this ensemble [48].

Lemma 2. *Let $|\psi_{AB}\rangle$ be a pure bipartite state. Then*

$$I_{\mathrm{loc}}(A:B) = S(\rho_A), \tag{D5}$$

Proof. The value $S(\rho_A)$ for the maximal mutual information is obviously achieved when both A and B measure in the bases corresponding to the Schmidt decomposition of $|\psi_{AB}\rangle$. So, it suffices to prove that a higher value cannot be achieved.

We need to maximize over Alice's and Bob's local POVMs $\{M_x^A\}_{x\in\mathcal{X}}$ and $\{M_y^B\}_{y\in\mathcal{Y}}$. Denote X and Y the random variables corresponding to their outcomes. We can express the maximal mutual information as a sequential maximization:

$$I_{\mathrm{loc}}(A:B) = \max_{\{M_x^A\}} \max_{\{M_y^B\}} I(X:Y), \tag{D6}$$

where Bob's POVM can depend on Alice's one. In other words, for each Alice's POVM, we optimize over Bob's POVMs and obtain a function of Alice's POVM. Then we optimize it over Alice's POVMs.

Let p_x be the probabilities of Alice's outcomes and $\rho_B^{(x)}$ be the corresponding postmeasurement states of Bob, so that $\sum_x p_x \rho_B^{(x)} = \rho_B$. Hence, $I(X:Y)$ maximized over Bob's POVM for a fixed Alice's POVM is nothing else as the accessible information for the ensemble $\{p_x, \rho_B^{(x)}\}_{x\in\mathcal{X}}$ [48]. It is upper bounded by the Holevo quantity, which, it turn, is upper bounded by the entropy of the average state of the ensemble ρ_B:

$$\max_{\{M_y^B\}_y} I(X:Y) \leq S(\rho_B) - \sum_{x\in\mathcal{X}} p_x S(\rho_B^{(x)}) \leq S(\rho_B). \tag{D7}$$

Since this inequality is true for any Alice's POVM, we conclude that also

$$I_{\mathrm{loc}}(X:Y) \leq S(\rho_B) = S(\rho_A). \tag{D8}$$

□

Corollary 1. *Consider a more general bipartite state:*

$$\rho_{AB} = |\psi_{A'B'}\rangle\langle\psi_{A'B'}| \otimes \rho_{A''}\rho_{B''}, \tag{D9}$$

i.e., besides the pure (possibly entangled) bipartite state $|\psi_{A'B'}\rangle$, Alice and Bob have their own "private" uncoupled states $\rho_{A''}$ and $\rho_{B''}$, respectively, so that $A = (A', A'')$ and $B = (B', B'')$. Then

$$I_{\mathrm{loc}}(A : B) = S(\rho_{A'}), \tag{D10}$$

where, as before, ρ with subindices means the partial trace of $\rho_{AB} \equiv \rho_{A'A''B'B''}$ over the rest subsystems.

That is, additional "private" subsystems uncoupled from the pure bipartite state do not change the left-hand side of Eq. (D10).

Proof. The right-hand side of Ineq. (D10) is achieved when Alice and Bob again measure A' and B' in the bases corresponding to the Schmidt decomposition of $|\psi_{A'B'}\rangle$ and perform the trivial measurements (i.e., corresponding to the identity operators) on A'' and B''. The fact that this bound cannot be overcome follows from Lemma 2. Indeed, preparation of local subsystems A'' and B'' uncoupled from the entangled state $\psi_{A'B'}$ and local joint measurements on $A'A''$ and $B'B''$ falls into the general concept of local POVMs on A' and B'. □

Lemma 3. *If $|\psi_{\vec{A}}\rangle = \bigotimes_{e\in\mathcal{E}} |\psi_e\rangle$ is a pure PEN state and $\mathcal{P}$ is a partition of $[N]$ (14), then*

$$I_{\mathrm{loc}}(A_{J_1} : \ldots : A_{J_p}) \leq \sum_{e\in\mathcal{E}(\mathcal{P})} S_e. \tag{D11}$$

Proof. Let us apply the following decomposition of the multipartite mutual information:

$$\begin{aligned} I(X_{J_1} : X_{J_2} : \ldots : X_{J_p}) = {} & I(X_{J_1} : X_{J_2}) \\ & + I(X_{J_3} : X_{J_1}X_{J_2}) + \ldots \\ & + I(X_{J_p} : X_{J_1} \ldots X_{J_{p-1}}). \end{aligned} \tag{D12}$$

Thus, we have reduced the multipartite mutual information to a sum of bipartite ones.

Consider the first term $I(J_1 : J_2)$. The corresponding quantum state $\rho_{A_{J_1\cup J_2}}$ has the form (D9):

$$\rho_{A_{J_1\cup J_2}} = \bigotimes_{e\in\mathcal{E}(J_1,J_2)} |\psi_e\rangle\langle\psi_e| \otimes \rho^{(J_1,\overline{J}_2)} \otimes \rho^{(J_2,\overline{J}_1)}, \tag{D13}$$

where $\mathcal{E}(J_1, J_2) \subset \mathcal{E}$ denotes the set of edges whose one endvertex belongs to J_1 and the other one belongs to J_2 and $\rho^{(J_1,\overline{J}_2)}$ (analogously $\rho^{(J_2,\overline{J}_1)}$) denotes a state originating from vertices connecting J_1 to vertices from $\overline{J}_2 = [N]\backslash J_2$. That is, we have pure states $|\psi_e\rangle$ for the edges connecting vertices inside the subset J_1 and the partial traces of $|\psi_e\rangle\langle\psi_e|$ for the edges connecting J_1 with vertices not from J_1 or J_2. Hence, in force of Corollary 1,

$$\max I(J_1 : J_2) = \sum_{e\in\mathcal{E}(J_1,J_2)} S_e \tag{D14}$$

and the maximum is achieved on the measurements of $|\psi_e\rangle$, $e \in \mathcal{E}(J_1, J_2)$, corresponding to their Schmidt decompositions.

Analogously,

$$\begin{aligned} \max I(J_3 : J_1J_2) &= \sum_{e\in\mathcal{E}(J_1\cup J_2,J_3)} S_e, \\ &\ldots \\ \max I(J_{|\mathcal{P}|} : J_1 \ldots J_{|\mathcal{P}|-1}) &= \sum_{e\in\mathcal{E}(J_1\cup\ldots\cup J_{|\mathcal{P}|-1},J_{|\mathcal{P}|})} S_e, \end{aligned}$$

where the maxima are achieved on the measurements of $|\psi_e\rangle$ (for disjoint subsets of edges) corresponding to their Schmidt decompositions. Since $\mathcal{E}(J_1, J_2)$, $\mathcal{E}(J_1 \cup J_2, J_3)$, …, and $\mathcal{E}(J_1 \cup \ldots \cup J_{|\mathcal{P}|-1}, J_{|\mathcal{P}|})$ constitute a decomposition of $\mathcal{E}$,

$$\max I(X_{J_1} : X_{J_2} : \ldots : X_{J_{|\mathcal{P}|}}) \leq \sum_{e\in\mathcal{E}} S_e. \tag{D15}$$

Since the measurement achieving the maximums for the terms in Eq. (D12) are compatible (act nontrivially on disjoint subsets of edges), the upper bound $\sum_{e\in\mathcal{E}} S_e$ is also achievable (on the measurements corresponding to the Schmidt decompositions of all $|\psi_e\rangle$). □

Lemma 4. *Consider arbitrary random variables X_1, …, X_p and a random variable C, which is a function of, e.g., X_1 and private local randomness of the user 1. Then*

$$I(X_1 : \ldots : X_p|C) \leq I(X_1 : \ldots : X_p). \tag{D16}$$

Proof. We have

$$I(X_1 : \ldots : X_p|C) = \sum_{\alpha=1}^{p} H(X_\alpha|C) - H(X_1 \ldots X_p|C). \tag{D17}$$

We can write

$$\begin{aligned} H(X_1|C) &= H(X_1C) - H(C) \\ &= H(X_1) + H(C|X_1) - H(C). \end{aligned} \tag{D18}$$

Analogously,

$$\begin{aligned} & H(X_1 \ldots X_p|C) \\ & \quad = H(X_1 \ldots X_p) + H(C|X_1 \ldots X_p) - H(C) \\ & \quad = H(X_1 \ldots X_p) + H(C|X_1) - H(C), \end{aligned} \tag{D19}$$

where we have used that $X_2 \ldots X_p$ do not contain additional information on C with respect to X_1, hence, $H(C|X_1 \ldots X_p) = H(C|X_1)$.

Substitution of Eqs. (D18) and (D19) as well as the inequalities $H(X_\alpha|C) \leq H(X_\alpha)$ for $\alpha = 2, \ldots, p$ into Eq. (D17) gives the statement of the lemma. □

Corollary 2. *Consider arbitrary random variables X_1, …, X_p, and C, and a random variable C', which is a function of, e.g., X_1, C, and private local randomness of the user 1. Then*

$$I(X_1 : \ldots : X_p|CC') \leq I(X_1 : \ldots : X_p|C). \tag{D20}$$

Such generalization is straightforward: We simply replace C by C' and add conditioning on C in all calculations in the proof of Lemma 4.

Lemma 4 and Corollary 2 say that the classical multipartite information cannot be increased by local calculations and public communication.

Proof of Theorem 4. Consider an apbitrary I-proper partition $\mathcal{P}$ and consider the ideal state (4). Consider the subsets $J_1, \dots, J_p \in \mathcal{P}$ as "aggregated" users (i.e., merge users from the same subset together). Then, since each J_α intersects with I, the corresponding aggregated user has its own copy of the key. Denote the corresponding random variable K_{J_α}. It is straightforward to calculate that

$$I(K_{J_1} \colon K_{J_2} \colon \dots \colon K_{J_p}) = (p-1)m. \tag{D21}$$

From the other side, from Lemmas 3, 4 and Corollary 2, we conclude that the multipartite information between measurement outcomes $X_{J_1}, \dots, X_{J_p}$ followed by any classical postprocessing with public communication, cannot exceed the right-hand side of (6), which proves the theorem. □

Appendix E: Proof of Theorem 5

Consider an arbitrary decomposition (19). So, Alice's and Bob's density ρ_{AB} can be obtained as $\mathrm{Tr}_E |\psi\rangle_{ABE}\langle\psi|$ for the following tripartite state $|\psi\rangle_{ABE}$ with Eve:

$$|\psi\rangle_{ABE} = \sum_x \sqrt{p_x}\, |\psi_x\rangle_{AB} |x\rangle_E\,, \tag{E1}$$

where $|x\rangle_E$ are orthonormal vectors in Eve's space. Suppose that Eve measures her register in the standard basis and announces the result x. Of course, the fact of announcement is advantageous for Alice and Bob. Then they know that they share a pure state $|\psi_x\rangle$ in this position. After a large number n rounds, Alice and Bob have a sequence of $|\psi_x\rangle$, where, with a high probability, the number of occurrences of each x is approximately np_x. Since the distillable key is additive for a pure states and is equal to the entanglement entropy, we arrive at the conclusion that distillable key is the entanglement entropy averaged over the ensemble $\{p_\alpha, |\psi_\alpha\rangle\}$. This is an upper bound since it corresponds to a particular Eve's attack (purification) with the announcement of Eve's outcomes to Alice and Bob, which is, of course, advantageous for them.

Minimization over decompositions (19) gives $E_{\mathrm{F}}(\rho_{AB})$ as an upper bound. The same arguments applied to n rounds give the upper bound $E_{\mathrm{F}}(\rho_{AB}^{\otimes n})/n$. Taking the limit $n \to \infty$ gives the regularized entanglement entropy as an upper bound for the distillable key in the bipartite scenario. This idea (for the bipartite case) was suggested in Ref. [40]. We give a detailed rigorous proof.

For simplicity of notations, let us first prove the known statement that the bipartite distillable key is upper bounded by the regularized entanglement of formation based on this intuition. Then we will generalize this proof for the multipartite case.

Lemma 5. *Let two parties A (Alice) and B (Bob) have a source of bipartite state ρ_{AB} acting on a Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ want to establish a secret key. Then the distillable key is upper bounded by $E_F^\infty(\rho_{AB})$.*

Proof. Consider an arbitrary decomposition

$$\rho_{AB}^{\otimes n} = \sum_{x\in\mathcal{X}} p_x\, |\psi_x\rangle\langle\psi_x| \tag{E2}$$

for some $n > 0$ and a purification

$$|\Psi_{ABE}\rangle^{\otimes n} = \sum_{x\in\mathcal{X}} \sqrt{p_x}\, |\psi_x\rangle_{(AB)^n} |x\rangle_{E^n}\,, \tag{E3}$$

where $\{|x\rangle\}$ is a set of orthonormal vectors in $\mathcal{H}_E^{\otimes n}$. Without loss of generality, assume that all p_x are positive.

For $M \geq 1$, denote $\mathbf{x} = (x_1, \dots, x_M) \in \mathcal{X}^M$ (we will also refer to $\mathbf{x}$ as sequences) and

$$p_{\mathbf{x}} = \prod_{i=1}^M p_{y_i}, \quad |\psi_{\mathbf{x}}\rangle = \bigotimes_{i=1}^M |\psi_{y_i}\rangle\,, \quad |\mathbf{x}\rangle = \bigotimes_{i=1}^M |x_i\rangle\,, \tag{E4}$$

Then

$$|\Psi\rangle_{ABE}^{\otimes nM} = \sum_{\mathbf{x}\in\mathcal{X}^m} \sqrt{p_{\mathbf{x}}}\, |\psi_{\mathbf{x}}\rangle\, |\mathbf{x}\rangle\,. \tag{E5}$$

Let us consider the distillable key (3) for the state $\rho_{AB}^{\otimes n}$, i.e., a block of n rounds we consider now as a one "aggregated" round:

$$\overline{R} = \lim_{\varepsilon\to 0} \sup_{L,M,\Lambda} \Big\{ \frac{L}{M} \,\Big|\, \frac{1}{2}\|\Lambda(\rho_{ABE}^{\otimes nM}) - \rho_{K_A K_B E^{nM} C}^{(L),\,\mathrm{ideal}}\| \leq \varepsilon \Big\}. \tag{E6}$$

We are going to prove that

$$\overline{R} \leq \overline{S}_{\mathrm{ent}} = \sum_{x\in\mathcal{X}} p_x S_{\mathrm{ent}}(|\psi_x\rangle). \tag{E7}$$

This means that, for any $\Delta > 0$, there exists $\varepsilon > 0$ such that, if $L/M > \overline{S}_{\mathrm{ent}} + \Delta$, then

$$\frac{1}{2}\|\Lambda(\rho_{ABE}^{\otimes nM}) - \rho_{K_A K_B E C}^{(L),\,\mathrm{ideal}}\| > \varepsilon_0 \tag{E8}$$

for any LOSR+PP map Λ.

Consider the channel $\mathcal{D}$ acting on Eve's subsystem which decoheres in the $\{|e_{\mathbf{x}}\rangle\}$ basis, or, in other words, performs a nonselective measurement in this basis. The map $\mathcal{D}$ commutes with Λ_M (since they act nontrivially on different subsystems) and

$$\mathcal{D}\big(\rho_{ABE}^{\otimes nM}\big) = \widetilde{\rho}_{ABE}^{\otimes nM} = \sum_{\mathbf{x}\in\mathcal{X}^M} p_{\mathbf{x}}\, |\psi_{\mathbf{x}}\rangle\langle\psi_{\mathbf{x}}| \otimes |\mathbf{x}\rangle\langle\mathbf{x}| \tag{E9}$$

Obviously, the action of $\mathcal{D}$ on the ideal state gives the ideal state $\widetilde{\rho}^{(L_M),\,\mathrm{ideal}}_{K_A K_B EC}$ corresponding to $\widetilde{\rho}^{\otimes nM}_{ABE}$, i.e., uniformly distributed key uncoupled from E^n and C, and E^n having the same marginal state as in $\rho^{\otimes nM}_{ABE}$:

$$\widetilde{\rho}^{(L_M),\,\mathrm{ideal}}_{K_A K_B EC} = \tau_{K_A K_B} \otimes \sum_{\mathbf{x}\in\mathcal{X}^M} p_{\mathbf{x}} \left|\mathbf{x}\right\rangle \left\langle\mathbf{x}\right| \otimes \rho_{C|\mathbf{x}}, \quad \text{(E10)}$$

where

$$\tau_{K_A K_B} = 2^{-m} \sum_{k\in\{0,1\}^m} \left|k,k\right\rangle \left\langle k,k\right|. \quad \text{(E11)}$$

The action of a CPTP map cannot increase the trace distance, hence, it suffices to prove the property with Ineq. (E8) for $\widetilde{\rho}_{ABE}$ rather than ρ_{ABE} and the corresponding ideal state.

Due to the block-diagonal structure of $\widetilde{\rho}^{\otimes nM}_{ABE}$ and $\widetilde{\rho}^{(L_M),\,\mathrm{ideal}}_{K_A K_B EC}$ with respect to the vectors $|\mathbf{x}\rangle$, it turns out that

$$\begin{aligned}&\|\Lambda(\widetilde{\rho}^{\otimes nM}_{ABE}) - \widetilde{\rho}^{(L),\,\mathrm{ideal}}_{K_A K_B EC}\| \\ &= \sum_{\mathbf{x}\in\mathcal{X}^M} p_{\mathbf{x}} \big\|\Lambda(\left|\psi_{\mathbf{x}}\right\rangle \left\langle\psi_{\mathbf{x}}\right|^{\otimes M}) - \tau_{K_A K_B} \otimes \rho_{C|\mathbf{x}}\big\|. \quad \text{(E12)}\end{aligned}$$

It turns out (see below) that it suffices to prove that, for all $\Delta > 0$, there exists $\varepsilon_1 > 0$ and $\overline{M} > 0$ such that, if $L/M > \overline{S}_{\mathrm{ent}} + \Delta$ and $M \geq \overline{M}$, then

$$\frac{1}{2}\big\|\Lambda(\left|\psi_{\mathbf{x}}\right\rangle \left\langle\psi_{\mathbf{x}}\right|^{\otimes M}) - \tau_{K_A K_B} \otimes \rho_{C|\mathbf{x}}\big\| \geq \varepsilon_1 \quad \text{(E13)}$$

for any LOSR+PP map Λ and for any sequence $\mathbf{x}$ from a high-probability (typical) subset.

Let us use the following definition of a typical sequence [49]: A sequence $\mathbf{y}$ is said to be typical (denoted as $\mathbf{x} \in T_M$) if

$$\left|\frac{M_x^{(\mathbf{x})}}{M} - p_x\right| \leq \delta_M \quad \text{(E14)}$$

for all $x \in \mathcal{X}$, where $M_x^{(\mathbf{x})}$ is the number of occurrences of the symbol x in the sequence $\mathbf{x}$. As in Ref. [49], we will assume that $\delta_M \to 0$ and $\sqrt{M}\delta_M \to \infty$ as $M \to \infty$. Then, the total probability of typical sequences is at least $1-\gamma_M$, where $\gamma_M \to 0$ as $M \to \infty$. Also we assume that δ_M is non-increasing with M.

If the property with Ineq. (E13) is true for all typical sequences and $M \geq \overline{M}$, then Ineq. (E8) is also true with

$$\varepsilon_0 = (1-\gamma_{\overline{M}})\varepsilon_1 \quad \text{(E15)}$$

for $M \geq \overline{M}$. Then, for $M < \overline{M}$, the left-hand side of Ineq. (E8) cannot be zero or even be made arbitrarily close to zero because it would lead to the left-hand side equal or arbitrarily close to zero for arbitrary large M by concatenations of the shorter keys. Then, taking the minimum between $(1-\gamma_{\overline{M}})\varepsilon_1$ and the infimum of left-hand side of Ineq. (E8) for $M < \overline{M}$ gives ε_0 for which Ineq. (E8) is satisfied for all M.

In order to prove Ineq. (E13) for typical sequences, we need to gather the data of some length M_0 such that $\lceil M_0(p_x+\delta_{M_0})\rceil/M_0 \approx p_x$. For this purpose, consider the following family of pure states depending on M_0:

$$\left|\psi_T\right\rangle = \bigotimes_{x\in\mathcal{X}} \left|\psi_x\right\rangle^{\otimes\lceil M_0(p_x+\delta_{M_0})\rceil} \quad \text{(E16)}$$

(here T is for "typical"). This is a pure state, so its distillable key is equal to

$$\begin{aligned}S_{\mathrm{ent}}(\left|\psi_T\right\rangle) &= \sum_{x\in\mathcal{X}} \lceil M_0(p_x+\delta_{M_0})\rceil S_{\mathrm{ent}}(\left|\psi_x\right\rangle) \\ &= M_0(\overline{S}_{\mathrm{ent}} + \eta_{M_0}),\end{aligned} \quad \text{(E17)}$$

where $\eta_{M_0} \to 0$ as $M_0 \to \infty$. We assume that M_0 is fixed and large enough to ensure $\eta_{M_0} < \Delta$. That is, there exists $\varepsilon_1 > 0$ such that, if $L'/M' > M_0(\overline{S}_{\mathrm{ent}} + \Delta)$, then

$$\frac{1}{2}\|\Lambda'(\left|\psi_T\right\rangle \left\langle\psi_T\right|^{\otimes M'}) - \rho^{(L'),\,\mathrm{ideal}}_{K_A K_B C}\| > \varepsilon_1 \quad \text{(E18)}$$

for any LOSR+PP map Λ'.

Consider $M > M_0$ and define $M' = \lceil M/M_0\rceil$. For a typical sequence $\mathbf{y}$ of length M, we have

$$M_y^{(\mathbf{y})} \leq M(p_y+\delta_M) \leq M'\lceil M_0(p_y+\delta_{M_0})\rceil, \quad \text{(E19)}$$

so, the states $|\psi_{\mathbf{x}}\rangle$ for typical $\mathbf{x}$ can be obtained from $|\psi_T\rangle^{\otimes M'}$ by permutation and elimination of some subsystems by both parties simultaneously.

We are ready to prove Ineq. (E13) with the same $\varepsilon_1 = \varepsilon_1(\Delta)$ as from Ineq. (E18) for large enough M. Suppose that Ineq. (E13) is not satisfied for some L, M, $\mathbf{x} \in T_M$, and Λ and $L/M > \overline{S}_{\mathrm{ent}} + \Delta$. Then consider a quantum channel $\Lambda' = \Lambda \circ \Phi_{\mathbf{x}}$ acting on $|\psi_T\rangle^{\otimes M'}$, where $\Phi_{\mathbf{x}}$ are local permutations and eliminations of subsystems (depending on $\mathbf{x}$ but not requiring even classical communication). For such choice of the channel Λ', in the notations of Ineq. (E18), $L' = L$ and the left-hand sides of Ineqs. (E13) and (E18) coincide. Hence, the left-hand side of Ineq. (E18) is not bigger than ε_1. From the other side, from our assumption of violation of Ineq. (E13), we have

$$\frac{L'}{M/M_0} > M_0(\overline{S}_{\mathrm{ent}} + \Delta). \quad \text{(E20)}$$

We have not yet obtained a contradiction with Ineq. (E18) because a condition for it is $L'/M' > M_0(\overline{S}_{\mathrm{ent}} + \Delta)$, but $M' \geq M/M_0$. However,

$$\frac{L'}{M'} = \frac{L'}{M/M_0} - L'\frac{M'M_0 - M}{MM'}. \quad \text{(E21)}$$

By construction, $M \geq M_0(M'-1)$, so, the last term in Eq. (E21) is upper bounded by $(L'/M')(M_0/M)$ and, thus, is infinitesimal as $M \to \infty$. Then,

$$\frac{L'_{M'}}{M'} > M_0(\overline{S}_{\text{ent}} + \Delta) \tag{E22}$$

for large enough M. Thus, Ineq. (E18) is violated for large enough M. Hence, Ineq. (E13) also cannot be violated for large enough M. This finishes the proof of Ineq. (E7).

Minimization over decomposition (19) gives $\overline{R} < E_{\text{F}}(\rho_{AB}^{\otimes n})$. If we remember that we consider a block of n rounds and return to the original definition of the distillable key (3), we obtain

$$\overline{r}_{\text{key}} \leq \frac{1}{n} E_{\text{F}}(\rho_{AB}^{\otimes n}). \tag{E23}$$

Taking the limit $n \to \infty$ gives that the bipartite distillable key cannot be larger than the regularized entropy of formation, or entanglement cost. □

Proof of Theorem 5. A generalization to the multipartite case is straightforward. For simplicity, consider first the case $I = [N]$ (i.e., a conference key is required for all parties) and the finest partition, i.e., each subset in the partition $\mathcal{P}$ consists from a single element. We are going to prove that

$$\overline{r}_{\text{key}}(\vec{A}) \leq \frac{1}{N-1} \sum_{e \in \mathcal{E}} E_{\text{F}}^{\infty}(\rho_e). \tag{E24}$$

The proof actually repeats the above prove for the bipartite case. Consider arbitrary decompositions

$$\rho_e^{\otimes n} = \sum_{x^{(e)} \in \S^{(e)}} p_{x^{(e)}} \left|\psi_{x^{(e)}}\right\rangle \left\langle\psi_{x^{(e)}}\right| \tag{E25}$$

for every edge and some $n > 0$ and a purification

$$\left|\Psi^{(e)}\right\rangle = \sum_{x^{(e)} \in \mathcal{X}^{(e)}} \sqrt{p_{x^{(e)}}} \left|\psi_{x^{(e)}}\right\rangle \otimes \left|x^{(e)}\right\rangle. \tag{E26}$$

Here $\left|x^{(e)}\right\rangle$ are bipartite unit vectors for the corresponding edges and $\left|x^{(e)}\right\rangle$ are orthogonal vectors in Eve's space. Denote

$$\vec{x} = (x^{(e)})_{e \in \mathcal{E}} \in \prod_{e \in \mathcal{E}} \mathcal{X}^{(e)} = \mathcal{X}, \tag{E27}$$

$$p_{\vec{x}} = \prod_{e \in \mathcal{E}} p_{x^{(e)}}, \quad \left|\psi_{\vec{x}}\right\rangle = \bigotimes_{e \in \mathcal{E}} \left|\psi_{x^{(e)}}\right\rangle, \quad \left|\vec{x}\right\rangle = \bigotimes_{e \in \mathcal{E}} \left|x^{(e)}\right\rangle. \tag{E28}$$

Now for $M \geq 1$, we again introduce notations $\mathbf{x} = (\vec{x}_1, \ldots, \vec{x}_M) \in \mathcal{X}^M$, and

$$p_{\mathbf{x}} = \prod_{i=1}^{M} p_{\vec{x}_i}, \quad \left|\psi_{\mathbf{x}}\right\rangle = \bigotimes_{i=1}^{M} \left|\psi_{\vec{x}_i}\right\rangle, \quad \left|\mathbf{x}\right\rangle = \bigotimes_{i=1}^{M} \left|\vec{x}_i\right\rangle. \tag{E29}$$

That is, like in the proof for the bipartite case, we again consider sequences $\mathbf{x}$, but now we simply consider $\vec{x}$ as their "letters". In this notation, Eq. (E5) is again true and we can repeat all the reasonings. The only difference is as follows. Instead of Ineq. (E7), we prove

$$\begin{aligned} \overline{R} &\leq \sum_{\vec{x} \in \mathcal{X}} \frac{p_{\vec{x}}}{N-1} \sum_{e \in \mathcal{E}} S_{\text{ent}}(\left|\psi_{x^{(e)}}\right\rangle). \\ &= \frac{1}{N-1} \sum_{e \in \mathcal{E}} \sum_{x^{(e)} \in \mathcal{X}^{(e)}} p_{x^{(e)}} S_{\text{ent}}(\left|\psi_{x^{(e)}}\right\rangle) \\ &= \frac{1}{N-1} \sum_{e \in \mathcal{E}} \overline{S}_e, \end{aligned} \tag{E30}$$

where we have introduced the notation $\overline{S}_e$ for the sum over $x^{(e)}$. Correspondingly, we need to modify Eq. (E17). We define now the state $\left|\psi_T\right\rangle$ analogously:

$$\left|\psi_T\right\rangle = \bigotimes_{\vec{x} \in \mathcal{X}} \left|\psi_{\vec{x}}\right\rangle^{\otimes \lceil M_0(p_{\vec{x}} + \delta_{M_0}) \rceil}. \tag{E31}$$

According to Theorem 4, its distillable conference key is upper bounded (actually, is equal, as we know from the main text) by

$$\sum_{\vec{x} \in \mathcal{X}} \frac{\lceil M_0(p_{\vec{x}} + \delta_{M_0}) \rceil}{N-1} \sum_{e \in \mathcal{E}} S_{\text{ent}}(\left|\psi_{x^{(e)}}\right\rangle). \tag{E32}$$

That is, we have replaced $S_{\text{ent}}(\left|\psi_x\right\rangle)$ with $\frac{1}{N-1} \sum_e S_{\text{ent}}(\left|\psi_{x^{(e)}}\right\rangle)$. All other reasonings are repeated without modification (up to replacement of x and $\overline{S}_{\text{ent}}$ with $\frac{1}{N-1} \sum_e \overline{S}_e$). This finished the proof for the case $I = [N]$ and the finest partition $\mathcal{P}$:

$$\overline{r}_{\text{key}}(\vec{A}) \leq \frac{1}{N-1} \sum_{e \in \mathcal{E}} E_{\text{F}}^{\infty}(\rho_e). \tag{E33}$$

The general case of an arbitrary $I \subset [N]$ and an I-proper partition $\mathcal{P}$ is reduced to it. We can consider the graph contraction corresponding to the partition $\mathcal{P}$, i.e., the graph where the elements of $\mathcal{P}$ are vertices and the quantum state corresponding to the edge (J, J') for $J, J' \in \mathcal{P}$ is

$$\rho_{(J,J')} = \bigotimes_{e \in \mathcal{E}(J,J')} \rho_e. \tag{E34}$$

Here $\mathcal{E}(J, J') \subset \mathcal{E}$ is the subset of edges of the original graph where one endvertex belongs to J and the other one belongs to J'. Let us relax the restriction of the allowed class of operations to the $\mathcal{P}$-local ones (and, as before, with shared randomness and classical postprocessing), i.e., nonlocal operations inside the partition subsets are allowed. Then the problem of conference key distillation for this problem is obviously weaker then the problem of conference key distillation for the subset I using the usual LOSR+PP. Thus, application of Ineq. (E33) to this setting [i.e., replacement of N with $|I|$ and the summation is over $\mathcal{E}(\mathcal{P})$] gives Ineq. (17). □

[1] H. Kimble, The quantum internet, Nature **453**, 1023 (2008).

[2] S. Pirandola and S. Braunstein, Physics: Unite to build a quantum internet, Nature **532**, 169 (2016).

[3] C. Simon, Towards a global quantum network, Nature Photon. **11**, 678 (2017).

[4] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Nature Photon. **11**, eaam9288 (2018).

[5] P. P. Rohde, *The Quantum Internet. The second Quantum Revolution* (Cambridge University Press, Cambridge, 2021).

[6] P. P. Rohde, Z. Huang, Y. Ouyang, H.-L. Huang, Z.-E. Su, S. Devitt, R. Ramakrishnan, A. Mantri, S.-H. Tan, N. Liu, S. Harrison, C. Radhakrishnan, G. K. Brennen, B. Q. Baragiola, J. P. Dowling, T. Byrnes, and W. J. Munro, The quantum internet (technical version) (2025), arXiv:2501.12107 [quant-ph].

[7] N. H. Valencia, A. Ma, S. Goel, S. Leedumrongwatthanakun, F. Graffitti, A. Fedrizzi, W. McCutcheon, and M. Malik, A large-scale reconfigurable multiplexed quantum photonic network (2025), arXiv:2501.07272 [quant-ph].

[8] V. Kumar, C. Cicconetti, M. Conti, and A. Passarella, Quantum internet: Technologies, protocols, and research challenges (2025), arXiv:2502.01653 [quant-ph].

[9] R. Shi and H. Zhong, Multi-party quantum key agreement with bell states and bell measurements, Quantum Information Processing **12**, 921 (2013).

[10] C. Shukla, N. Alam, and A. Pathak, Protocols of quantum key agreement solely using bell states and bell measurement, Quantum Information Processing **13**, 2391 (2014).

[11] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, New. J. Phys. **19**, 093012 (2017).

[12] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Advanced Quantum Technologies **3**, 2000025 (2020).

[13] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa, Secure anonymous conferencing in quantum networks, arXiv preprint (2021), 2111.05363.

[14] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, Conference key agreement in a quantum network, npj Quantum Information **9**, 82 (2023).

[15] P. Contreras-Tejada, C. Palazuelos, and J. de Vicente, Asymptotic survival of genuine multipartite entanglement in noisy quantum networks depends on the topology, Phys. Rev. Lett. **128**, 220501 (2022).

[16] I. Devetak and A. Winter, General upper bound for conferencing keys in arbitrary quantum networks, Proc. R. Soc. A **207–235**, 041016 (2005).

[17] M. Christandl, The structure of bipartite quantum states - insights from group theory and cryptography (2006), arXiv:quant-ph/0604183 [quant-ph].

[18] R. Augusiak and P. Horodecki, Multipartite secret key distillation and bound entanglement, Phys. Rev. A **80**, 042307 (2009).

[19] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network, Physical Review X **11**, 041016 (2021).

[20] F. Buscemi, All entangled quantum states are nonlocal, Phys. Rev. Lett. **108**, 200401 (2012).

[21] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens, Genuine network multipartite entanglement, Phys. Rev. Lett. **125**, 240505 (2020).

[22] T. Kraft, S. Designolle, C. Ritz, N. Brunner, O. Gühne, and M. Huber, Quantum entanglement in the triangle network, Phys. Rev. A **103**, L060401 (2021).

[23] K. Hansenne, Z.-P. Xu, T. Kraft, and O. Gühne, Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques, Nature Comm. **13**, 496 (2022).

[24] J. Neumann, T. V. Kondra, K. Hansenne, L. T. Weinbrenner, H. Kampermann, O. Gühne, D. Bruß, and N. Wyderka, No quantum advantage without classical communication: Fundamental limitations of quantum networks, arXiv preprint (2025), 2503.09473.

[25] G. Carrara, H. Kampermann, D. Bruß, and G. Murta, Genuine multipartite entanglement is not a precondition for secure conference key agreement, Phys. Rev. Res. **3**, 013264 (2021).

[26] L. Wooltorton, P. Brown, and R. Colbeck, Genuine multipartite entanglement is not necessary for standard device-independent conference key agreement, Phys. Rev. Lett. **135**, 220803 (2025).

[27] S. Pirandola, General upper bound for conferencing keys in arbitrary quantum networks, IET Quantum Commun. **1**, 22 (2020).

[28] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, Secret key generation for a pairwise independent network model, IEEE Trans. Inf. Theory **56**, 6482 (2010).

[29] S. Nitinawarat and P. Narayan, Perfect omniscience, perfect secrecy, and steiner tree packing, IEEE Trans. Inf. Theor. **56**, 6490–6500 (2010).

[30] A. Trushechkin, H. Kampermann, and D. Bruß, Spanning-tree-packing protocol for conference key propagation in quantum networks (2025).

[31] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proceedings of the Royal Society A **461**, 207 (2005).

[32] R. Augusiak and P. Horodecki, Multipartite secret key distillation and bound entanglement, Physical Review A—Atomic, Molecular, and Optical Physics **80**, 042307 (2009).

[33] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, New Journal of Physics **20**, 113014 (2018).

[34] I. Csiszár and P. Narayan, Secrecy capacities for multiple terminals, IEEE Trans. Inf. Theory **50**, 3047 (2004).

[35] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens, Genuine network multipartite entanglement, Physical Review Letters **125**, 240505 (2020).

[36] R. Diestel, *Graph Theory*, 5th ed. (Springer, Berlin, 2017).

[37] S. Khatri and M. M. Wilde, Principles of quantum communication theory: A modern approach (2024), arXiv:2011.04672 [quant-ph].

[38] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof, IEEE Trans. Inf. Theory **55**, 3375 (2009).

[39] K. P. Seshadreesan, M. Takeoka, and M. M. Wilde, Bounds on entanglement distillation and secret key agreement for quantum broadcast channels, IEEE Trans. Inf. Theory **62**, 2849 (2016).

[40] M. Koashi and A. Winter, Monogamy of quantum entanglement and other correlations, Phys. Rev. A **69**, 022309 (2004).

[41] R. Chaves, C. Majenz, and D. Gross, Information–theoretic implications of quantum causal structures, Nature communications **6**, 5766 (2015).

[42] E. Wolfe, R. W. Spekkens, and T. Fritz, The inflation technique for causal inference with latent variables, Journal of Causal Inference **7**, 20170020 (2019), article ID 20170020.

[43] E. Wolfe, A. Pozas-Kerstjens, M. Grinberg, D. Rosset, A. Acín, and M. Navascués, Quantum inflation: A general approach to quantum causal compatibility, Phys. Rev. X **11**, 021043 (2021).

[44] G. Tóth and O. Gühne, Entanglement detection in the stabilizer formalism, Phys. Rev. A **72**, 022340 (2005).

[45] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619 (1998).

[46] K. M. R. Audenaert and J. Eisert, Continuity bounds on the quantum relative entropy – II, J. Math. Phys. **52**, 112201 (2011).

[47] M. J. Donald and M. Horodecki, Continuity of relative entropy of entanglement, Phys. Lett. A **264**, 257 (1999).

[48] A. Holevo, *Quantum Systems, Channels, Information. A Mathematical Introduction* (De Gruyter, Berlin, Boston, 2013).

[49] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. (Cambridge University Press, Cambridge, 2011).

Paper C

Fundamental limitations on entanglement extraction from purity

The following text is reproduced from the preprint

Tulja Varun Kondra, Pedro Barrios Hita, Justus Neumann, Hermann Kampermann, and Dagmar Bruß

Fundamental limitations on entanglement extraction from purity arXiv preprint, 2026. arXiv:2605.29197 [quant-ph].

Statement of contribution

My contribution to this work consisted of showing that there is no nontrivial subset of the set of absolutely separable states that is closed under tensor products. In particular, this implies that the set of completely absolutely separable states is not closed under tensor products. I also contributed to the analysis of completely absolutely separable states and helped characterize boundary points of this set. The main theorem was derived by Pedro Barrios Hita and Tulja Varun Kondra. The results, their interpretation, and their relation to entanglement extraction from purity were discussed jointly. Hermann Kampermann and Dagmar Bruß contributed to discussions and provided feedback on the presentation of the work. The manuscript was finalized with input from all authors. The project was supervised by Hermann Kampermann and Dagmar Bruß.

arXiv:2605.29197v1 [quant-ph] 28 May 2026

Fundamental limitations on entanglement extraction from purity

Tulja Varun Kondra[‡,1,*] Pedro Barrios Hita[‡,2,1,†] Justus Neumann,[1] Hermann Kampermann,[1] and Dagmar Bruß[1]

[1]*Heinrich Heine University Düsseldorf, Faculty of Mathematics and Natural Sciences, Institute for Theoretical Physics III*
[2]*Institute of Software Technology, German Aerospace Center (DLR), Sankt Augustin, Germany*

States of sufficiently low purity are separable and cannot be entangled by unital (purity-non-generating) operations. Since high-purity states are experimentally demanding, it is natural to ask how much purity a state must possess to enable entanglement generation. Absolutely separable states remain separable under all deterministic unital channels, and so cannot deterministically generate entanglement in this setting. We show, however, that some absolutely separable states can generate entanglement via probabilistic protocols that do not produce purity. This motivates the study of states that fail to generate entanglement with *any* non-zero probability, which we call *completely absolutely separable*; we give a full characterization of this class. Along the way, we derive a novel sufficient condition for separability that depends only on the largest and smallest eigenvalues, along with the smallest local dimension and is independent of all previously known spectral separability criteria.

Quantum entanglement is a fundamental resource in quantum information science, playing a key role in tasks such as quantum cryptography [1], quantum teleportation [2] and quantum metrology [3]. The investigation of entanglement and its properties has not only deepened our understanding of quantum mechanics, but has also shown how quantum effects can be controlled and exploited for practical applications [4]. In a broader context, quantum resource theories provide a unified mathematical framework for studying a range of other quantum resources, such as coherence [5], athermality [6], and magic [7]. Purity is one such resource, quantifying the deviation of a quantum state from the maximally mixed state [8]. In many experimental platforms, the preparation of high-purity states is itself a demanding task, as unavoidable noise, decoherence, and imperfect control tend to introduce mixing [9–11]. As a result, the ability to generate and maintain high-purity states is often a significant practical limitation, making it important to understand what can be achieved under restricted purity.

Therefore, a natural question is: *how much purity is required to enable entanglement generation?* To address this question, we consider the most general physical processes that do not generate purity, namely unital channels [8, 12, 13]. This setting captures the fundamental interplay between purity and entanglement. It is known that states sufficiently close to the maximally mixed state cannot be transformed into entangled states by any unital channel [14, 15]. This naturally leads to the problem of characterizing those states that are fundamentally incapable of producing entanglement under purity-non-generating dynamics. This set coincides with the class of so-called *absolutely separable* (AS) states [16, 17], originally introduced as states that remain separable under all global unitary operations. A complete characterization of such states is known when one of the local dimensions is equal to two [18]. For higher local dimensions, however, the problem remains open and is known as the longstanding *separability from spectrum* problem [19].

Even though a complete characterization is not known, the positive-partial-transpose (PPT) criterion for separability [20, 21] can be used to provide necessary conditions in arbitrary local dimensions. These conditions are expressed as linear matrix inequalities and are tight for small local dimensions (in particular, when one of the local dimensions is two). However, for higher local dimensions it remains an open conjecture whether the PPT criterion can detect all absolutely separable states [22]. Other variants of necessary conditions can be obtained, for instance, from the reduction criterion [23] and from bounds based on conditional entropy [24]. On the other hand, various sufficient conditions have also been proposed, which approximate the set of absolutely separable states from below [14, 15, 25, 26].

In recent years, there has been growing interest in probabilistic protocols [27, 28]. Unlike deterministic transformations, probabilistic protocols allow for a nonzero probability of failure and only require the desired transformation to occur conditionally upon success. This additional flexibility can enlarge the set of achievable state transformations and, in particular, allows one to overcome limitations that are unavoidable in the deterministic setting [29, 30]. These developments indicate that any fundamental constraint on converting purity into entanglement must account for such general probabilistic transformations, rather than only trace-preserving ones. In particular, a purely deterministic notion of absolute separability may fail to capture the strongest possible limitation to entanglement generation from purity.

In this letter, we allow for the most general probabilistic processes that do not generate purity, even when conditioned on any individual outcome; we refer to such processes as *probabilistic unital channels*. We first show that certain absolutely separable states can generate entanglement with nonzero probability under suitable probabilistic unital channels. This demonstrates that absolute separability does not capture the ultimate purity based limitation on entanglement generation. Motivated by this observation, we introduce a stricter notion, which we call *completely absolutely separable* (CAS) states, defined as bipartite

‡ These authors contributed equally to this work.

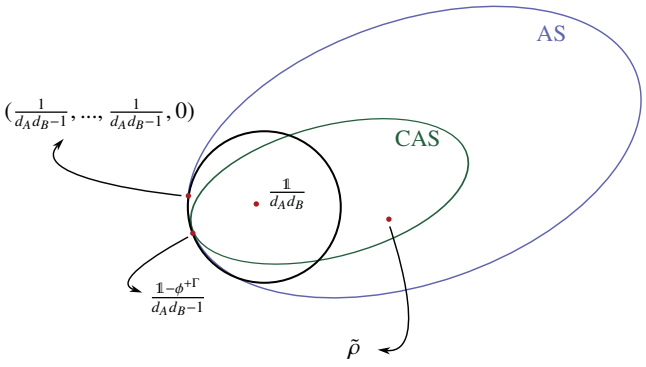


FIG. 1. Graphical representation of the absolutely separable set (AS), completely absolutely separable set (CAS) and the separable ball introduced in [14] (black circle) for unequal local dimensions d_A and d_B. The state $(\frac{1}{d_Ad_B-1},\ldots,\frac{1}{d_Ad_B-1},0)$ is on the boundary of both the purity ball and the AS set [31]. The state $\frac{\mathbb{1}-|\Phi^+\rangle\langle\Phi^+|^\Gamma}{(d_Ad_B)-1}$ (Γ is the partial transpose of B) is on the boundary of every set. The state $\tilde{\rho}$ lies outside the purity ball. Moreover, it remains undetected by every known criterion for absolute separability in the literature. However, it lies within CAS and thus AS (see Sec. G of the Supplemental Material).

states that cannot generate entanglement with any nonzero probability under any probabilistic unital channel. We show that the set of CAS states admits a remarkably simple characterization in terms of necessary and sufficient spectral conditions, valid for arbitrary local dimensions. Furthermore, we establish an interesting connection between this newly introduced notion of CAS and the conventional definition of absolute separability. In particular, we show that CAS states are precisely those states that remain absolutely separable even after attaching (via tensor product) a maximally mixed ancillary system of arbitrary dimension, to one of the subsystems.

Our analysis yields a new sufficient condition for separability, expressed solely in terms of the largest and smallest eigenvalues of the state and the smallest local dimension. This condition is independent of all previously known sufficient criteria for absolute separability [14, 15, 25, 26]. To the best of our knowledge, all earlier sufficient conditions depend on the global dimension rather than the smallest local dimension. As a consequence, our criterion certifies absolute separability for states beyond the reach of all previously known sufficient criteria (see Fig. 1). Indeed, we explicitly construct (see Sec. G of the Supplemental Material), for every bipartite system with unequal local dimensions, an absolutely separable state $\tilde{\rho}$ that escapes detection by all existing sufficient conditions but is certified by ours.

Entanglement extraction from purity.— A bipartite state ρ^{AB} is called absolutely separable if

$$U_{AB}\rho^{AB}U_{AB}^\dagger \in \mathcal{S} \tag{1}$$

for every global unitary U_{AB}, where $\mathcal{S}$ denotes the set of separable states. Absolute separability has been extensively studied; see, for example, Refs. [17–19, 22, 32, 33]. Considerable effort has been devoted to characterizing this set.

An equivalent formulation is that absolutely separable states are precisely those bipartite states that remain separable under all unital dynamics. More explicitly, ρ^{AB} is absolutely separable if and only if

$$\Lambda[\rho^{AB}] \in \mathcal{S} \tag{2}$$

for every completely positive trace-preserving (CPTP) map Λ satisfying $\Lambda(\mathbb{1}) = \mathbb{1}$.

To see the equivalence between these two definitions of absolute separability, first note that every unitary channel is unital, so invariance under all unital channels immediately implies invariance under all global unitaries. Conversely, if ρ^{AB} is absolutely separable and Λ is any unital channel, then $\Lambda[\rho^{AB}]$ is majorized by ρ^{AB}. This implies that there exist probabilities $\{p_i\}$ and unitaries $\{U_i\}$ such that [8, 34]

$$\Lambda[\rho^{AB}] = \sum_i p_i\, U_i\rho^{AB}U_i^\dagger. \tag{3}$$

Since each state $U_i\rho^{AB}U_i^\dagger$ is separable by absolute separability, and since the set $\mathcal{S}$ is convex, it follows that $\Lambda[\rho^{AB}]$ is also separable. Hence the two formulations are equivalent. Therefore, absolutely separable states are precisely those states from which entanglement cannot be generated by any deterministic physical process that preserves the maximally mixed state.

Now consider the absolutely separable two-qubit state

$$\rho = \frac{1}{3}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|). \tag{4}$$

In Sec. C of the Supplemental Material, we show that there exists a stochastic quantum operation $\tilde{\Lambda}$ such that

$$\tilde{\Lambda}[\mathbb{1}] = \frac{5}{12}\mathbb{1} \quad \text{and} \quad \tilde{\Lambda}[\rho] = \frac{2}{9}\rho_W, \tag{5}$$

where ρ_W is an entangled Werner state. Here, $\tilde{\Lambda}$ is a completely positive, trace-non-increasing map and therefore corresponds to a valid quantum operation associated with a particular measurement outcome. In this sense, it describes a stochastic process. Moreover, $\tilde{\Lambda}$ is purity non-generating (unital), in the sense that it does not create purity, even conditionally on the successful outcome. Nevertheless, it probabilistically generates entanglement from the absolutely separable state ρ (see Eq. (5)). Note that, any probabilistic unital channel can be completed to a deterministic unital channel by assigning the failure outcome to the preparation of the maximally mixed state. Consequently, every probabilistic unital channel can be embedded in a deterministic unital channel.

This example shows that some absolutely separable states can still be used to generate entanglement with nonzero probability. This naturally motivates the question of characterizing all bipartite states from which entanglement

cannot be generated with any nonzero probability. Such states represent the most fundamental limitation on entanglement generation from purity-non-generating processes.

We define a bipartite state ρ^{AB} to be *completely absolutely separable* if

$$\frac{\tilde{\Lambda}[\rho^{AB}]}{\mathrm{Tr}\left[\tilde{\Lambda}[\rho^{AB}]\right]} \in \mathcal{S} \tag{6}$$

for every probabilistic unital channel $\tilde{\Lambda}$, i.e. if no physical process can generate entanglement from it. We now state our main result.

Theorem 1. *A bipartite state ρ^{AB} is completely absolutely separable if and only if*

$$R(\rho^{AB}) \leq \frac{d+1}{d-1}. \tag{7}$$

Here $R(\rho^{AB}) := \frac{\lambda_{\max}}{\lambda_{\min}}$ is the ratio of the largest and smallest eigenvalues of ρ^{AB}, and $d := \min\{d_A, d_B\}$ is the smaller local dimension.

This result provides a complete and remarkably simple spectral characterization of completely absolutely separable states. In contrast, a complete characterization of absolutely separable states remains open. Note that, completely absolutely separable states must be full-rank (see Supplemental Material, Sec. D), so the quantity $R(\rho^{AB})$ is always well defined.

The proof proceeds in three steps: First, we show that every state satisfying $R(\rho^{AB}) \leq \frac{d+1}{d-1}$ is separable. Second, we show that the bound is tight; see Supplemental Material, Sec. E. Third, we use the fact that R is a complete monotone under probabilistic unital operations (Supplemental Material, Sec. D), meaning that ρ can be transformed into σ with nonzero probability if and only if $R(\rho) \geq R(\sigma)$ [27, 28]. These three ingredients together establish the theorem.

A novel sufficient condition for separability.— A key ingredient in the proof of Theorem 3 is the following sufficient condition for separability: a bipartite state ρ^{AB} is separable whenever Eq. (24) is satisfied. The proof of this statement can be found in Sec. B of the Supplemental Material and it relies on an important structural property of bipartite entanglement witnesses. Recall that an *entanglement witness* is a Hermitian operator W such that $\mathrm{Tr}\left[\rho^{AB}W\right] \geq 0$ for all separable states ρ^{AB}. This property is also known as block-positivity. At the same time, there exists at least one entangled state ρ^{AB}_{ent} such that $\mathrm{Tr}\left[\rho^{AB}_{\mathrm{ent}}W\right] < 0$, in which case W is said to *detect* ρ^{AB}_{ent}. Several spectral properties of entanglement witnesses are known [35–37]. In Sec. A of the Supplemental Material, we show that any bipartite witness with trace 1, satisfies the following condition

$$\|W\|_1 \leq d := \min\{d_A, d_B\}, \tag{8}$$

where $\|\cdot\|_1$ denotes the trace norm. This resolves an open question posed in [35]. The criterion in Eq. (24) depends only on the eigenvalue ratio R and the smaller local dimension. Since it is based solely on the spectrum of the state, it constitutes a spectral sufficient condition for separability. This is especially appealing from a practical standpoint, as spectral information is often more accessible than full state tomography [38–40]. To the best of our knowledge, all previously known spectral separability criteria depend on the global dimension and become trivial in the limit of large global dimension [14, 15, 25, 26]. In contrast, our new criterion depends only on the smaller local dimension of the bipartite system. This has important implications for certifying separability from spectral data: in particular, for systems with unequal local dimensions, it detects separable states beyond the reach of previously known spectral criteria.

To illustrate this, consider the largest separable ball criterion of Ref. [14], which guarantees that a state is separable whenever its purity satisfies

$$\mathrm{Tr}\left(\rho^2\right) \leq \frac{1}{d_A d_B - 1}. \tag{9}$$

Now, if one increases one local dimension while keeping the other fixed, the corresponding separable ball shrinks and in the limit where one subsystem dimension becomes arbitrarily large, it collapses to the maximally mixed state. This behavior stands in sharp contrast to our criterion, which remains invariant under an enlargement of one local dimension because it depends only on the smaller local dimension.

Indeed, in Sec. G of the Supplemental Material, we construct, for every pair of unequal local dimensions, an explicit absolutely separable state that is not detected either by the purity-ball criterion or by the criterion of Ref. [25], but is detected by our condition in Eq. (24). By contrast, when the local dimensions are equal, the set of completely absolutely separable states is contained within the purity ball. A proof of this fact is given in Sec. H of the Supplemental Material.

Note that, since unitary transformations preserve purity, every state satisfying Eq. (9) is absolutely separable. The converse is false: there exist absolutely separable states that violate Eq. (9) (see [14]). We show in Sec. I of the Supplemental Material that any absolutely separable state must satisfy

$$\mathrm{Tr}\left(\rho^2\right) \leq \frac{2}{d_A d_B}. \tag{10}$$

This yields an analytical upper bound on the maximal purity of absolutely separable states and improves upon the previously known analytical bounds of Ref. [41].

Application to multipartite states.— Let $\rho^{A_1,\ldots,A_N}$ be an N-partite state on subsystems $A_1, \ldots, A_N$. Suppose that, for some $l \in \mathbb{N}$,

$$R(\rho^{A_1,\ldots,A_N}) := \frac{\lambda_{\max}}{\lambda_{\min}} \leq \frac{l+1}{l-1}, \tag{11}$$

where $\lambda_{\max}$ and $\lambda_{\min}$ denote the largest and smallest eigenvalues of $\rho^{A_1,\ldots,A_N}$, respectively. Then $\rho^{A_1,\ldots,A_N}$ is

separable across every bipartition

$$A_1, \ldots, A_x \,|\, A_{x+1}, \ldots, A_N$$

for which at least one side has Hilbert-space dimension at most l. As a simple application, consider the Gibbs state

$$\rho_T = \frac{e^{-H/(k_B T)}}{\mathrm{Tr}(e^{-H/(k_B T)})}$$

of a multipartite Hamiltonian H with eigenvalues $\{E_i\}_i$. In this setting, one may ask for temperatures above which entanglement cannot persist. By Eq. (11), the Gibbs state is separable across any bipartition whose smaller subsystem has dimension at most (l), provided that

$$T \geq \frac{2\|H\|_\infty}{k_B \ln\left(\frac{l+1}{l-1}\right)}. \tag{12}$$

Here, $\|H\|_\infty := \max |E_i|$ denotes the Schatten ∞-norm of H. We used the bound $E_{\max} - E_{\min} \leq 2\|H\|_\infty$.

Relation between absolute separability and complete absolute separability.— Recall that a bipartite state ρ^{AB} is called *absolutely separable* iff $U\rho^{AB}U^\dagger$ is separable for every unitary U acting on AB. Closely related is the notion of an *absolutely PPT* (APPT) state, namely a state whose partial transpose remains positive under all global unitaries. A longstanding open problem asks whether the sets of absolutely separable and absolutely PPT states coincide for arbitrary local dimensions [19, 22]. This question has been answered affirmatively when one of the local dimensions is equal to two [18] but remains open otherwise.

An important structural property of the set of absolutely separable states (which includes the set of completely absolutely separable states) is that it is not closed under tensor products. Every non maximally mixed bipartite state ρ^{AB} fails to remain absolutely separable under sufficiently many tensor powers. Precisely, there exists a finite $n \in \mathbb{N}$ such that $(\rho^{AB})^{\otimes n}$ can be entangled by a global unitary and is therefore not absolutely separable. In Sec. J of the Supplemental Material, we show that it is enough to take

$$n > \frac{\ln\left(R(\rho_{AB}) + 2\sqrt{R(\rho_{AB})}\right)}{\ln R(\rho_{AB})}. \tag{13}$$

with $R(\rho^{AB})$ the ratio of the largest to the smallest eigenvalue of ρ^{AB}. In fact, there even exist absolutely separable states, which are not closed even under attaching maximally mixed states. To illustrate this, let $D = d_A d_B$ denote the total dimension, and recall that any absolutely separable state must have rank at least $D - 1$ [22] (see Fig. 1). Consider an absolutely separable state ρ whose spectrum consists of $D-1$ equal nonzero eigenvalues and one zero eigenvalue; such states are known to be absolutely separable [14]. For any ancillary maximally mixed state of dimension $\tilde{D}$, we have

$$\mathrm{rank}\left(\rho \otimes \frac{\mathbb{1}}{\tilde{D}}\right) = \mathrm{rank}(\rho) \cdot \tilde{D} = (D-1) \cdot \tilde{D} < D\tilde{D} - 1. \tag{14}$$

Therefore, $\rho \otimes \frac{\mathbb{1}}{\tilde{D}}$ cannot be absolutely separable, regardless of the bipartition. This naturally leads to the following question: can one characterize the set of bipartite states ρ^{AB} such that $\rho^{AB} \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ remains absolutely separable for every $d_{B'} \in \mathbb{N}$? In the following theorem, we show that this set coincides exactly with the set of completely absolutely separable states, when $d_A \leq d_B$.

Theorem 2. *Let ρ^{AB} be a state acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then the following statements are equivalent:*

(i) $\rho^{AB} \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ is absolutely separable for all $d_{B'} \in \mathbb{N}$.

(ii) $\rho^{AB} \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ is absolutely PPT for all $d_{B'} \in \mathbb{N}$.

(iii) $R(\rho^{AB}) \leq \frac{d_A+1}{d_A-1}$.

The proof is given in Sec. F of the Supplemental Material. Note that, when $d_A \leq d_B$, this class is precisely the set of completely absolutely separable states (see Theorem (3)). This motivates the name *completely* absolutely separable in analogy to *completely* positive maps.

Conclusion and final remarks.— We have investigated the most fundamental limitations on entanglement generation from purity by going beyond deterministic unital dynamics and considering the full class of probabilistic unital channels. In this more general setting, we showed that absolute separability is not the ultimate obstruction to entanglement extraction: certain absolutely separable states can still generate entanglement with nonzero probability. Motivated by this, we introduced the notion of *complete absolute separability* (CAS), capturing precisely those states from which entanglement cannot be generated with any nonzero probability by any probabilistic purity-non-generating process.

Our main result is a complete characterization of CAS states in arbitrary bipartite dimensions. Remarkably, this characterization is purely spectral and depends only on the ratio between the largest and smallest eigenvalues and on the smaller local dimension. Along the way, we obtained a new sufficient condition for separability, also expressed only in terms of the eigenvalue ratio and the smallest local dimension. This criterion is independent of previously known spectral separability tests and is especially powerful for systems with unequal local dimensions, where it detects absolutely separable states beyond the reach of any earlier sufficient conditions. We further showed that the same spectral threshold has multipartite implications, yielding a simple guarantee of separability across broad classes of bipartitions.

Finally, we established a structural connection between CAS and the longstanding separability-from-spectrum problem: CAS states are exactly those that remain absolutely separable after adjoining an arbitrary maximally mixed ancilla locally. We hope that these results help clarify the operational role of purity as a resource for entanglement generation, and that the perspective developed here will

prove useful for further progress on absolute separability and multipartite entanglement structure.

Acknowledgments.— We thank Anna Sanpera for introducing us to problem of absolute separability. We also thank Eric Chitambar, Michael Epping, Ludovico Lami, Peter Ken Schuhmacher, and Nikolai Wyderka for helpful discussions.

This work has been supported by the German Ministry of Education and Research (Projects QuKuK, BMBF Grant No. 16KIS1618K and QSolid, BMFTR Grant No. 13N16163). P.B thanks the DLR Quantum Computing Initiative and the Federal Ministry for Economic Affairs and Climate Action. We also acknowledge financial support by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769.

* tuljavarun@gmail.com
† pbhita99@gmail.com

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Physical Review Letters **70**, 1895 (1993).
[3] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum metrology, Phys. Rev. Lett. **96**, 010401 (2006).
[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[5] A. Streltsov, G. Adesso, and M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. **89**, 041003 (2017).
[6] M. Lostaglio, An introductory review of the resource theory approach to thermodynamics, Reports on Progress in Physics **82**, 114001 (2019).
[7] V. Veitch, S. A. Hamed Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New Journal of Physics **16**, 013009 (2014).
[8] A. Streltsov, H. Kampermann, S. Wölk, M. Gessner, and D. Bruß, Maximal coherence and the resource theory of purity, New Journal of Physics **20**, 053058 (2018).
[9] W. H. Zurek, Decoherence, einselection, and the quantum origins of the classical, Rev. Mod. Phys. **75**, 715 (2003).
[10] M. S. Anwar, D. Blazina, H. A. Carteret, S. B. Duckett, T. K. Halstead, J. A. Jones, C. M. Kozak, and R. J. K. Taylor, Preparing high purity initial states for nuclear magnetic resonance quantum computing, Phys. Rev. Lett. **93**, 040501 (2004).
[11] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, A quantum engineer's guide to superconducting qubits, Applied Physics Reviews **6**, 10.1063/1.5089550 (2019).
[12] C. B. Mendl and M. M. Wolf, Unital quantum channels – convex structure and revivals of birkhoff's theorem, Communications in Mathematical Physics **289**, 1057–1086 (2009).
[13] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Yunger Halpern, The resource theory of informational nonequilibrium in thermodynamics, Physics Reports **583**, 1–58 (2015).
[14] L. Gurvits and H. Barnum, Largest separable balls around the maximally mixed bipartite quantum state, Phys. Rev. A **66**, 062311 (2002).
[15] R. Hildebrand, Entangled states close to the maximally mixed state, Phys. Rev. A **75**, 062330 (2007).
[16] M. Kuś and K. Życzkowski, Geometry of entangled states, Phys. Rev. A **63**, 032307 (2001).
[17] A. Patra, A. Maity, and A. Sen(De), Resource theory of nonabsolute separability, Phys. Rev. A **108**, 042402 (2023).
[18] N. Johnston, Separability from spectrum for qubit-qudit states, Phys. Rev. A **88**, 062330 (2013).
[19] E. Knill, Separability from spectrum, Open Quantum Problems, IQOQI Vienna, Problem 15 (2003), problem page last updated 2013.
[20] A. Peres, Separability criterion for density matrices, Phys. Rev. Lett. **77**, 1413 (1996).
[21] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Physics Letters A **223**, 1–8 (1996).
[22] S. Arunachalam, N. Johnston, and V. Russo, Is absolute separability determined by the partial transpose? (2015), arXiv:1405.5853 [quant-ph].
[23] M. A. Jivulescu, N. Lupa, I. Nechita, and D. Reeb, Positive reduction from spectra, Linear Algebra and its Applications **469**, 276 (2015).
[24] S. Patro, I. Chakrabarty, and N. Ganguly, Non-negativity of conditional von neumann entropy and global unitary operations, Phys. Rev. A **96**, 062102 (2017).
[25] J. Abellanet-Vidal, G. Müller-Rigat, G. Rajchel-Mieldzioć, and A. Sanpera, Sufficient criteria for absolute separability in arbitrary dimensions via linear map inverses, Reports on Progress in Physics **88**, 107601 (2025).
[26] M. Lewenstein, R. Augusiak, D. Chruściński, S. Rana, and J. Samsonowicz, Sufficient separability criteria and linear maps, Physical Review A **93**, 10.1103/physreva.93.042335 (2016).
[27] B. Regula, Probabilistic transformations of quantum resources, Phys. Rev. Lett. **128**, 110505 (2022).
[28] B. Regula, Tight constraints on probabilistic convertibility of quantum states, Quantum **6**, 817 (2022).
[29] B. Regula, L. Lami, and M. M. Wilde, Overcoming entropic limitations on asymptotic state transformations through probabilistic protocols, Phys. Rev. A **107**, 042401 (2023).
[30] B. Regula and L. Lami, Reversibility of quantum resources through probabilistic protocols, Nature Communications **15**, 10.1038/s41467-024-47243-2 (2024).
[31] R. Hildebrand, Positive partial transpose from spectra, Phys. Rev. A **76**, 052325 (2007).
[32] F. Verstraete, K. Audenaert, and B. De Moor, Maximally entangled mixed states of two qubits, Phys. Rev. A **64**, 012316 (2001).
[33] S. Halder, S. Mal, and A. Sen(De), Characterizing the boundary of the set of absolutely separable states and their generation via noisy environments, Phys. Rev. A **103**, 052431 (2021).
[34] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, The resource theory of informational nonequilibrium in thermodynamics, Physics Reports **583**, 1–58 (2015).
[35] Z. Song and L. Chen, Spectral characterizations of entanglement witnesses (2025), arXiv:2508.11308 [quant-ph].
[36] G. Sarbicki, Spectral properties of entanglement witnesses,

Journal of Physics A: Mathematical and Theoretical **41**, 375303 (2008).
[37] G. Champagne, N. Johnston, M. MacDonald, and L. Pipes, Spectral properties of symmetric quantum states and symmetric entanglement witnesses, Linear Algebra and its Applications **649**, 273–300 (2022).
[38] M. Keyl and R. F. Werner, Estimating the spectrum of a density operator, Phys. Rev. A **64**, 052311 (2001).
[39] P. Cieśliński, S. Imai, J. Dziewior, O. Gühne, L. Knips, W. Laskowski, J. Meinecke, T. Paterek, and T. Vértesi, Analysing quantum systems with randomised measurements, Physics Reports **1095**, 1 (2024), analysing quantum systems with randomised measurements.
[40] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, Sample-optimal tomography of quantum states, IEEE Transactions on Information Theory **63**, 5628 (2017).
[41] S. N. Filippov, K. Y. Magadov, and M. A. Jivulescu, Absolutely separating quantum maps and channels, New Journal of Physics **19**, 083010 (2017).
[42] H. P. Dung and V. T. Khoi, On the maximum purity of absolutely separable bipartite states (2025), arXiv:2510.19508 [math-ph].

SUPPLEMENTAL MATERIAL

A. Upper bound on the 1-norm of entanglement witnesses

Lemma 1. *Let W be a hermitian block-positive operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\operatorname{Tr} W = 1$. Then*

$$\|W\|_1 \leq d. \tag{15}$$

where, $d = \min\{d_A, d_B\}$.

Proof. Without loss of generality, let us assume $d_A \leq d_B$. Rewrite W via its block decomposition by choosing a basis $\{|i\rangle\}_i$ of $\mathcal{H}_A$

$$W = \sum_{i,j=1}^{d_A} |i\rangle\langle j| \otimes \widetilde{W}_{ij}, \qquad t_i := \operatorname{Tr} \widetilde{W}_{ii} \geq 0, \qquad \sum_{i=1}^{d_A} t_i = 1, \tag{16}$$

Note that, the condition $\widetilde{W}_{ii} \geq 0$ follows from block-positivity of W. Fix $i \neq j$ and a unit vector $|\psi\rangle \in \mathcal{H}_B$. Block positivity gives

$$\begin{aligned} 0 &\leq \Big((\alpha^* \langle i| + \beta^* \langle j|) \otimes \langle\psi|\Big) W \Big((\alpha |i\rangle + \beta |j\rangle) \otimes |\psi\rangle\Big) \\ &= |\alpha|^2 a + |\beta|^2 f + \alpha^* \beta\, c + \beta^* \alpha\, c^* \\ &= (\alpha^* \ \beta^*) \begin{pmatrix} a & c \\ c^* & f \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \ \forall\ \alpha, \beta \in \mathbb{C}, \end{aligned} \tag{17}$$

where $a = \langle\psi|\widetilde{W}_{ii}|\psi\rangle$, $f = \langle\psi|\widetilde{W}_{jj}|\psi\rangle$, $c = \langle\psi|\widetilde{W}_{ij}|\psi\rangle$. Note that, since W is Hermitian, we have

$$\widetilde{W}_{ij} = \widetilde{W}_{ji}^{\dagger}.$$

Hence, if $\langle\psi|\widetilde{W}_{ij}|\psi\rangle = c$, then

$$\langle\psi|\widetilde{W}_{ji}|\psi\rangle = \langle\psi|\widetilde{W}_{ij}^{\dagger}|\psi\rangle = \langle\psi|\widetilde{W}_{ij}|\psi\rangle^* = c^*.$$

Hence the 2×2 matrix $M = \left(\begin{smallmatrix} a & c \\ c^* & f \end{smallmatrix}\right)$ is positive-semidefinite. Because M is Hermitian, Sylvester's criterion says that M is positive-semidefinite *iff* its principal minors are non-negative, therefore

$$\det M = af - |c|^2 \geq 0. \tag{18}$$

Hence

$$|c|^2 \leq af \implies |c| \leq \sqrt{af}. \tag{19}$$

The arithmetic geometric mean inequality gives $\sqrt{af} \leq \frac{1}{2}(a + f)$, so altogether

$$|c| \leq \frac{1}{2}(a + f). \tag{20}$$

We can write the 1-norm of any linear operator X as $\|X\|_1 = \sup_U |\operatorname{Tr}(UX)|$ with U a unitary operator. Choose X to be $\widetilde{W}_{ij}$ and choose an orthonormal basis $\{|\psi_k\rangle\}_k$ of $\mathcal{H}_B$. Without loss of generality we can choose $\{|\psi_k\rangle\}_k$ to be the eigenbasis of U. Then,

$$\begin{aligned} |\operatorname{Tr}\big(U\widetilde{W}_{ij}\big)| &= \Big|\sum_k e^{i\theta_k} \langle\psi_k|\widetilde{W}_{ij}|\psi_k\rangle\Big| \leq \sum_k |\langle\psi_k|\widetilde{W}_{ij}|\psi_k\rangle| \\ &\overset{(20)}{\leq} \frac{1}{2}\sum_k \Big(\langle\psi_k|\widetilde{W}_{ii}|\psi_k\rangle + \langle\psi_k|\widetilde{W}_{jj}|\psi_k\rangle\Big) = \frac{1}{2}(t_i + t_j), \end{aligned} \tag{21}$$

with $\theta_k \in [0, 2\pi]$ and $t_j = \operatorname{Tr} \widetilde{W}_{jj}$. We used the fact that U is unitary and thus, $U|\psi_k\rangle = e^{i\theta_k}|\psi_k\rangle$. Taking the supremum over U yields

$$\|\widetilde{W}_{ij}\|_1 \leq \frac{1}{2}(t_i + t_j) \qquad \forall i, j. \tag{22}$$

Now using that $\||i\rangle\langle j| \otimes \widetilde{W}_{ij}\|_1 = \|\widetilde{W}_{ij}\|_1$ and the triangular inequality

$$\begin{aligned} \|W\|_1 &\leq \sum_{i,j}^{d_A} \||i\rangle\langle j| \otimes \widetilde{W}_{ij}\|_1 = \sum_{i,j}^{d_A} \|\widetilde{W}_{ij}\|_1 \\ &\overset{(22)}{\leq} \sum_{i,j}^{d_A} \frac{1}{2}(t_i + t_j) = d_A. \end{aligned} \tag{23}$$

The last inequality follows from $\sum_{i=1}^{d_A} t_i = 1$. This completes the proof. □

B. Proof of the sufficient condition for separability

Lemma 2. *A bipartite state ρ is separable if*

$$R(\rho) \leq \frac{d+1}{d-1}, \tag{24}$$

where $d = \min\{d_A, d_B\}$.

Proof. By assumption,

$$R(\rho) \leq \frac{d+1}{d-1},$$

so $\lambda_{\min}(\rho) > 0$. Define

$$\Delta := I - \frac{\rho}{\lambda_{\max}(\rho)}.$$

Then $\Delta \geq 0$, and

$$\|\Delta\|_\infty = 1 - \frac{\lambda_{\min}(\rho)}{\lambda_{\max}(\rho)} = 1 - \frac{1}{R(\rho)} \leq 1 - \frac{d-1}{d+1} = \frac{2}{d+1}.$$

Let W be any entanglement witness normalized by $\operatorname{Tr} W = 1$. Write

$$W = W_+ - W_-, \qquad W_+, W_- \geq 0, \qquad W_+ W_- = 0.$$

Set

$$a^+ := \operatorname{Tr} W_+, \qquad a^- := \operatorname{Tr} W_-.$$

Since $\operatorname{Tr} W = 1$,

$$a^+ - a^- = 1.$$

Moreover, by Lemma 1,

$$\|W\|_1 = a^+ + a^- \le d.$$

Hence

$$a^+ \le \frac{d+1}{2}.$$

Now

$$\operatorname{Tr}(\rho W) = \lambda_{\max} \operatorname{Tr}((I-\Delta)W) = \lambda_{\max}(1 - \operatorname{Tr}(\Delta W)).$$

Since $\Delta \ge 0$,

$$\operatorname{Tr}(\Delta W) = \operatorname{Tr}(\Delta W_+) - \operatorname{Tr}(\Delta W_-) \le \operatorname{Tr}(\Delta W_+).$$

Using $\Delta \le \|\Delta\|_\infty I$, we get

$$\operatorname{Tr}(\Delta W_+) \le \|\Delta\|_\infty \operatorname{Tr} W_+ \le \frac{2}{d+1} \cdot \frac{d+1}{2} = 1.$$

Therefore

$$\operatorname{Tr}(\rho W) = \lambda_{\max}(1 - \operatorname{Tr}(\Delta W)) \ge 0.$$

Thus $\operatorname{Tr}(\rho W) \ge 0$ for every entanglement witness W with $\operatorname{Tr} W = 1$. Since every entangled state is detected by some entanglement witness, ρ is separable. □

C. Example of an absolutely but not completely absolutely separable state

Consider the two-qubit state

$$\rho = \frac{1}{3}\Big(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|\Big) = \operatorname{diag}\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0\right),$$

which is absolutely separable in $2 \otimes 2$. Let

$$\rho_W = \frac{1}{2}\left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + \frac{\mathbb{1}}{8}, \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

This Werner state is full rank and entangled. Set

$$\lambda = \frac{5}{2}, \qquad \sigma = \lambda\frac{\mathbb{1}}{4} - \rho_W.$$

Note that, $\sigma \ge 0$ and

$$\operatorname{Tr}\sigma = \lambda - 1 = \frac{3}{2}.$$

Thus the normalized state associated with σ is

$$\widehat{\sigma} := \frac{\sigma}{\operatorname{Tr}\sigma} = \frac{2}{3}\sigma.$$

Now define the sub-POVM effects

$$E_\sigma = |11\rangle\langle 11| = \operatorname{diag}(0,0,0,1),$$

and

$$E_W = \frac{2}{9}\Big(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|\Big) = \operatorname{diag}\left(\frac{2}{9}, \frac{2}{9}, \frac{2}{9}, 0\right).$$

They satisfy

$$E_\sigma + E_W = \operatorname{diag}\left(\frac{2}{9}, \frac{2}{9}, \frac{2}{9}, 1\right) \le \mathbb{1}.$$

Equivalently, the missing failure effect is

$$E_{\text{fail}} = I_4 - E_\sigma - E_W = \operatorname{diag}\left(\frac{7}{9}, \frac{7}{9}, \frac{7}{9}, 0\right) \ge 0.$$

Hence $\{E_\sigma, E_W, E_{\text{fail}}\}$ is a valid POVM.

Define the stochastic measure-and-prepare map

$$\Lambda[X] = \operatorname{Tr}(E_\sigma X)\,\widehat{\sigma} + \operatorname{Tr}(E_W X)\,\rho_W.$$

The map is completely positive because it is measure-and-prepare, and it is trace-non-increasing because

$$E_\sigma + E_W \le \mathbb{1}.$$

We now check stochastic unitality. Note that,

$$\operatorname{Tr}(E_\sigma) = 1, \qquad \operatorname{Tr}(E_W) = \frac{2}{3}.$$

Therefore

$$\Lambda[\mathbb{1}] = \widehat{\sigma} + \frac{2}{3}\rho_W = \frac{5}{12}\mathbb{1}$$

Hence Λ is stochastic unital. Finally, evaluate Λ on ρ. Since ρ has no support on $|11\rangle$,

$$\operatorname{Tr}(E_\sigma \rho) = 0.$$

On the other hand,

$$\operatorname{Tr}(E_W \rho) = \frac{2}{9}\left(\frac{1}{3} + \frac{1}{3} + \frac{1}{3}\right) = \frac{2}{9}.$$

Thus

$$\Lambda[\rho] = \frac{2}{9}\rho_W.$$

Thus the post-selected output is

$$\frac{\Lambda[\rho]}{\operatorname{Tr}\Lambda[\rho]} = \rho_W,$$

which is entangled, and the success probability is

$$\operatorname{Tr}\Lambda[\rho] = \frac{2}{9}.$$

D. Probabilistic unital transformations

We now characterize state transformations under stochastic unital maps. Throughout this section, the input and output systems have the same dimension D. A stochastic unital map is a completely positive trace-nonincreasing map Λ such that

$$\Lambda(\mathbb{1}) = q\mathbb{1} \tag{25}$$

for some $q > 0$.

We first prove a simple necessary condition. Let ρ be full rank. Then

$$\lambda_{\min}(\rho)\mathbb{1} \le \rho \le \lambda_{\max}(\rho)\mathbb{1}. \tag{26}$$

Applying a stochastic unital map Λ, we obtain

$$q\lambda_{\min}(\rho)\mathbb{1} \le \Lambda(\rho) \le q\lambda_{\max}(\rho)\mathbb{1}. \tag{27}$$

Assume that the transformation succeeds with nonzero probability and define

$$\sigma = \frac{\Lambda(\rho)}{\mathrm{Tr}[\Lambda(\rho)]}. \tag{28}$$

It follows that

$$\lambda_{\min}(\sigma) \ge \frac{q\lambda_{\min}(\rho)}{\mathrm{Tr}[\Lambda(\rho)]}, \qquad \lambda_{\max}(\sigma) \le \frac{q\lambda_{\max}(\rho)}{\mathrm{Tr}[\Lambda(\rho)]}. \tag{29}$$

Hence

$$\frac{\lambda_{\max}(\sigma)}{\lambda_{\min}(\sigma)} \le \frac{\lambda_{\max}(\rho)}{\lambda_{\min}(\rho)}. \tag{30}$$

In particular, a full-rank state cannot be transformed with nonzero probability into a non-full-rank state.

We now prove sufficiency. We show that if either ρ is singular, or both ρ and σ are full rank and

$$\frac{\lambda_{\max}(\rho)}{\lambda_{\min}(\rho)} \ge \frac{\lambda_{\max}(\sigma)}{\lambda_{\min}(\sigma)},$$

then there exists a stochastic unital map transforming ρ into σ with nonzero probability.

If $\sigma = \mathbb{1}/D$, the claim is immediate, since the channel

$$\mathcal{E}(X) = \mathrm{Tr}(X)\frac{\mathbb{1}}{D}$$

is unital and maps every state to $\mathbb{1}/D$. Hence assume $\sigma \neq \mathbb{1}/D$.

First suppose that σ is full rank. Define

$$\alpha = D\lambda_{\max}(\sigma), \qquad \beta = \frac{1}{D\lambda_{\min}(\sigma)}.$$

Then $\alpha, \beta > 1$, and

$$\alpha\beta = \frac{\lambda_{\max}(\sigma)}{\lambda_{\min}(\sigma)}.$$

Set

$$\phi_1 = \frac{\sigma - \beta^{-1}\frac{\mathbb{1}}{D}}{1-\beta^{-1}}, \qquad \phi_2 = \frac{\alpha\frac{\mathbb{1}}{D} - \sigma}{\alpha - 1}.$$

Since

$$\beta^{-1}\frac{\mathbb{1}}{D} \le \sigma \le \alpha\frac{\mathbb{1}}{D},$$

both ϕ_1 and ϕ_2 are states. Moreover,

$$(1-\beta^{-1})\phi_1 + (\alpha-1)\phi_2 = \left(\alpha - \beta^{-1}\right)\frac{\mathbb{1}}{D}.$$

Choose unit vectors $|x\rangle, |y\rangle$ such that

$$\frac{\langle x|\rho|x\rangle}{\langle y|\rho|y\rangle} = \alpha\beta.$$

This is possible by the assumed spectral-ratio condition if ρ is full rank. If ρ is singular, choose $|x\rangle$ as a maximal-eigenvalue eigenvector and interpolate with a vector in $\ker\rho$.

Now set

$$k = \frac{\alpha-1}{1-\beta^{-1}} > 0, \qquad 0 < c \le \frac{1}{1+k},$$

and define

$$M_1 = c\,|x\rangle\langle x|, \qquad M_2 = ck\,|y\rangle\langle y|.$$

Then

$$M_1 + M_2 \le c(1+k)\mathbb{1} \le \mathbb{1},$$

so $\{M_1, M_2\}$ is a valid sub-POVM. Define

$$\mathcal{E}_{\mathrm{s}}(X) = \mathrm{Tr}(M_1X)\phi_1 + \mathrm{Tr}(M_2X)\phi_2.$$

This map is completely positive and trace nonincreasing. Furthermore,

$$\begin{aligned}\mathcal{E}_{\mathrm{s}}(\mathbb{1}) &= c\phi_1 + ck\phi_2 \\ &= \frac{c}{1-\beta^{-1}}\left[(1-\beta^{-1})\phi_1 + (\alpha-1)\phi_2\right] \\ &= \frac{c(\alpha-\beta^{-1})}{1-\beta^{-1}}\frac{\mathbb{1}}{D}.\end{aligned}$$

Hence $\mathcal{E}_{\mathrm{s}}$ is stochastic unital.

It remains to check the output on ρ. Let

$$a = \mathrm{Tr}(M_1\rho), \qquad b = \mathrm{Tr}(M_2\rho).$$

Then

$$\frac{b}{a} = k\frac{\langle y|\rho|y\rangle}{\langle x|\rho|x\rangle} = \frac{k}{\alpha\beta} = \frac{\alpha-1}{\alpha(\beta-1)} =: r.$$

A direct substitution gives

$$\phi_1 + r\phi_2 = (1+r)\sigma.$$

Therefore

$$\mathcal{E}_s(\rho) = a\phi_1 + b\phi_2 = a(\phi_1 + r\phi_2) = (a+b)\sigma.$$

Since $a + b > 0$, the normalized post-selected output is σ.

It remains only to handle the case where ρ is singular and σ is arbitrary. Choose

$$\alpha > D\lambda_{\max}(\sigma)$$

and define

$$\phi_1 = \sigma, \qquad \phi_2 = \frac{\alpha\frac{\mathbb{1}}{D} - \sigma}{\alpha - 1}.$$

Then ϕ_2 is a state. Let $|x\rangle$ be a maximal-eigenvalue eigenvector of ρ, and choose $|y\rangle \in \ker\rho$. Set

$$k = \alpha - 1, \qquad 0 < c \le \frac{1}{1+k},$$

and define

$$M_1 = c\,|x\rangle\langle x|, \qquad M_2 = ck\,|y\rangle\langle y|.$$

Again $M_1 + M_2 \le \mathbb{1}$, so the map

$$\mathcal{E}_s(X) = \mathrm{Tr}(M_1X)\phi_1 + \mathrm{Tr}(M_2X)\phi_2$$

is completely positive and trace nonincreasing. Moreover,

$$\mathcal{E}_s(\mathbb{1}) = c\sigma + c(\alpha-1)\phi_2 = c\alpha\frac{\mathbb{1}}{D},$$

so it is stochastic unital. Since $|y\rangle \in \ker\rho$,

$$\mathcal{E}_s(\rho) = c\lambda_{\max}(\rho)\sigma.$$

Thus the transformation succeeds with nonzero probability and the normalized output is σ.

This proves the sufficiency of the stated condition.

E. Proof of theorem 1

Theorem 3. *A bipartite state ρ^{AB} is completely absolutely separable if and only if*

$$R(\rho^{AB}) \le \frac{d+1}{d-1},$$

where

$$R(\rho) := \frac{\lambda_{\max}(\rho)}{\lambda_{\min}(\rho)}, \qquad d = \min\{d_A, d_B\}.$$

Proof. Suppose first that

$$R(\rho) \le \frac{d+1}{d-1}.$$

Then ρ is full rank. Let Λ be any stochastic unital operation with $\Lambda(\rho) \neq 0$, and define

$$\sigma = \frac{\Lambda(\rho)}{\mathrm{Tr}[\Lambda(\rho)]}.$$

By monotonicity of the spectral ratio under stochastic unital maps,

$$R(\sigma) \le R(\rho) \le \frac{d+1}{d-1}.$$

Hence, by Lemma 2, σ is separable. Thus no stochastic unital operation can produce entanglement from ρ, so ρ is completely absolutely separable.

Conversely, suppose

$$R(\rho) > \frac{d+1}{d-1}.$$

We show that ρ can be mapped probabilistically to an entangled state.

Let

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle_A \otimes |i\rangle_B, \qquad W = \left|\Phi^+\rangle\langle\Phi^+\right|^{\Gamma}.$$

Here Γ denotes partial transposition with respect to B. For $0 \le t < d$, define

$$\omega_t = \frac{\mathbb{1} - tW}{D - t}, \qquad D = d_Ad_B.$$

Since W has spectrum contained in $[-1/d, 1/d]$, the operator ω_t is a state. Its spectral ratio is

$$R(\omega_t) = \frac{1 + t/d}{1 - t/d}.$$

Moreover,

$$\omega_t^{\Gamma} = \frac{\mathbb{1} - t|\Phi^+\rangle\langle\Phi^+|}{D - t}.$$

Thus, whenever $t > 1$, the partial transpose has eigenvalue

$$\frac{1-t}{D-t} < 0,$$

so ω_t is entangled. Now choose

$$t = d\left(\frac{R(\rho)-1}{R(\rho)+1}\right).$$

The assumption $R(\rho) > (d+1)/(d-1)$ implies $t > 1$, and clearly $t < d$. Therefore ω_t is entangled and satisfies

$$R(\omega_t) = R(\rho).$$

If ρ is full rank, the stochastic-unital transformation criterion gives a stochastic unital map sending ρ to ω_t with nonzero probability, since $R(\rho) = R(\omega_t)$. If ρ is not full rank, the singular-input case of the same criterion allows a stochastic unital transformation from ρ to any target state, in particular to ω_t.

Hence, whenever

$$R(\rho) > \frac{d+1}{d-1},$$

the state ρ can be probabilistically transformed by a stochastic unital operation into an entangled state. Therefore ρ is not completely absolutely separable. This proves the theorem. □

F. Proof of Theorem 2

Theorem 4. *Let ρ be a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_B$, with $d_A \leq d_B$. Then the following statements are equivalent:*

(i) $\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ is absolutely separable across the bipartition $A : BB'$ for every $d_{B'} \in \mathbb{N}$.

(ii) $\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ is absolutely PPT across the bipartition $A : BB'$ for every $d_{B'} \in \mathbb{N}$.

(iii)

$$R(\rho) \leq \frac{d_A + 1}{d_A - 1}.$$

Proof. We prove the implications

$$\text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(i)} \Rightarrow \text{(ii)}.$$

Proof of (ii) $\Rightarrow$ (iii). Assume that $\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$ is absolutely PPT for every $d_{B'}$. Thus, for every unitary U and every vector $|\psi\rangle$,

$$\operatorname{Tr}\left[\left(U\left(\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}\right)U^\dagger\right)^\Gamma |\psi\rangle\langle\psi|\right] \geq 0.$$

Equivalently,

$$\operatorname{Tr}\left[\left(\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}\right)U^\dagger |\psi\rangle\langle\psi|^\Gamma U\right] \geq 0.$$

Here Γ denotes partial transposition with respect to BB'.

Since condition (ii) holds for every $d_{B'}$, choose

$$d_{B'} \geq \frac{d_A(d_A + 1)}{2}. \tag{31}$$

Write the Schmidt decomposition of $|\psi\rangle$ across $A : BB'$ as

$$|\psi\rangle = \sum_{i=1}^{d_A} \sqrt{p_i}\, |i\rangle_A \otimes |i\rangle_{BB'}, \qquad p_i \geq 0, \qquad \sum_i p_i = 1.$$

The spectrum of $|\psi\rangle\langle\psi|^\Gamma$ consists of

$$p_i, \qquad \pm\sqrt{p_i p_j} \quad (i < j),$$

together with possible additional zero eigenvalues. Hence it has

$$\frac{d_A(d_A - 1)}{2}$$

negative eigenvalues and

$$\frac{d_A(d_A + 1)}{2}$$

positive eigenvalues. The eigenvalues of

$$\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$$

are the eigenvalues of ρ divided by $d_{B'}$, each repeated $d_{B'}$ times. By the choice of $d_{B'}$ (see Eq. (31)), there are enough copies of $\lambda_{\max}(\rho)/d_{B'}$ to pair with all negative eigenvalues of $|\psi\rangle\langle\psi|^\Gamma$, and enough copies of $\lambda_{\min}(\rho)/d_{B'}$ to pair with all positive eigenvalues.

Using the rearrangement inequality for Hermitian matrices, we therefore obtain

$$\begin{aligned} 0 &\leq \min_U \operatorname{Tr}\left[\left(\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}\right)U^\dagger |\psi\rangle\langle\psi|^\Gamma U\right] \\ &= -\frac{\lambda_{\max}(\rho)}{d_{B'}} \sum_{i<j} \sqrt{p_i p_j} + \frac{\lambda_{\min}(\rho)}{d_{B'}}\left(\sum_i p_i + \sum_{i<j} \sqrt{p_i p_j}\right). \end{aligned}$$

Since $\sum_i p_i = 1$, this implies

$$\lambda_{\max}(\rho) \sum_{i<j} \sqrt{p_i p_j} \leq \lambda_{\min}(\rho)\left(1 + \sum_{i<j} \sqrt{p_i p_j}\right).$$

Thus, whenever $\sum_{i<j} \sqrt{p_i p_j} > 0$,

$$R(\rho) \leq 1 + \frac{1}{\sum_{i<j} \sqrt{p_i p_j}}.$$

Now choose $|\psi\rangle$ maximally entangled across a d_A-dimensional subspace, i.e.

$$p_i = \frac{1}{d_A} \qquad \text{for all } i = 1, \ldots, d_A.$$

Then

$$\sum_{i<j} \sqrt{p_i p_j} = \frac{d_A - 1}{2}.$$

Therefore

$$R(\rho) \leq 1 + \frac{2}{d_A - 1} = \frac{d_A + 1}{d_A - 1}.$$

This proves (iii).

Proof of (iii) $\Rightarrow$ (i). Assume

$$R(\rho) \leq \frac{d_A + 1}{d_A - 1}.$$

For every $d_{B'}$,

$$R\left(\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}\right) = R(\rho).$$

Moreover, for the bipartition $A : BB'$, the smaller local dimension is d_A. Hence for every global unitary U,

$$R\left(U\left(\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}\right)U^\dagger\right) = R(\rho) \leq \frac{d_A + 1}{d_A - 1}.$$

By Lemma 2, every state in the unitary orbit of

$$\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$$

is separable across $A : BB'$. Therefore

$$\rho \otimes \frac{\mathbb{1}_{B'}}{d_{B'}}$$

is absolutely separable for every $d_{B'}$. This proves (i).

Proof of $(i) \Rightarrow (ii)$. This is immediate, since every separable state is PPT. Therefore absolute separability implies absolute PPT.

Combining the three implications proves the equivalence. □

G. CAS states which cannot be detected by other existing spectral separability conditions

The best previously known spectral sufficient condition for absolute separability that we compare with is the convex hull of the two regions [25]

$$A := \left\{\rho : \rho \geq \frac{\mathbb{1}}{D+2},\ \mathrm{Tr}\,\rho = 1\right\}, \tag{32}$$

$$B := \left\{\rho : \mathrm{Tr}\left(\rho^2\right) \leq \frac{1}{D-1},\ \mathrm{Tr}\,\rho = 1\right\}. \tag{33}$$

We denote this region by

$$C := \mathrm{conv}(A \cup B).$$

The next lemma shows that the eigenvalue-ratio criterion detects states that are not contained in this convex hull.

Lemma 3. *Let* $2 \leq d_A < d_B$, $D = d_A d_B$, *and*

$$R := \frac{d_A + 1}{d_A - 1}.$$

Set

$$p := \lfloor D/2 \rfloor, \qquad q := \lceil D/2 \rceil, \qquad \ell := \frac{1}{p + qR}.$$

Define

$$\tilde{\rho} = \mathrm{diag}\left(\underbrace{\ell, \ldots, \ell}_{p}, \underbrace{R\ell, \ldots, R\ell}_{q}\right).$$

Then

$$R(\tilde{\rho}) = R = \frac{d_A + 1}{d_A - 1},$$

but

$$\tilde{\rho} \notin C.$$

Thus the eigenvalue-ratio criterion is not contained in the previously known convex-hull criterion.

Proof. The identity $R(\tilde{\rho}) = R$ is immediate from the definition.

Let P be the spectral projection of $\tilde{\rho}$ corresponding to the eigenvalue ℓ, and define

$$Z := \frac{1}{p} P - \frac{1}{q}(\mathbb{1} - P).$$

Then

$$\mathrm{Tr}\, Z = 0, \qquad \|Z\|_2^2 = \frac{1}{p} + \frac{1}{q} = \frac{D}{pq}.$$

Let us define W

$$W := \frac{\mathbb{1}}{D} + \sqrt{\frac{D-1}{D}}\,\frac{Z}{\|Z\|_2}.$$

We show that W is nonnegative on C, but negative on $\tilde{\rho}$.

First let $\rho \in B$ (see Eq. (33)). Writing $X = \rho - \mathbb{1}/D$, we have

$$\mathrm{Tr}\, X = 0, \qquad \|X\|_2^2 = \mathrm{Tr}\left(\rho^2\right) - \frac{1}{D} \leq \frac{1}{D(D-1)}.$$

Hence, by Cauchy–Schwarz,

$$\mathrm{Tr}(W\rho) = \frac{1}{D} + \sqrt{\frac{D-1}{D}}\,\frac{\mathrm{Tr}(ZX)}{\|Z\|_2} \geq \frac{1}{D} - \sqrt{\frac{D-1}{D}}\,\frac{1}{\sqrt{D(D-1)}} = 0.$$

Thus W is nonnegative on B.

Next let $\rho \in A$ (see Eq. (32)). Write

$$\rho = \frac{\mathbb{1}}{D+2} + X, \qquad X \geq 0, \qquad \mathrm{Tr}\, X = \frac{2}{D+2}.$$

Since

$$\lambda_{\min}(W) = \frac{1}{D} - \frac{1}{D}\sqrt{\frac{(D-1)p}{q}},$$

we get

$$\begin{aligned}\mathrm{Tr}(W\rho) &\geq \frac{1}{D+2} + \frac{2}{D+2}\lambda_{\min}(W) \\ &= \frac{D + 2 - 2\sqrt{\frac{(D-1)p}{q}}}{D(D+2)} \geq 0.\end{aligned}$$

Indeed, $p \leq q$, so whenever $D > 4$

$$2\sqrt{\frac{(D-1)p}{q}} \leq 2\sqrt{D-1} < D + 2.$$

Therefore W is nonnegative on A, and hence on $C = \mathrm{conv}(A \cup B)$.

It remains to evaluate W on $\tilde{\rho}$. Since

$$\mathrm{Tr}(Z\tilde{\rho}) = \ell - R\ell = -(R-1)\ell,$$

and

$$\ell = \frac{1}{p + qR}, \qquad \|Z\|_2^2 = \frac{D}{pq},$$

we get

$$\mathrm{Tr}(W\tilde{\rho}) = \frac{1}{D} - \frac{(R-1)}{p+qR}\sqrt{\frac{D-1}{D}}\,\frac{1}{\|Z\|_2}.$$

Equivalently,

$$\mathrm{Tr}(W\tilde{\rho}) = \frac{1}{D}\left[1 - \frac{(R-1)\sqrt{(D-1)pq}}{p+qR}\right].$$

Hence $\mathrm{Tr}(W\tilde{\rho}) < 0$ iff

$$(R-1)\sqrt{(D-1)pq} > p + qR. \qquad (*)$$

For $R = (d_A+1)/(d_A-1)$, $D = d_A d_B$, and $p = \lfloor D/2 \rfloor$, $q = \lceil D/2 \rceil$, inequality $(*)$ holds whenever $2 \le d_A < d_B$. Indeed, if D is even, $(*)$ reduces to

$$\sqrt{D-1} > d_A,$$

which follows from $D = d_A d_B$ and $d_B > d_A$. If D is odd, $(*)$ reduces, after squaring, to

$$d_A d_B\left[d_A^2 d_B(d_B - d_A) - d_A d_B - 2d_A - 1\right] > 0,$$

which is true for all $d_B > d_A$; the bracket is increasing in d_B and at $d_B = d_A + 1$ equals $d_A^3 - 3d_A - 1 > 0$.

Therefore $\mathrm{Tr}(W\tilde{\rho}) < 0$. Since W is nonnegative on C, it separates $\tilde{\rho}$ from C. Hence

$$\tilde{\rho} \notin C.$$

□

H. Maximum purity of CAS states

Lemma 4. *Let ρ be a completely absolutely separable state on $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\dim \mathcal{H}_A = d_A$, $\dim \mathcal{H}_B = d_B$, and $d_A \le d_B$. Then*

$$\mathrm{Tr}\left(\rho^2\right) \le \left(\frac{d_A}{d_B}\right)\frac{1}{d_A^2 - 1}. \qquad (34)$$

Proof. Write $D := d_A d_B$ for the total dimension and let $\{\lambda_i\}_{i=1}^D$ be the eigenvalues of ρ. Denote by $\lambda_{\max}$ and $\lambda_{\min}$ the largest and smallest eigenvalue, respectively. We start from a simple inequality that relates the purity to the extreme eigenvalues.

For every i, the eigenvalue λ_i lies between $\lambda_{\min}$ and $\lambda_{\max}$, i.e.,

$$\lambda_{\max} - \lambda_i \ge 0 \qquad \text{and} \qquad \lambda_i - \lambda_{\min} \ge 0. \qquad (35)$$

Therefore,

$$(\lambda_{\max} - \lambda_i)(\lambda_i - \lambda_{\min}) \ge 0 \qquad \text{for all } i. \qquad (36)$$

Summing over i and expanding the product gives

$$\begin{aligned} 0 &\le \sum_{i=1}^{D}(\lambda_{\max} - \lambda_i)(\lambda_i - \lambda_{\min}) \\ &= \sum_{i=1}^{D}(\lambda_{\max}\lambda_i - \lambda_{\max}\lambda_{\min} - \lambda_i^2 + \lambda_{\min}\lambda_i) \qquad (37) \\ &= \lambda_{\max}\sum_{i=1}^{D}\lambda_i \;-\; D\lambda_{\max}\lambda_{\min} \;-\; \sum_{i=1}^{D}\lambda_i^2 \;+\; \lambda_{\min}\sum_{i=1}^{D}\lambda_i. \end{aligned}$$

Using $\sum_i \lambda_i = \mathrm{Tr}(\rho) = 1$ and $\sum_i \lambda_i^2 = \mathrm{Tr}\left(\rho^2\right)$, we obtain

$$0 \le (\lambda_{\max} + \lambda_{\min}) - D\lambda_{\max}\lambda_{\min} - \mathrm{Tr}\left(\rho^2\right), \qquad (38)$$

or equivalently,

$$\mathrm{Tr}\left(\rho^2\right) \le \lambda_{\max} + \lambda_{\min} - D\lambda_{\max}\lambda_{\min} = \lambda_{\max}(1 - D\lambda_{\min}) + \lambda_{\min}. \qquad (39)$$

Next we use complete absolute separability. By assumption $\lambda_{\max} \le \left(\frac{d_A+1}{d_A-1}\right)\lambda_{\min}$. Plugging this into (39) yields a bound that depends only on $\lambda_{\min}$:

$$\mathrm{Tr}\left(\rho^2\right) \le \left(\frac{d_A+1}{d_A-1} + 1\right)\lambda_{\min} - D\frac{d_A+1}{d_A-1}\lambda_{\min}^2. \qquad (40)$$

The right hand side of (40) is a concave quadratic function of $\lambda_{\min}$, hence it attains its maximum at the unique critical point

$$\lambda_{\min} = \frac{1}{d_B(d_A+1)}. \qquad (41)$$

Therefore,

$$\mathrm{Tr}\left[\rho^2\right] \le \left(\frac{d_A}{d_B}\right)\frac{1}{d_A^2 - 1} \qquad (42)$$

which is the desired bound. □

Note that, for equal local dimensions (i.e. $d_A = d_B$), Eq. (34) coincides with the purity ball criterion $\left(\mathrm{Tr}\left(\rho^2\right) \le \frac{1}{d_A d_B - 1}\right)$. This means that, for equal local dimensions, CAS is a subset of the purity ball.

I. Maximum purity of AS states

For two qubits, $d_A = d_B = 2$, the maximal purity achievable by an absolutely separable state is known exactly and is equal to $3/8$ [42]. The next lemma gives an upper bound on the corresponding maximal purity in total dimension $D = d_A d_B > 4$.

Lemma 5. *There does not exist any absolutely separable state with purity more than $2/D$, where D is the total dimension of the system.*

Proof. We now combine the bound (39) with the APPT necessary condition. By the arithmetic–geometric mean inequality,

$$2\sqrt{\lambda_D\lambda_{D-2}} \le \lambda_D + \lambda_{D-2}. \tag{43}$$

Hence the APPT necessary condition

$$\lambda_{\max} \le \lambda_{D-1} + 2\sqrt{\lambda_D\lambda_{D-2}} \tag{44}$$

implies the simpler bound

$$\lambda_{\max} \le \lambda_{D-2} + \lambda_{D-1} + \lambda_D. \tag{45}$$

Since $\lambda_D = \lambda_{\min}$, and since $\lambda_{D-2}, \lambda_{D-1}$ are the two smallest eigenvalues among $\lambda_2, \ldots, \lambda_{D-1}$, we have (for $D > 4$)

$$\lambda_{D-2} + \lambda_{D-1} \le \frac{2}{D-2}\sum_{i=2}^{D-1}\lambda_i = \frac{2}{D-2}(1 - \lambda_{\max} - \lambda_{\min}). \tag{46}$$

Therefore, combining Eq. (45) and Eq. (46), we get

$$\lambda_{\max} \le \frac{2}{D-2}(1 - \lambda_{\max} - \lambda_{\min}) + \lambda_{\min}, \tag{47}$$

which simplifies to

$$D\lambda_{\max} \le 2 + (D-4)\lambda_{\min}. \tag{48}$$

Substituting this into (39), we obtain

$$\begin{aligned}
\mathrm{Tr}\left(\rho^2\right) &\le \lambda_{\max} + \lambda_{\min} - D\lambda_{\max}\lambda_{\min} \\
&= \lambda_{\max}(1 - D\lambda_{\min}) + \lambda_{\min} \\
&\le \frac{2 + (D-4)\lambda_{\min}}{D} + \lambda_{\min} - \lambda_{\min}(2 + (D-4)\lambda_{\min}) \\
&= \frac{2}{D} - \frac{4}{D}\lambda_{\min} - (D-4)\lambda_{\min}^2 \\
&\le \frac{2}{D}.
\end{aligned} \tag{49}$$

Thus,

$$\mathrm{Tr}\left(\rho^2\right) \le \frac{2}{D}. \tag{50}$$

□

In higher dimensions ($D > 4$), only upper bounds (Proposition 1 of Ref. [41]) were previously known. We now compare it with the bound obtained above and show that our bound of $2/D$ is strictly stronger. In our notation, Proposition 1 of Ref. [41] states that, if

$$\frac{1}{k} \le \mathrm{Tr}\left(\rho^2\right) \le \frac{1}{k-1},$$

then every absolutely separable state satisfies

$$1 + \sqrt{\frac{k\,\mathrm{Tr}(\rho^2) - 1}{k-1}} \le 3k\sqrt{\frac{\mathrm{Tr}(\rho^2)}{D+8}}.$$

Substituting $\mathrm{Tr}\left(\rho^2\right) = 2/D$, the condition is satisfied strictly. Indeed, for even D, choosing $k = D/2$, the condition becomes

$$1 < 3\sqrt{\frac{D}{2(D+8)}},$$

which holds for all even $D \ge 4$. For odd D, choosing $k = (D+1)/2$, the condition becomes

$$1 + \sqrt{\frac{2}{D(D-1)}} < \frac{3(D+1)}{2}\sqrt{\frac{2}{D(D+8)}},$$

which holds for all odd $D \ge 5$. Thus the condition of Proposition 1 in Ref. [41] is satisfied strictly at $\mathrm{Tr}\left(\rho^2\right) = 2/D$. By continuity, it remains satisfied for all values of $\mathrm{Tr}\left(\rho^2\right)$ in some interval above $2/D$. Hence Proposition 1 of Ref. [41] allows purities strictly larger than $2/D$, whereas the lemma above excludes all such purities. Therefore, the bound obtained here is strictly stronger than the bound of Ref. [41].

J. Proof that AS is not closed under k-copy tensor product

Lemma 6. *Let ρ_{AB} be a full-rank absolutely separable state distinct from the maximally mixed state. Then for every natural number*

$$n > \frac{\ln\left(R(\rho_{AB}) + 2\sqrt{R(\rho_{AB})}\right)}{\ln R(\rho_{AB})}, \tag{51}$$

we have $\rho_{AB}^{\otimes n} \notin AS$, where $R(\rho_{AB}) := \frac{\lambda_1}{\lambda_D}$ and $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_D > 0$ are the eigenvalues of ρ_{AB}.

Proof. Recall that absolutely separable states are absolutely PPT. Therefore, it is sufficient to show that $\rho_{AB}^{\otimes n}$ violates a necessary condition for absolute PPT. An absolutely PPT state with decreasingly ordered spectrum $\{\lambda_1, \ldots, \lambda_D\}$ satisfies the spectral inequality [31]

$$\lambda_1 \le \lambda_{D-1} + 2\sqrt{\lambda_D\lambda_{D-2}}. \tag{52}$$

For the spectrum of $n \ge 2$ copies of the state ρ_{AB}, the largest eigenvalue is λ_1^n, while the three smallest eigenvalues are

$$\lambda_D^n, \qquad \lambda_D^{n-1}\lambda_{D-1}, \qquad \lambda_D^{n-1}\lambda_{D-1}. \tag{53}$$

Hence, in order for $\rho_{AB}^{\otimes n}$ to be absolutely PPT, its eigenvalues have to satisfy

$$\begin{aligned}
\lambda_1^n &\le \lambda_D^{n-1}\lambda_{D-1} + 2\sqrt{\lambda_D^n\lambda_D^{n-1}\lambda_{D-1}} \\
&= \lambda_D^n\left(\frac{\lambda_{D-1}}{\lambda_D} + 2\sqrt{\frac{\lambda_{D-1}}{\lambda_D}}\right).
\end{aligned} \tag{54}$$

Dividing by $\lambda_D^n > 0$, we obtain the necessary condition

$$R(\rho_{AB})^n \le \frac{\lambda_{D-1}}{\lambda_D} + 2\sqrt{\frac{\lambda_{D-1}}{\lambda_D}}. \tag{55}$$

Since

$$\frac{\lambda_{D-1}}{\lambda_D} \leq \frac{\lambda_1}{\lambda_D} = R(\rho_{AB}), \tag{56}$$

we have

$$\frac{\lambda_{D-1}}{\lambda_D} + 2\sqrt{\frac{\lambda_{D-1}}{\lambda_D}} \leq R(\rho_{AB}) + 2\sqrt{R(\rho_{AB})}. \tag{57}$$

Therefore, if

$$R(\rho_{AB})^n > R(\rho_{AB}) + 2\sqrt{R(\rho_{AB})}, \tag{58}$$

then the necessary APPT condition (52) is violated. Equivalently, this violation occurs whenever

$$n > \frac{\ln\left(R(\rho_{AB}) + 2\sqrt{R(\rho_{AB})}\right)}{\ln R(\rho_{AB})}. \tag{59}$$

Thus $\rho_{AB}^{\otimes n}$ is not absolutely PPT, and since absolute separability implies absolute PPT, we conclude that $\rho_{AB}^{\otimes n} \notin AS$. The required number of copies decreases monotonically with $R(\rho_{AB})$. It diverges as $R(\rho_{AB}) \to 1^+$, i.e. as the state approaches the maximally mixed state, while it approaches 1 as $R(\rho_{AB}) \to \infty$. □

Paper D

The relative entropy of magic and its nonadditivity

The following text is reproduced from the preprint

Carolin Deckers, Justus Neumann, Hermann Kampermann, and Dagmar Bruß
The relative entropy of magic and its nonadditivity arXiv preprint, 2026. arXiv:2605.22392 [quant-ph].

Statement of contribution

My contribution consisted of supervising the project, contributing to the formulation of the research questions, discussing and developing the proof strategies, interpreting the results, and revising the manuscript. The main analytical results were derived by Carolin Deckers. Hermann Kampermann and Dagmar Bruß contributed to discussions and provided feedback on the presentation of the work. The manuscript was finalized with input from all authors.

arXiv:2605.22392v1 [quant-ph] 21 May 2026

The relative entropy of magic and its nonadditivity

Carolin Deckers, Justus Neumann, Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine Universität Düsseldorf, D-40225 Düsseldorf, Germany
(Dated: May 22, 2026)

In most stabilizer-based quantum computing schemes, so-called magic states are a necessary resource for implementing non-transversal quantum gates. With the resource theory of magic, it is possible to analyze and quantify the generation of the non-stabilizer states. The relative entropy is a measure used in various resource theories. For single qubits, we characterize magic states and their closest stabilizer states by applying analytical results known from the relative entropy of entanglement and show that the magic states and their closest stabilizer states are arranged symmetrically around the states at the centers of the faces of the stabilizer octahedron. For tensor products of single-qubit states, we prove analytically that the relative entropy of magic is nonadditive in almost all cases.

I. INTRODUCTION

Quantum computation promises advantages over classical computation by enabling information processing beyond classical capabilities. Quantum algorithms, such as Shor's factoring algorithm [1] and Grover's quantum search [2], have shown that quantum devices can outperform their classical counterparts.

For fault-tolerant quantum computation, the usage of error correction is mandatory, where stabilizer codes are used. In such schemes, easy-to-implement quantum circuits consist only of Clifford gates and stabilizer states, however they do not offer benefits because they are efficiently classically simulable as stated in the Gottesman-Knill theorem [3]. To achieve universal quantum computation, resources beyond the stabilizer formalism are required.

Adding a nonstabilizer (magic) state can solve this problem [4]. This motivates the resource theory of magic, which provides a theoretical framework to quantify the magic resources. Here, the set of free states is the convex hull of all stabilizer states. Various magic measures with distinct properties have been introduced for quantum applications. Well-known examples include the robustness of magic, see e.g., [5–7], the stabilizer Rényi entropies [8–11], and the relative entropy of magic [12]. The robustness of magic provides, for instance, bounds for tasks like gate synthesis costs [5]. Stabilizer Rényi entropies form a newer family of stabilizer measures proposed in [8] that are both efficiently computable [9] and experimentally accessible [10]. For two-qubit states, numerical optimizations identify specific states as candidates for maximizing this magic measure [11].

Veitch et al. introduced the relative entropy of magic as a measure in [12], defined analogously to the relative entropy of entanglement [13]. It quantifies how distinguishable a given state is from the set of stabilizer states and exhibits favorable properties such as subadditivity, faithfulness, and convexity. However, unlike some other measures, it lacks a closed analytic form and is often analyzed in the asymptotic regime [12]. In general, computing the relative entropy of a resource is a difficult optimization task, as it requires evaluating the distance to the full free set. The complexity of this computation depends strongly on the structure of the free set. In the resource theory of entanglement, for instance, determining the relative entropy of entanglement is known to be NP-hard [14]. Remarkably, it was shown that one can instead solve the converse problem: starting from a free state on the boundary of the free set, one can characterize all resourceful states for which it is the closest in terms of the relative entropy. This strategy led to a closed analytic expression for the entangled states that have the same closest separable state. This approach was first introduced in [13] in the context of the resource theory of entanglement and has been generalized to resource theories with a compact convex set of free states in [15], which holds for the set of stabilizer states.

In this paper, we apply the results of [13] to the resource theory of magic and use them to analyze the relative entropy of magic. For a single qubit, we investigate the distribution of magic states and their closest stabilizer states in the Bloch ball, distinguishing between stabilizer states that lie on edges and those on the facets of the stabilizer octahedron. A well-known single-qubit state is the T-state defined by

$$|T\rangle\langle T| = \frac{1}{2}\left(I_2 + \frac{1}{\sqrt{3}}(X+Y+Z)\right) \tag{1}$$

where I_2 denotes the identity and X, Y, and Z are the Pauli matrices. This state has the maximal single-qubit magic for the relative entropy of magic. On the Bloch sphere, there are in total eight states attaining this maximal magic, called T-like states, obtained by all sign combinations in front of X, Y, and Z, i.e.,

$$\rho_{T-\text{like}} = \frac{1}{2}\left(I_2 + \frac{1}{\sqrt{3}}(\pm X \pm Y \pm Z)\right). \tag{2}$$

Another important single-qubit state is the H-state, defined by

$$|H\rangle\langle H| = \frac{1}{2}\left(I_2 + \frac{1}{\sqrt{2}}(X+Y)\right). \tag{3}$$

This state is used for implementing the T-gate via magic-state injection [4]. Similar to the T-state, there

are twelve states with the same magic as the H-state, called H-like states. They are obtained by all unordered pairs of distinct Pauli matrices from X, Y, Z and all sign combinations in front of the chosen Paulis. In particular, we show that the relative entropy of magic decreases in a spherically symmetric manner with increasing distance from the T-like states.

We also analyze multi-qubit states, in particular, the additivity of the relative entropy of magic. The conditions under which the relative entropy is additive on multiple copies of a state were studied in Ref. [16]. For tensor products of single-qubit states, additivity holds if all but one states belong to a symmetry axis of the stabilizer octahedron, i.e., the magic state and its optimal stabilizer commute. Analogous sufficient conditions are known for tensor products of two- and three-qubit states [17]. Nevertheless, explicit counterexamples demonstrate that the relative entropy of magic is not additive in general [17].

The precise structure of nonadditivity, however, remains incompletely understood, and only isolated examples are known.

We identify a family of states for which additivity must fail and analytically show that the relative entropy of magic is not additive for these states. This establishes an infinite class of nonadditivity examples and reveals an underlying mechanism for the failure of additivity, rather than isolated counterexamples as previously known. We also provide a brief numerical analysis showing that the relative entropy of magic of the state $|\psi\rangle = (|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle)/2$, potentially the state with the maximal magic for the Rényi stabilizer entropy for two qubits [11], is not maximal, but smaller than the relative entropy of magic of two copies of the T states.

This paper is organized as follows. In Section II, we introduce the definitions needed for the rest of the paper. Section III presents our main results: for single qubits, we focus on the distribution of magic states and their closest stabilizer states (Sec. III A), then for multiple qubits, we prove nonadditivity for a particular class of n-qubit states and emphasize the potential importance of the class of magic states that commute with their respective stabilizer states (Sec. (III B). We discuss our results in Section IV.

II. METHODS AND DEFINITIONS

In the resource theory of magic, the set of free states is given by the convex hull of the pure stabilizer states. The corresponding free operations are Clifford unitaries. The set of pure stabilizer states of n qubits is defined as

$$\mathcal{S} := \left\{ U\big(\,|0\rangle\langle 0|\,\big)^{\otimes n} U^\dagger \;:\; U \in \mathcal{C}_n \right\}, \tag{4}$$

where $\mathcal{C}_n$ is the Clifford group on n qubits.

Definition II.1. *The set of stabilizer states of n qubits is the convex hull of the pure stabilizer states*

$$\mathcal{F}(\mathcal{H}^{\otimes n}) := \big\{\sigma \in \mathcal{D}(\mathcal{H}^{\otimes n}) : \sigma = \sum_j p_j S_j \;\; \textit{with} \tag{5}$$

$$0 \le p_j \le 1,\, \sum_j p_j = 1,\, S_j \in \mathcal{S}\;\forall\, j\big\}, \tag{6}$$

where $\mathcal{D}(\mathcal{H}^{\otimes n})$ denotes the set of density matrices. The remaining states $\mathcal{D}(\mathcal{H}^{\otimes n}) \setminus \mathcal{F}(\mathcal{H}^{\otimes n})$ are called magic states.

A magic measure is a function that does not increase under free operations and vanishes for free states. In this work, we focus on the relative entropy of magic, which quantifies the distinguishability between a magic state and stabilizer states.

Definition II.2. *For a state $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$, the relative entropy of magic is defined by*

$$\mathcal{R}_{rel}(\rho) = \inf_{\tilde\sigma \in \mathcal{F}(\mathcal{H}^{\otimes n})} S(\rho\|\tilde\sigma)\,, \tag{7}$$

where $S(\rho\|\tilde\sigma) = \mathrm{Tr}(\rho\log_2\rho) - \mathrm{Tr}(\rho\log_2\tilde\sigma)$ is the relative entropy for $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\tilde\sigma)$ and $S(\rho\|\tilde\sigma) = \infty$ otherwise.

We denote the optimal stabilizer state that achieves the minimum in the definition of the relative entropy of magic by σ, i.e., $\sigma = \mathrm{argmin}_{\tilde\sigma\in\mathcal{F}(\mathcal{H}^{\otimes n})} S(\rho\|\tilde\sigma)$.

To describe all magic states in terms of their closest stabilizer state σ, we use the following characterization derived in [13] and [15] for compact convex free sets. Let σ be a full-rank stabilizer state that lies on the boundary of the stabilizer polytope. Such boundary points admit at least one operator defining a supporting hyperplane ϕ that satisfies $\mathrm{Tr}(\phi^2) = 1$ and $\mathrm{Tr}(\phi\sigma') \ge \mathrm{Tr}(\phi\sigma) = 0$ for all $\sigma' \in \mathcal{F}(\mathcal{H}^{\otimes n})$. It has been shown in [13] and generalized in [15] that given such σ on the boundary of the set of free states $\partial\mathcal{F}(\mathcal{H}^{\otimes n})$ and an operator defining a supporting hyperplane ϕ, any resource state whose closest free state is σ has the following form:

$$\rho = \rho(\sigma,\phi,t) \coloneqq \sigma - t\,\phi \odot L(\sigma), \tag{8}$$

where $\odot$ denotes the entrywise product between two matrices, also called the Hadamard product. For a diagonal matrix $\sigma = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)$ with $\lambda_i \neq 0$ for all $i = 1,\ldots,n$, the matrix $L(\sigma)$ is the entrywise inverse of the divided differences of the matrix logarithm and is given by $L(\sigma)$ so that

$$[L(\sigma)]_{kl} \coloneqq \begin{cases} \lambda_k\,, & \lambda_k = \lambda_l \\ \frac{\lambda_k - \lambda_l}{\ln(\lambda_k) - \ln(\lambda_l)}\,, & \lambda_k \neq \lambda_l \end{cases}. \tag{9}$$

The parameter $t \in [0, t_{\max}]$ increases the "distance" from σ until positivity is lost, and $t_{\max}$ is the largest value for which $\rho(\sigma,\phi,t)$ remains a valid quantum state. Note that, since the Hadamard product is basis dependent, Eq. (8) is defined in the eigenbasis of the stabilizer state σ.

III. RESULTS

In the following, we apply the results from [13] to the resource theory of magic. First, we study the single-qubit case in the Bloch vector representation and we visualize and analyze the distribution of the magic states and their closest stabilizer states. Then we move on to multiple qubits and discuss the nonadditivity and the extremal magic states with respect to the relative entropy.

A. Single qubits

For single qubits, it is convenient to use the Bloch representation. Then the set of pure stabilizer states $\mathcal{S}$ forms a finite set of the six eigenstates of the Pauli matrices. Their Bloch vectors are

$$|+\rangle : \mathbf{s}_1 = (1,0,0), \qquad |-\rangle : \mathbf{s}_4 = (-1,0,0), \tag{10}$$
$$|+i\rangle : \mathbf{s}_2 = (0,1,0), \qquad |-i\rangle : \mathbf{s}_5 = (0,-1,0), \tag{11}$$
$$|0\rangle : \mathbf{s}_3 = (0,0,1), \qquad |1\rangle : \mathbf{s}_6 = (0,0,-1). \tag{12}$$

The set of the stabilizer states $\mathcal{F}(\mathcal{H})$ is the convex hull of these pure stabilizer states and forms an octahedron within the Bloch ball, see Fig. 1.
Consider a full-rank free state $\sigma \in \partial\mathcal{F}(\mathcal{H})$ represented by

$$\sigma = \frac{1}{2}\left(I_2 + \mathbf{x}_\sigma \cdot \boldsymbol{\sigma}\right), \tag{13}$$

where I_2 denotes the identity in two dimensions, $\mathbf{x}_\sigma$ is the Bloch vector with length $r_\sigma = |\mathbf{x}_\sigma|$, and $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ with the Pauli matrices $\sigma_1 = X$, $\sigma_2 = Y$, and $\sigma_3 = Z$.
The supporting hyperplane can be represented by the following Hermitian 2×2 matrix

$$\phi = \frac{1}{2}\left(\varphi_0 I_2 + \mathbf{x}_\phi \cdot \boldsymbol{\sigma}\right), \quad \mathbf{x}_\phi = (\varphi_1, \varphi_2, \varphi_3) \tag{14}$$

with $r_\phi \coloneqq |\mathbf{x}_\phi|$. It must satisfy the condition

$$0 = \mathrm{Tr}\left(\phi\sigma\right), \tag{15}$$

which is equivalent to $\varphi_0 = -\mathbf{x}_\sigma^T \mathbf{x}_\phi$. Choosing any boundary state σ with $\mathrm{Tr}(\phi\sigma) = 0$, we can rewrite Eq. (8) in the following Bloch vector form

$$\mathbf{x}_\rho = \mathbf{x}_\sigma - \frac{t}{2r_\sigma^2}\left[(r_\sigma^2 - 1)\varphi_0\, \mathbf{x}_\sigma + 2g_{r_\sigma}\left(\varphi_0 \mathbf{x}_\sigma + r_\sigma^2 \mathbf{x}_\phi\right)\right] \tag{16}$$

with $g_{r_\sigma} \coloneqq \frac{r_\sigma}{\ln\left(\frac{1+r_\sigma}{1-r_\sigma}\right)}$. See Appendix A for more details on the expression. The factor $t \in [0, t_{\max}]$ is a free parameter, whose maximal value $t_{\max}$ is reached for $r_\rho = 1$. Note that this Bloch vector expression holds for all resource theories with a compact convex set of free states, see [15]. If the Bloch vector of the stabilizer state and the Bloch vector of its supporting hyperplane are parallel, the stabilizer state is a depolarized version of the magic states it is closest to, i.e., $\sigma = m\, I_2 + (1-m)\rho$ with $m \in (0,1)$, equivalently $[\sigma, \phi] = 0 = [\rho, \sigma]$. This can only be fulfilled for the states at the center of the facets and edges.

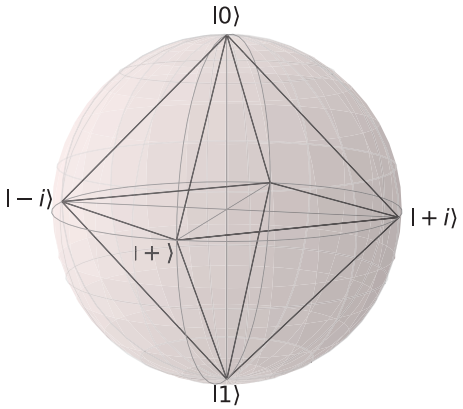


FIG. 1: Bloch ball with stabilizer octahedron. The magic states are outside the stabilizer octahedron.

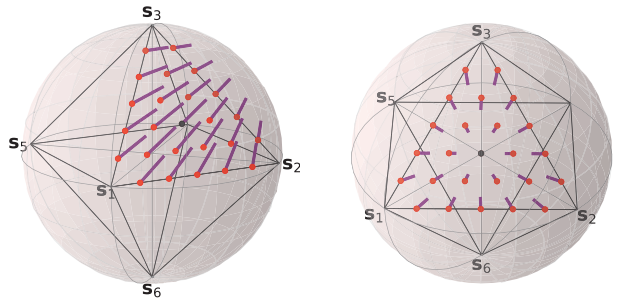
A state on the surface of this octahedron can lie either at a vertex, or on an edge, or on a facet. A vertex cannot be the closest stabilizer state σ for any magic state ρ, as the vertices of the octahedron correspond to pure states and the relative entropy $S(\rho\|\sigma)$ becomes infinite in such cases. If we consider states on the edges, a continuous set of supporting hyperplanes exists. The supporting hyperplane is unique only for states lying in the relative interior of the facets.
Because the vertices cannot correspond to the closest stabilizer states, they can be excluded from our consideration. We begin by studying the facets since they have a unique supporting hyperplane, and then move on to the edges. It is sufficient to restrict our attention to a single facet and edge since the octahedron is symmetric, and the Clifford operations, the free operations, correspond to rotations of a state in the Bloch ball.

1. States on a facet

Consider the facet given by the convex hull of the stabilizer states with Bloch vector $\mathbf{s}_i\,, i \in \{1,2,3\}$. Any point in this triangle can be expressed as

$$\mathbf{x}_{\sigma'} = \sum_{i=1}^{3} \alpha_i \mathbf{s}_i = (\alpha_1, \alpha_2, \alpha_3) \;\text{ with }\; \sum_{i=1}^{3} \alpha_i = 1\,,\; \alpha_i \geq 0\,. \tag{17}$$

The vector $\mathbf{x}_\phi$ of the supporting hyperplane, which satisfies $0 = \mathrm{Tr}\left(\phi\sigma\right) \leq \mathrm{Tr}\left(\phi\sigma'\right)$ for all stabilizer states σ', is given by $\mathbf{x}_\phi = -\frac{1}{\sqrt{2}}(1,1,1)$ due to $\mathrm{Tr}\left(\phi^2\right) = 1$. For the



(a) Side view (b) Top view

FIG. 2: The purple lines are $\mathbf{x}_\rho(\sigma,t)$ for $0<t\leq t_{\max}$ for some σ in the triangle spanned by $\mathbf{s}_1$, $\mathbf{s}_2$ and $\mathbf{s}_3$. The red circles represent the closest stabilizer states to the states on the purple line that they intersect. The stabilizer state at the center of the triangle is black. The intersection of the Bloch sphere and the purple line starting at the black dot is the T-state.

Bloch vectors of the magic states, it follows

$$x_{\rho,i}(\mathbf{x}_\sigma,t)=x_{\sigma,i}-\frac{t}{\sqrt{8}\,r_\sigma^2}\left[(r_\sigma^2-1)x_{\sigma,i}+2g_{r_\sigma}\left(x_{\sigma,i}-r_\sigma^2\right)\right] \tag{18}$$

with $i\in\{1,2,3\}$. A fixed stabilizer state in the triangle is closest to only one magic state for each value of t since the supporting hyperplane is unique. If a stabilizer state satisfies $x_{\sigma,i}=r_\sigma^2$ for all three coordinates, then the last term in Eq. (18) vanishes, i.e., $[\rho,\sigma]=0$. This is only satisfied for the state at the center of the triangle, which is closest to the T-state

$$|T\rangle\langle T|=\frac{1}{2}\left(I_2+\frac{1}{\sqrt{3}}\left(\sigma_1+\sigma_2+\sigma_3\right)\right) \tag{19}$$

and its depolarized versions, see [17].
In Fig. 2, magic states and their closest stabilizer states on the triangle spanned by $\mathbf{s}_1$, $\mathbf{s}_2$ and $\mathbf{s}_3$ are shown from different viewpoints. The purple lines represent the magic states, and the red circles with which they intersect denote their closest stabilizer states. The magic states are described by $\mathbf{x}_\rho(t)$ for $0<t\leq t_{\max}$ from Eq. (18).

Observe in Fig. 2 that the further the stabilizer states are from the center of the triangle, the more the connecting lines deviate from the normal vector of the triangle. Fig. 2b shows the figure along the normal vector of the triangle. For the stabilizer state at the center of the triangle, the corresponding magic states are not visible as they are normal to the triangle. For all the other stabilizer states of this facet, the lines of magic states are tilted symmetrically towards the center. In Fig. 2b, we can see that the vectors $\mathbf{x}_\rho(\sigma,t)$ are tilted in the direction of the T-state. The further the stabilizer states are from the T-state, the steeper the slope. The figure also shows that the distribution of the magic states of the closest stabilizer states in the triangle has a rotational symmetry. With the scalar product of a vector representing a purple line, $\mathbf{x}_\mathrm{d}=\mathbf{x}_\rho(\sigma,t_{\max})-\mathbf{x}_\sigma$ and the normal vector $\mathbf{n}=\frac{1}{\sqrt{3}}(1,1,1)$, the inclination angle is given by

$$\alpha_{d,n}(r_\sigma)=\arccos\left(\frac{1}{\sqrt{3}r_\sigma}\frac{(1-r_\sigma^2)(1-2g_{r_\sigma})}{\sqrt{(1-r_\sigma^2)^2+4g_{r_\sigma}^2\,(3r_\sigma^2-1)}}\right).$$

This expression shows that the angle depends solely on the Bloch vector length of the stabilizer state r_σ. Given the inclination angle $\alpha_{d,n}$ we can derive an analytic expression to find the stabilizer state closest to a given magic state such that we can calculate the amount of magic that a given state holds. The results can be found in Appendix B.

2. *States on an edge*

As previously noted, the supporting hyperplanes of the edges are not unique. For a given stabilizer state σ, different hyperplanes that result in different magic states being closest to them exist. Consider the edge connecting the vertices $\mathbf{s}_1$ and $\mathbf{s}_3$. Each state on this edge can be expressed by

$$\mathbf{s}'=\alpha_1\mathbf{s}_1+\alpha_3\mathbf{s}_3=(\alpha_1,0,\alpha_3)\ \text{ with }\alpha_1+\alpha_3=1,\ \alpha_i\geq 0. \tag{20}$$

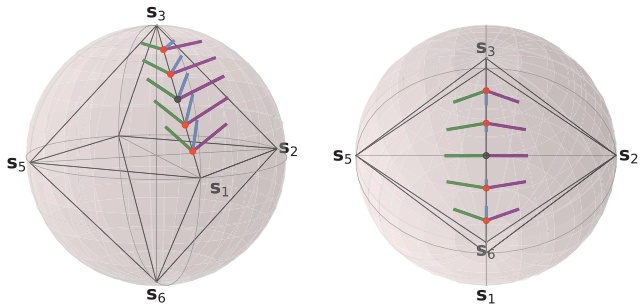
For a state σ on this edge, the supporting hyperplanes are represented by the Bloch vector $\mathbf{x}_\phi=(-b,c,-b)$ with $b=\sqrt{(2-c^2)/3}$ and $-b\leq c\leq b$. With Eq. (16) it follows that the corresponding Bloch vectors of the magic states are

$$x_{\rho,i}(\mathbf{x}_\sigma,t,c)=x_{\sigma,i}-\sqrt{\frac{2-c^2}{12}}\frac{t}{r_\sigma^2}\left[(r_\sigma^2-1)\,x_{\sigma,i}+2g_{r_\sigma}\left(x_{\sigma,i}-r_\sigma^2\right)\right]\quad\text{for } i\in\{1,3\}, \tag{21}$$

$$x_{\rho,2}(\sigma,t,c)=-\,c\,t\,g_{r_\sigma}. \tag{22}$$

This Bloch vector expression has, compared to the one of the facet, the additional variable c because the supporting hyperplane is not unique. Due to $x_{\sigma,2}=0$, the expression for $x_{\rho,2}$ simplifies. The value of c determines how far and in which direction the magic states are tilted to the side for a given stabilizer state.

Consequently, compared to the previous facet, any stabilizer state on the edge is the closest free state to a one-parameter family of magic states. Since Eq. (21) is identical for $i=1,3$, it is sufficient to consider only one half of the edge, as the values for the other half follow by symmetry. Let us distinguish between two cases: $c=0$ and $c\neq 0$.



(a) Side view (b) Top view

FIG. 3: Magic states are represented by the lines starting at their closest stabilizer state (red circles) on the edge with vertices $\mathbf{s}_1$ and $\mathbf{s}_3$. The lines are the magic states for different values of c. For $c = 1/\sqrt{2}$ ($c = 1/\sqrt{8}$), the lines are green (purple), and for $c = 0$, the lines are blue. The black dot is the stabilizer state at the center of the edge, which is closest to the H-like state at the end of the blue line. The magic states are described by Eqs. (21), (22).

Case 1: $c = 0$. Then $x_{\rho,2} = 0$ for all stabilizer states σ on the edge $(\mathbf{s}_1, \mathbf{s}_3)$, so every associated magic state lies in the x_1–x_3 plane, describing the circular arc above the edge connecting $\mathbf{s}_1$ and $\mathbf{s}_3$ (see Fig. 3a). At the edge midpoint $(\alpha_1, \alpha_3) = (\frac{1}{2}, \frac{1}{2})$, we have $x_{\sigma,1} = x_{\sigma,3} = r_\sigma^2$, such that the trajectory is orthogonal to the edge and corresponds to the H-like magic state

$$|H'\rangle\langle H'| = \tfrac{1}{2}\Big(I_2 + \tfrac{1}{\sqrt{2}}(\sigma_1 + \sigma_3)\Big)$$

on the Bloch sphere for $t_{\max}$, see [17]. This state is at the midpoint of the circular arc between $\mathbf{s}_1$ and $\mathbf{s}_3$.

Case 2: $c \neq 0$. The supporting hyperplane tilts into the x_2-direction, generating a continuum of lines (21) parameterized by c (see Fig. 3b). The sign of c selects which adjacent facet region the line bends toward; increasing $|c|$ produces a stronger tilt away from the edge normal. For the extremal values $|c| = 1/\sqrt{2}$, the states meet the facet states.

3. *Values of the relative entropy of magic*

With the expression for the magic states closest to a stabilizer state, we can now calculate the relative entropy of magic rather than performing a numerical search. Inserting the magic state Bloch vector expression, Eq. (16), in the Bloch vector expression for the relative entropy in [18] yields

$$\mathcal{R}_{\mathrm{rel}}(\rho(\sigma,\phi,t)) = \begin{cases} 1 - \frac{1}{2}\left[\log_2(1-r_\sigma^2) + \left[r_\sigma - \frac{t_{\max}\varphi_0}{2r_\sigma}(r_\sigma^2-1)\right]\log_2\left(\frac{1+r_\sigma}{1-r_\sigma}\right)\right] & \text{if } r_\rho = 1, \\ \frac{1}{2}\left[r_\rho \log_2\left(\frac{1+r_\rho}{1-r_\rho}\right) + \log_2\left(\frac{1-r_\rho^2}{1-r_\sigma^2}\right) - \left[r_\sigma - \frac{t\varphi_0}{2r_\sigma}(r_\sigma^2-1)\right]\log_2\left(\frac{1+r_\sigma}{1-r_\sigma}\right)\right] & \text{else.} \end{cases} \tag{23}$$

Calculating the relative entropy for the pure states in the spherical triangle with the vertices $\mathbf{s}_1$, $\mathbf{s}_2$ and $\mathbf{s}_3$ leads to the distribution of the values of the relative entropy in Fig. 4. This includes the states on the edges of the triangle, for which the hyperplanes with $-b \leq c \leq 0$ are considered to describe the full spherical triangle.

We see that the closer a state is to the vertices of the octahedron, the lower the value of the relative entropy of magic. The T-state reaches the maximal relative entropy of magic for a single qubit. Among the magic states whose closest stabilizer state is on the edge, the H-state achieves the largest amount of magic. More generally, for each face of the single-qubit stabilizer polytope, the relative entropy of magic is maximized with respect to the center of that face. Comparing Fig. 4 with Fig. 2b shows that the magic states with the largest values of the relative entropy have their closest stabilizer state on a facet of the octahedron and not on the edges.

B. Nonadditivity of the relative entropy of magic

For tensor products of magic states, commutation between the magic states of the subsystems and their closest stabilizer states has been identified as a sufficient condition for additivity of the relative entropy of magic [17]. For single-qubit states, the authors showed that if all or all but one magic state commute with their closest stabilizer states, the relative entropy of the tensor product of these states is additive. However, it was still unclear if the relative entropy of magic is additive for the remaining states, except for explicit examples of nonadditivity. To close this gap, we prove that the relative entropy of magic is not additive for states that do not belong to the class described above. Requiring that a magic state ρ and its closest stabilizer state σ commute is equivalent to the condition that a stabilizer state and the corresponding supporting hyperplane ϕ commute, which we

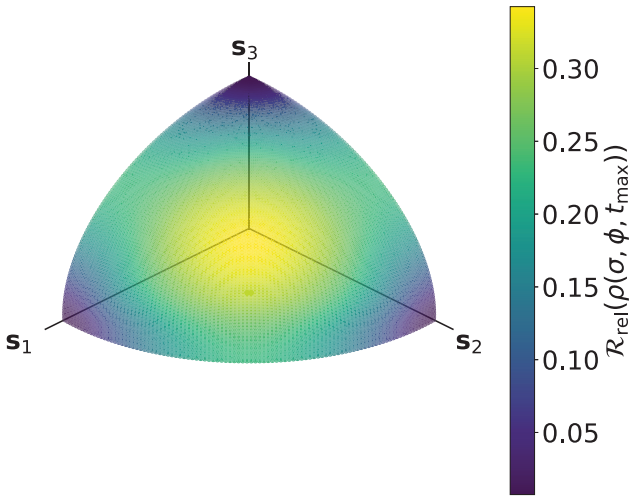


FIG. 4: Relative entropy of magic $\mathcal{R}_{\mathrm{rel}}(\rho(\sigma,\phi,t_{\mathrm{max}}))$ determined by Eq. (23) for stabilizer states in the triangle with the vertices $\mathbf{s}_1$, $\mathbf{s}_2$ and $\mathbf{s}_3$ including the hyperplanes with $-b \leq c \leq 0$ for the states on the edges.

can see using Eq. (8):

$$0 = [\rho,\sigma] = -t[\phi \odot L(\sigma),\sigma] = -t[\phi,\sigma] \odot L(\sigma) \tag{24}$$
$$\Rightarrow [\phi,\sigma] = 0\,. \tag{25}$$

Here, σ is represented in its eigenbasis. We used the property of the Hadamard product that for a diagonal matrix D and the matrices A and B of the same size, it holds $(A \odot B)\,D = (A\,D) \odot B$ and $D\,(A \odot B) = (D\,A) \odot B$. We show that the relative entropy of magic is not additive for a large class of magic states.

Theorem III.1. *Let $\rho^{(i)} \in \mathcal{D}(\mathcal{H}_i) \setminus \mathcal{F}(\mathcal{H}_i)$ with $i = 1,\ldots,n$ be single-qubit magic states and $\sigma^{(i)} \in \mathcal{F}(\mathcal{H}_i)$ their closest stabilizer states. The relative entropy of magic of their tensor product $\rho = \bigotimes_{i=1}^{n} \rho^{(i)}$ cannot be additive if both of the following conditions hold*

1. *$\left[\rho^{(i)},\sigma^{(i)}\right] \neq 0$ for at least two $i \in \{1\ldots,n\}$,*
2. *at least one $\sigma^{(i)}$ with $\left[\rho^{(i)},\sigma^{(i)}\right] \neq 0$ lies in the relative interior of a facet of the stabilizer octahedron.*

Here, we briefly outline the idea of the proof by contradiction, see Appendix C for details.
Let $\sigma^{(i)} \in \mathcal{F}(\mathcal{H}_i)$ with $i = 1,\ldots,n$ be single-qubit stabilizer states closest to the magic states $\rho^{(i)} \in \mathcal{D}(\mathcal{H}_i) \setminus \mathcal{F}(\mathcal{H}_i)$ satisfying the conditions in the theorem.
We assume that the relative entropy of magic is additive for $\rho = \bigotimes_{i=1}^{n} \rho^{(i)}$. Then, $\sigma = \bigotimes_{i=1}^{n} \sigma^{(i)}$ is a closest stabilizer state to which Eq. (8) applies, yielding an explicit expression that the supporting hyperplane of the n-qubit stabilizer polytope must satisfy. For states in the class, we identify that the stabilizer states do not define a supporting hyperplane. Consequently, the relative entropy is not additive for the magic state ρ.

For two-qubit states where both single-qubit stabilizer states are on the edges of the stabilizer octahedron and do not commute with their respective magic states, we performed a numerical search under the assumption of additivity and did not find valid supporting hyperplanes. Hence, we conjecture that the relative entropy of magic is also not additive for these states.
When we determine the values of the relative entropy of magic for two-qubit states, we cannot find larger values than for two copies of the T-state. The T-state has the largest relative entropy of magic for a single qubit. Since the relative entropy of magic is additive for this state, two copies of the T-state have the largest relative entropy of magic for states whose closest stabilizer states lie in faces with only separable states at the face-defining vertices. In [11], numerical optimizations suggest that the state $|\psi\rangle = (|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle)/2$ is one of the states that potentially reach the maximal magic for the stabilizer Rényi entropy. However, the relative entropy of magic of this state is not maximal, but only close to the value of the relative entropy of magic of two copies of the T-state

$$\mathcal{R}_{\mathrm{rel}}(|\psi\rangle\langle\psi|) \approx 0.678 \;<\; \mathcal{R}_{\mathrm{rel}}\left(|T\rangle\langle T|^{\otimes 2}\right) \approx 0.685\,. \tag{26}$$

The state $|\psi\rangle$ also commutes with its closest stabilizer state [17], which lies at the center of a face, such as the stabilizer state closest to two copies of the T-state. Since the relative entropy of magic is additive for the T-state [17], i.e.,

$$\mathcal{R}_{\mathrm{rel}}\left(|T\rangle\langle T|^{\otimes n}\right) = n\,\mathcal{R}_{\mathrm{rel}}\left(|T\rangle\langle T|\right)\,, \tag{27}$$

we conjecture the relative entropy of magic of n qubits is maximal for this type of states.

IV. CONCLUSION AND OUTLOOK

This work addresses the problem of finding analytical expressions for the relative entropy of magic. By applying the results of [13] to the resource theory of magic, we analyzed the distribution of magic states and their closest stabilizer state in the single-qubit case. We found that they are symmetrically aligned around the state closest to the centers of the boundary elements (T-like states, H-like states, and their depolarized versions).
The relative entropy of magic of tensor products of single-qubit states is additive if all or all but one single-qubit magic states commute with their closest stabilizer state [17]. For almost all other cases, we have proved that the relative entropy of magic is nonadditive. For the remaining states, which do not satisfy the condition, we conjecture that the relative entropy of magic is also nonadditive due to strong numerical evidence. We further conjecture that, in general, the relative entropy of magic is additive only for states that satisfy the commutativity condition.

For two qubits, the state $|\psi\rangle$ with the possibly largest amount of magic for the stabilizer Rényi entropy [11] does not have the maximal relative entropy of magic, as two copies of the T-state have a larger relative entropy of magic.

It is an open question whether the amount of magic held by commuting pairs of states, particularly for closest stabilizer states at the center of faces, correlates positively with a large relative entropy of magic.

ACKNOWLEDGMENTS

We thank Nikolai Wyderka for helpful discussions.

This work has been supported by the Federal Ministry of Research, Technology and Space (BMFTR Projects QR.N, Grant No. 16KIS2202 and QSolid, Grant No. 13N16163). We also acknowledge financial support by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769.

[1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing **26**, 1484 (1997), https://doi.org/10.1137/S0097539795293172.

[2] L. K. Grover, A fast quantum mechanical algorithm for database search (1996), arXiv:quant-ph/9605043 [quant-ph].

[3] D. Gottesman, The heisenberg representation of quantum computers (1998), arXiv:quant-ph/9807006 [quant-ph].

[4] S. Bravyi and A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).

[5] M. Howard and E. Campbell, Application of a resource theory for magic states to fault-tolerant quantum computing, Phys. Rev. Lett. **118** (2017), 090501.

[6] M. Heinrich and D. Gross, Robustness of Magic and Symmetries of the Stabiliser Polytope, Quantum **3**, 132 (2019).

[7] H. Hamaguchi, K. Hamada, and N. Yoshioka, Handbook for Quantifying Robustness of Magic, Quantum **8**, 1461 (2024).

[8] L. Leone, S. F. E. Oliviero, and A. Hamma, Stabilizer rényi entropy, Phys. Rev. Lett. **128**, 050402 (2022).

[9] L. Leone and L. Bittel, Stabilizer entropies are monotones for magic-state resource theory, Phys. Rev. A **110**, L040403 (2024).

[10] L. Bittel and L. Leone, Operational interpretation of the stabilizer entropy (2025), arXiv:2507.22883 [quant-ph].

[11] Q. Liu, I. Low, and Z. Yin, Maximal magic for two-qubit states (2025), arXiv:2502.17550 [quant-ph].

[12] V. Veitch, S. A. Hamed Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New Journal of Physics **16** (2014), 013009.

[13] S. Friedland and G. Gour, An explicit expression for the relative entropy of entanglement in all dimensions, Journal of Mathematical Physics **52** (2011), 052201.

[14] Y. Huang, Computing quantum discord is np-complete, New journal of physics **16**, 033027 (2014).

[15] M. W. Girard, G. Gour, and S. Friedland, On convex optimization problems in quantum information theory, Journal of Physics A: Mathematical and Theoretical **47** (2014), 505302.

[16] R. Rubboli and M. Tomamichel, New additivity properties of the relative entropy of entanglement and its generalizations, Communications in Mathematical Physics (2024).

[17] R. Rubboli, R. Takagi, and M. Tomamichel, Mixed-state additivity properties of magic monotones based on quantum relative entropies for single-qubit states and beyond, Quantum **8**, 1492 (2024).

[18] J. Cortese, Relative entropy and single qubit holevo-schumacher-westmoreland channel capacity (2002), arXiv:quant-ph/0207128 [quant-ph].

Appendix A: Determining the Bloch vector expression

To find the Bloch vector expression in Eq. (16) for a general resource theory with a compact convex set of free states, we start by using

$$\rho = \rho(\sigma, \phi, t) \coloneqq \sigma - t\,\phi \odot L(\sigma), \tag{A1}$$

derived in [13]. This expression holds in the eigenbasis of σ, $\sigma = \mathrm{diag}(\lambda_1, \lambda_2)$.
Consider a full-rank stabilizer state on the boundary of the free states $\sigma \in \partial\mathcal{F}(\mathcal{H})$

$$\sigma = \frac{1}{2}\left(I_2 + \mathbf{x}_\sigma \cdot \boldsymbol{\sigma}\right). \tag{A2}$$

In the Pauli basis, the supporting hyperplane can be represented by

$$\phi_P = \frac{1}{2}\left(\varphi_0 I_2 + \mathbf{x}_\phi \cdot \boldsymbol{\sigma}\right), \quad \mathbf{x}_\phi = (\varphi_1, \varphi_2, \varphi_3)$$

with $r_\phi \coloneqq |\mathbf{x}_\phi|$.
Since Eq. (8) is basis dependent, using the transformation matrices $U, U^\dagger$ with $\mathrm{diag}(\lambda_1, \lambda_2) = U^\dagger \sigma U$, the expression of the supporting hyperplane in the diagonal basis of σ, ϕ_σ, yields

$$\phi_\sigma = U^\dagger \phi_P U = \frac{1}{2r_\sigma}\begin{pmatrix} \phi_0(r_\sigma + 1) & p_- \\ p_+ & \phi_0(r_\sigma - 1)\end{pmatrix}, \text{ where} \tag{A3}$$

$$p_- \coloneqq \frac{-(\phi_3 r_\sigma^2 + \phi_0 x_3) - i r_\sigma(\phi_1 x_2 - \phi_2 x_1)}{\sqrt{r^2 - x_3^2}}, \tag{A4}$$

$$p_+ \coloneqq \frac{-(\phi_3 r_\sigma^2 + \phi_0 x_3) + i r_\sigma(\phi_1 x_2 - \phi_2 x_1)}{\sqrt{r^2 - x_3^2}}. \tag{A5}$$

For a single qubit, the elementwise inverse matrix of the divided differences is

$$S(\sigma) = \begin{pmatrix} \frac{1-r_\sigma}{2} & g_{r_\sigma} \\ g_{r_\sigma} & \frac{1+r_\sigma}{2}\end{pmatrix} \quad \text{with } g_{r_\sigma} \coloneqq \frac{r_\sigma}{\log\left(\frac{1+r_\sigma}{1-r_\sigma}\right)}.$$

To determine the Bloch vector of ρ, an additional basis change is necessary. It holds

$$M = U(\phi_\sigma \odot S(\sigma))U^\dagger = \frac{1}{4r_\sigma^2}\begin{pmatrix} m_{11} & m_{12} \\ m_{12}^* & -m_{11}\end{pmatrix}$$

with

$$\begin{aligned} m_{11} =& \phi_0(r_\sigma^2 - 1)x_3 + 2g_{r_\sigma}(r_\sigma^2\phi_3 + \phi_0 x_3), \\ m_{12} =& \phi_0(r_\sigma^2 - 1)x_1 + 2g_{r_\sigma}(r_\sigma^2\phi_1 + \phi_0 x_1) \\ & - i\left(\phi_0(r_\sigma^2 - 1)x_2 + 2g_{r_\sigma}(r_\sigma^2\phi_3 + \phi_0 x_2)\right). \end{aligned}$$

The Bloch vector of the state $\rho = \rho(\sigma, \phi, t)$ is

$$\mathbf{x}_\rho = \mathbf{x}_\sigma - \frac{t}{2r_\sigma^2}\left[(r_\sigma^2 - 1)\varphi_0\,\mathbf{x}_\sigma + 2g_{r_\sigma}\left(\varphi_0 \mathbf{x}_\sigma + r_\sigma^2 \mathbf{x}_\phi\right)\right] \tag{A6}$$

with $0 < t \leq t_{\max}$. With $r_\rho = |\mathbf{x}_\rho| \leq 1$, the parameter t yields

$$t = \frac{r_\sigma^2 - 1}{h}\left(\phi_0 - \sqrt{\phi_0^2 - h\frac{r_\sigma^2 - r_\rho^2}{r_\sigma^2(r_\sigma^2 - 1)^2}}\right) \tag{A7}$$

with $h = (r_\sigma^2 - 1)^2\phi_0^2 + 4g_{r_\sigma}^2\left(r_\sigma^2 r_\phi^2 - \phi_0^2\right)$.
For the maximal value $t_{\max}$, insert $r_\rho = 1$ in Eq. (A7).

Appendix B: Determining the stabilizer state closest to a given magic state

In Section III A, we used the results from [13] to find for a given stabilizer state the magic states it is closest to. In general, the inverse problem of finding the closest stabilizer state to a magic state is more useful since one can directly determine the amount of magic of a given magic state. If we orthogonally project a magic state onto the triangle, its projection, its closest stabilizer state, and the triangle's center all lie on the same straight line, see 2b. With this geometrical property, we find the following analytic Bloch vector expression for a stabilizer state on a facet, depending on the angle $\alpha_{d,n}$ between the normal vector and the magic state

$$\mathbf{x}_\sigma(\mathbf{x}_\rho, \alpha_{d,n}) = \mathbf{x}_C + b(\mathbf{x}_\rho, \alpha_{d,n})\left(\mathbf{x}_\rho - \frac{\sum_{i=1}^3 x_{\rho,i}}{\sqrt{3}}\,\mathbf{n}\right) \tag{B1}$$

with

$$b(\mathbf{x}_\rho, \alpha_{d,n}) = 1 + \tan(\alpha_{d,n})\sqrt{\frac{(1 - \sum_{i=1}^3 x_{\rho,i})^2}{3 - \left(\sum_{i=1}^3 x_{\rho,i}\right)^2}}. \tag{B2}$$

This expression is exact because it does not involve any approximations. However, since there is no analytic expression for the angle $\alpha_{d,n}$ that solely depends on the magic state, we need a linear regression. This allows us to obtain an approximate Bloch vector for the closest stabilizer state to a pure magic state, where the stabilizer state lies in the triangle. The correlation between the angle of inclination and the distance of the corresponding pure magic states to the T state is shown in Fig. 5. For small distances, the angle depends approximately linearly on the distance.

Appendix C: Proof of the nonadditivity of the relative entropy of magic for a class of n qubit states

In this section, we want to prove that the relative entropy of magic is nonadditive for a specific class of states. Consider an n-qubit magic state $\rho = \bigotimes_{i=1}^n \rho^{(i)}$ with the single qubit magic states $\rho^{(i)} \in \mathcal{D}(\mathcal{H}_i) \setminus \mathcal{F}(\mathcal{H}_i)$. Let

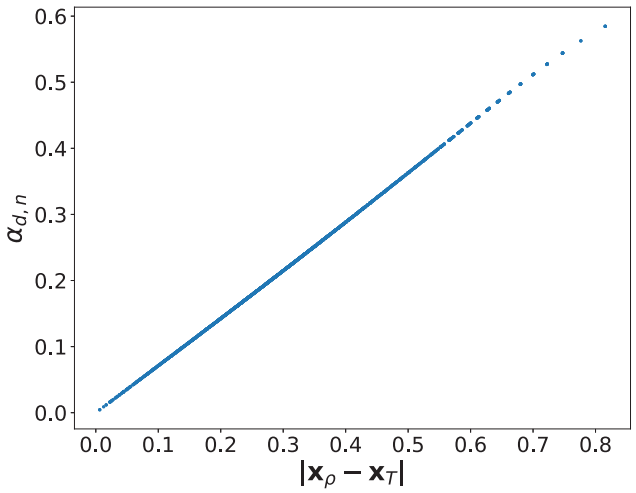


FIG. 5: Angle $\alpha_{d,n}$ between the purple lines of Fig. 2b and the normal vector of the triangle $\mathbf{n} = (1,1,1)/\sqrt{3}$, as a function of the distance between a pure magic state $\mathbf{x}_\rho$ and the T-state $\mathbf{x}_T$.

$\sigma^{(i)} \in \mathcal{F}(\mathcal{H}_i)$ be their closest stabilizer states.
For the proof, we start by assuming that the relative entropy of magic is additive, i.e., $\mathcal{R}(\rho) = \mathcal{R}(\bigotimes_{i=1}^n \rho^{(i)}) = \sum_{i=1}^n \mathcal{R}(\rho^{(i)})$, then we show by contradiction the relative entropy of magic is not additive for states of the class in the theorem.
Due to the additivity of the relative entropy, the relative entropy of magic yields

$$\mathcal{R}\left(\bigotimes_{i=1}^n \rho^{(i)}\right) = \min_{\sigma' \in \mathcal{F}} S\left(\bigotimes_{i=1}^n \rho^{(i)} \,||\, \sigma'\right) \tag{C1}$$

$$= S\left(\bigotimes_{i=1}^n \rho^{(i)} \,||\, \bigotimes_{i=1}^n \sigma^{(i)}\right). \tag{C2}$$

Hence, the stabilizer state $\sigma = \bigotimes_{i=1}^n \sigma^{(i)}$ composed of the closest single qubit stabilizer states is closest to $\rho = \bigotimes_{i=1}^n \rho^{(i)}$ if the relative entropy of magic is additive for ρ.
Consequently, the relative entropy of magic is not additive if σ is not closest to ρ. Since we prove nonadditivity for magic states for which at least two single-qubit magic states and their respective stabilizer states do not commute, and at least one of them lies in the relative interior of a facet of the stabilizer octahedron. W.l.o.g., suppose that $\left[\rho^{(i)}, \sigma^{(i)}\right] \neq 0$ for $i = 1, 2$ and $\sigma^{(1)}$ is in the relative interior of a facet.
With our fixed magic state and stabilizer state, we can use Eq. (8) to get an expression for the supporting hyperplane Φ of the n-qubit stabilizer polytope. If Φ is a supporting hyperplane of $\mathcal{F}(\mathcal{H}^{\otimes n})$, it has to satisfy $\mathrm{Tr}(\Phi\sigma') \geq 0$ for all $\sigma' \in \mathcal{F}(\mathcal{H}^{\otimes n})$. To contradict our initial statement, we identify a stabilizer state $\sigma' \in \mathcal{F}(\mathcal{H}^{\otimes n})$ such that $\mathrm{Tr}(\Phi\sigma') < 0$.
For the proof, we need the following property of the Hadamard product:
For matrices A, B, C and D of the same size, it holds that

$$(A \odot B) \otimes (C \odot D) = (A \otimes C) \odot (B \otimes D)\,. \tag{C3}$$

By applying Eq. (8) and using $\sigma = I \odot L(\sigma)$ and Eq. (C3)

$$\rho(\sigma, \Phi, t) = \bigotimes_{i=1}^n \rho^{(i)}(\sigma^{(i)}, \phi^{(i)} = t_i \tilde{\phi}^{(i)})\,, \tag{C4}$$

we obtain for the supporting hyperplane the expression

$$\Phi = \tilde{\Phi} + \chi \tag{C5}$$

with

$$\tilde{\Phi} = I^{\otimes n} - \bigotimes_{i=1}^n (I^{(i)} - \phi^{(i)})\,, \tag{C6}$$

$$\chi = \left[\bigotimes_{i=1}^n (I^{(i)} - \phi^{(i)})\right] \odot \Delta\,. \tag{C7}$$

The matrix Δ is given by

$$\Delta = J - \bigotimes_{i=1}^n L(\sigma^{(i)}) \oslash L\left(\bigotimes_{i=1}^n \sigma^{(i)}\right), \tag{C8}$$

where J is the all-ones matrix and $\oslash$ is the entrywise division.
To find states $\sigma' \in \mathcal{F}(\mathcal{H}^{\otimes n})$ such that $\mathrm{Tr}(\Phi\sigma') < 0$, we focus on separable states $\sigma' = \bigotimes_{i=1}^n \sigma'^{(i)}$ with $\mathrm{Tr}\left(\phi^{(i)}\sigma'^{(i)}\right) = 0$. Then the first part of the supporting hyperplane vanishes, i.e., $\mathrm{Tr}\left(\tilde{\Phi}\sigma'\right) = 0$.

To determine $\mathrm{Tr}(\chi\sigma')$, we rewrite the matrix Δ in tensor product structure and use the Dirac notation for simplification. We denote by $\{|\mathbf{j}\rangle\}_{\mathbf{j}\in\{0,1\}^n}$ the computational basis of $\mathcal{H}$, where $\mathbf{j} = (j_1, \ldots, j_n)$ with $j_k \in \{0,1\}$ and $|\mathbf{j}\rangle = |j_1\rangle \otimes \cdots \otimes |j_n\rangle$. We choose this basis such that σ is diagonal, i.e., $\sigma\,|\mathbf{j}\rangle = \lambda_{\mathbf{j}}\,|\mathbf{j}\rangle$ for all $|\mathbf{j}\rangle \in \{0,1\}^n$. In the following, we denote by $\bar{\mathbf{j}} = (\bar{j}_1, \ldots, \bar{j}_n)$ the "negation" of $\mathbf{j}$ with $\bar{j}_k = j_k \oplus 1$, where $\oplus$ is the addition modulo two. In the eigenbasis of σ, the matrices $\bigotimes_{i=1}^n L(\sigma^{(i)})$ and $L\left(\bigotimes_{i=1}^n \sigma^{(i)}\right)$ have the matrix elements $L_{\mathbf{j},\mathbf{l}}$ and $\mathcal{L}_{\mathbf{j},\mathbf{l}}$ defined by

$$\bigotimes_{i=1}^n L(\sigma^{(i)}) = \sum_{\mathbf{j},\mathbf{l}} L_{\mathbf{j},\mathbf{l}}\;\; |\mathbf{j}\rangle\langle\mathbf{l}|\,, \tag{C9}$$

$$L\left(\bigotimes_{i=1}^n \sigma^{(i)}\right) = \sum_{\mathbf{j},\mathbf{l}} \mathcal{L}_{\mathbf{j},\mathbf{l}}\;\; |\mathbf{j}\rangle\langle\mathbf{l}|\,. \tag{C10}$$

Using these expressions Δ yields

$$\Delta = \sum_{\mathbf{j},\mathbf{l}} \left(1 - \frac{L_{\mathbf{j},\mathbf{l}}}{\mathcal{L}_{\mathbf{j},\mathbf{l}}}\right)\;\; |\mathbf{j}\rangle\langle\mathbf{l}|\,. \tag{C11}$$

If $\mathbf{j} = \mathbf{l}$ or $j_i = \bar{l}_i$ for a single $i \in \{1, \ldots, n\}$, the entries $L_{\mathbf{j},\mathbf{l}}$, $\mathcal{L}_{\mathbf{j},\mathbf{l}}$ are equal since they are just the eigenvalues of the subsystems or only for a single subsystem the inverse finite difference. These remaining entries, where $\mathbf{j}$ and $\mathbf{l}$ differ in at least two entries, lie on the anti-diagonals of the subsystems or of the whole system. We denote the anti-diagonal matrix of a subsystem $S \subseteq N = \{1, \ldots, n\}$ of size $s = |S| \geq 2$ by $A^{(S)}$.
Then, Δ can be expressed by a sum of these anti-diagonal matrices $A^{(S)}$ and identities on the remaining systems

$$\Delta = \sum_{s=2}^{n} \sum_{\substack{S \subseteq N \\ |S|=s}} \left(A^{(S)} \otimes \bigotimes_{j \notin S} I^{(j)} \right) . \tag{C12}$$

Here, the size of the subsystems is denoted by $s \geq 2$, and it is at least two. The matrix is the sum over all possible combinations of the anti-diagonal matrices for these subsystems and the identities on the remaining systems. As an example take $n = 3$ and $N = \{1, 2, 3\}$. Then the matrix can be explicitly written as

$$\Delta = A^{(\{1,2\})} \otimes I^{(3)} + A^{(\{1,3\})} \otimes I^{(2)} \tag{C13}$$

$$+ A^{(\{2,3\})} \otimes I^{(1)} + A^{(\{1,2,3\})} . \tag{C14}$$

Due to the Hadamard product and

$$\bigotimes_{i=1}^{n} (I - \phi^{(i)}) = \sum_{s=0}^{n} (-1)^s \sum_{\substack{S \subseteq N \\ |S|=s}} \left(\phi^{(S)} \otimes \bigotimes_{j \notin S} I^{(j)} \right) , \tag{C15}$$

with $\phi^{(S)} = \bigotimes_{i \in S} \phi^{(i)}$ the second part of the expression for Φ yields

$$\chi = \sum_{s=2}^{n} (-1)^s \sum_{\substack{S \subseteq N \\ |S|=s}} \left(\left(\phi^{(S)} \odot A^{(S)} \right) \otimes \bigotimes_{j \notin S} I^{(j)} \right) . \tag{C16}$$

With this result, an n-qubit product state $\sigma' = \bigotimes_{i=1}^{n} \sigma'^{(i)}$, and $\mathrm{Tr}\big(\sigma'^{(i)}\big) = 1$, the trace $\mathrm{Tr}(\chi\sigma')$ yields

$$\mathrm{Tr}(\chi\sigma') = \sum_{s=2}^{n} (-1)^s \sum_{\substack{S \subseteq N \\ |S|=s}} \mathrm{Tr}\left(\left(\phi^{(S)} \odot A^{(S)} \right) \sigma'^{(S)} \right) \tag{C17}$$

with $\sigma'^{(S)} = \bigotimes_{i \in S} \sigma'^{(i)}$. To rewrite the above expression in a tensor product form, decompose the anti-diagonal matrices $A^{(S)}$ into linear combinations of 2×2 matrices so that

$$A^{(S)} = \sum_{\substack{\mathbf{m} \\ |\mathbf{m}|=s}} a_{\mathbf{m}} \sum_{\mathbf{k}} (-1)^{\mathbf{m} \cdot \mathbf{k}} \ |\mathbf{k}\rangle \left\langle \bar{\mathbf{k}} \right| , \tag{C18}$$

with

$$a_{\mathbf{m}} = \frac{1}{2^s} \sum_{\mathbf{j}} (-1)^{\mathbf{m} \cdot \mathbf{j}} \left(1 - \frac{L_{\mathbf{j},\bar{\mathbf{j}}}}{\mathcal{L}_{\mathbf{j},\bar{\mathbf{j}}}} \right) . \tag{C19}$$

Expressing the state $\sigma'^{(S)}$ of the subsystem S in the Dirac notation as $\sigma'^{(S)} = \sum_{\mathbf{r},\mathbf{l}} \sigma'^{(S)}_{\mathbf{r},\mathbf{l}} \, |\mathbf{r}\rangle \langle \mathbf{l}|$ yields

$$\mathrm{Tr}\left(\left(\phi^{(S)} \odot A^{(S)} \right) \sigma'^{(S)} \right) \tag{C20}$$

$$= \sum_{\substack{\mathbf{m} \\ |\mathbf{m}|=s}} a_{\mathbf{m}} \prod_{j \in S} \sum_{k_j} (-1)^{m_j k_j} \phi_{k_j, \bar{k}_j} \sigma'_{\bar{k}_j, k_j} . \tag{C21}$$

The last sum can be simplified to

$$\sum_{k_j} (-1)^{m_j k_j} \phi_{k_j, \bar{k}_j} \sigma'_{\bar{k}_j, k_j} = \frac{t_j}{2} i^{m_j} \, \mathbf{c}^{(j)}_{m_j} \cdot \mathbf{x}_{\sigma'^{(j)}} \tag{C22}$$

with

$$\mathbf{c}^{(j)}_{m_j} = \begin{cases} \frac{\mathbf{x}_{\sigma^{(j)}}}{r_{\sigma^{(j)}}} \times \mathbf{x}_{\phi^{(j)}} & \text{for } m_j = 1, \\ \left(\frac{\mathbf{x}_{\sigma^{(j)}}}{r_{\sigma^{(j)}}} \times \mathbf{x}_{\phi^{(j)}} \right) \times \frac{\mathbf{x}_{\sigma^{(j)}}}{r_{\sigma^{(j)}}} & \text{for } m_j = 0 . \end{cases} \tag{C23}$$

Combining everything leads to

$$\mathrm{Tr}(\chi\sigma') = \sum_{s=2}^{n} (-1)^s \sum_{\substack{S \subseteq N \\ |S|=s}} \sum_{\substack{\mathbf{m} \\ |\mathbf{m}|=s}} a_{\mathbf{m}} \prod_{j \in S} \frac{t_j}{2} i^{m_j} \, \mathbf{c}^{(j)}_{m_j} \cdot \mathbf{x}_{\sigma'^{(j)}} . \tag{C24}$$

Recall that we suppose $\left[\rho^{(j)}, \sigma^{(j)}\right] \neq 0$ for $j = 1, 2$. Choosing $\sigma' = \sigma'^{(1)} \otimes \sigma'^{(2)} \otimes \bigotimes_{i=3}^{n} \sigma^{(i)}$ with $\mathrm{Tr}\big(\phi^{(i)} \sigma'^{(i)}\big) = 0$ simplifies the expression to

$$\mathrm{Tr}(\chi\sigma') = \sum_{\substack{\mathbf{m} \\ |\mathbf{m}|=2}} a_{\mathbf{m}} \prod_{j=1}^{2} \frac{t_j}{2} i^{m_j} \, \mathbf{c}^{(j)}_{m_j} \cdot \mathbf{x}_{\sigma'^{(j)}} . \tag{C25}$$

The coefficients $a_{\mathbf{m}}$ are given by

$$a_{\mathbf{m}} = \begin{cases} \frac{\gamma_+ + \gamma_-}{2} & \text{if } \mathbf{m} = (0,0), \\ \frac{\gamma_+ - \gamma_-}{2} & \text{if } \mathbf{m} = (1,1), \\ 0 & \text{else.} \end{cases} \tag{C26}$$

with

$$\gamma_+ = 1 - \frac{[L(\sigma^{(1)})]_{12} [L(\sigma^{(2)})]_{12}}{[L(\sigma^{(1)} \otimes \sigma^{(2)})]_{14}} , \tag{C27}$$

$$\gamma_- = 1 - \frac{[L(\sigma^{(1)})]_{12} [L(\sigma^{(2)})]_{12}}{[L(\sigma^{(1)} \otimes \sigma^{(2)})]_{23}} . \tag{C28}$$

With Eq. (9) and the eigenvalues of the single-qubit states, we get for $r_{\sigma^{(1)}} \neq r_{\sigma^{(2)}}$

$$\gamma_\pm(r_{\sigma^{(1)}}, r_{\sigma^{(2)}}) = \frac{2 r_{\sigma^{(1)}} r_{\sigma^{(2)}}}{r_{\sigma^{(1)}} \pm r_{\sigma^{(2)}}} \frac{\ln\left(\frac{1+r_{\sigma^{(1)}}}{1-r_{\sigma^{(1)}}}\right) \pm \ln\left(\frac{1+r_{\sigma^{(2)}}}{1-r_{\sigma^{(2)}}}\right)}{\ln\left(\frac{1+r_{\sigma^{(1)}}}{1-r_{\sigma^{(1)}}}\right) \ln\left(\frac{1+r_{\sigma^{(2)}}}{1-r_{\sigma^{(2)}}}\right)} . \tag{C29}$$

If $r_{\sigma^{(1)}} = r_{\sigma^{(2)}}$, the expression for γ_- yields

$$\gamma_-(r_{\sigma^{(1)}}) = \frac{r^2_{\sigma^{(1)}}}{1 - r^2_{\sigma^{(1)}}} \frac{4}{\ln^2\left(\frac{1+r_{\sigma^{(1)}}}{1-r_{\sigma^{(1)}}}\right)} . \tag{C30}$$

The coefficients $a_{\mathbf{m}}$ are nonzero since $\gamma_+ \neq \gamma_-$ for the states on the boundary of the octahedron.
Thus, the trace yields

$$\mathrm{Tr}(\chi\,\sigma') = \frac{t_1 t_2}{8}\Big[(\gamma_- - \gamma_+)\left(\mathbf{c}_1^{(1)}\cdot\mathbf{x}_{\sigma'^{(1)}}\right)\left(\mathbf{c}_1^{(2)}\cdot\mathbf{x}_{\sigma'^{(2)}}\right) \tag{C31}$$

$$+(\gamma_+ + \gamma_-)\left(\mathbf{c}_0^{(1)}\cdot\mathbf{x}_{\sigma'^{(1)}}\right)\left(\mathbf{c}_0^{(2)}\cdot\mathbf{x}_{\sigma'^{(2)}}\right)\Big]\,. \tag{C32}$$

W.l.o.g., we chose that $\sigma^{(1)}$ with Bloch vector $\mathbf{x}_{\sigma^{(1)}}$ is in the relative interior of a facet. Then states exist that are located on the same facet with Bloch vector $\mathbf{x}_{\sigma'^{(1)}}$ and a small $\beta_1 \in \mathbb{R}\setminus\{0\}$. Since $\mathbf{c}_0^{(1)}$ and $\mathbf{x}_{\phi^{(1)}}$ are orthogonal, it holds that

$$\mathbf{c}_0^{(1)}\cdot\mathbf{x}_{\sigma'^{(1)}} = \beta_1\left|\mathbf{c}_0^{(1)}\right|^2, \quad \mathbf{c}_1^{(1)}\cdot\mathbf{x}_{\sigma'^{(1)}} = 0\,. \tag{C33}$$

Then the trace simplifies to

$$\mathrm{Tr}(\chi\,\sigma') = \frac{t_1 t_2}{8}(\gamma_+ - \gamma_-)\beta_1\left|\mathbf{c}_0^{(1)}\right|^2\left(\mathbf{c}_0^{(2)}\cdot\mathbf{x}_{\sigma'^{(2)}}\right)\,. \tag{C34}$$

Since the sign of β_1 is free to choose, we can find a state such that $\mathrm{Tr}(\chi\,\sigma') < 0$. Consequently, Φ is not a supporting hyperplane of the set of stabilizer states, and $\sigma = \bigotimes_{i=1}^n \sigma^{(i)}$ is not closest to $\rho = \bigotimes_{i=1}^n \rho^{(i)}$. Hence, the relative entropy of magic is not additive for ρ.