ON MULTIPARTITE ENTANGLEMENT AND ITS USE

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Aby Philip

December 2024

ON MULTIPARTITE ENTANGLEMENT AND

ITS USE

Aby Philip, Ph.D.

Cornell University 2024

Entanglement is a unique feature of quantum mechanics. Over the years, we have understood bipartite entanglement a lot more, while our understanding of multipartite entanglement has lagged. In this work, we aim to fill some gaps in this knowledge. Firstly, we provide a quantum algorithm to test whether a given multipartite state is multipartite entangled or multipartite separable. To develop this separability test, we start with a separability test for the bipartite scenario using the quantum steering effect. Our separability test consists of a distributed quantum computation involving two parties: a computationally limited verifier, who prepares a purification of the state of interest, and a computationally unbounded prover. We then modified the separability test to get a variational quantum steering algorithm (VQSA), implementable on quantum computers that are available today. We then simulate our VQSA on noisy quantum simulators and find favorable convergence properties on the examples tested. We extend our separability test to the multipartite scenario by using the appropriate definitions.

We expect that multipartite entanglement will find use in quantum network scenarios. Quantum networks consist of various quantum technologies, spread across vast distances, and involve various users at the same time. Certifying the functioning and efficiency of the individual components is a task that is well stud-

ied and widely used. However, the power of quantum networks can only be realized by integrating all the required quantum technologies and platforms across numerous users. In this work, we demonstrate how to certify the distillable entanglement available in multipartite states produced by quantum networks, without relying on the physical realization of its constituent components. We do so by using the paradigm of device independence.

Finally, we introduce multipartite intrinsic non-locality as a method for quantifying resources in the multipartite scenario of device-independent (DI) conference key agreement. We prove that multipartite intrinsic non-locality is additive, convex, and monotone under a class of free operations called local operations and common randomness. As one of our technical contributions, we establish a chain rule for two variants of multipartite mutual information, which we then use to prove that multipartite intrinsic non-locality is additive. This chain rule may be of independent interest in other contexts. All of these properties of multipartite intrinsic non-locality are helpful in establishing the main result: multipartite intrinsic non-locality is an upper bound on secret key rate in the general multipartite scenario of DI conference key agreement.

BIOGRAPHICAL SKETCH

Aby Philip completed his high school education in Bangalore, India. After clearing various national-level examinations, he started his undergraduate studies at the Indian Institute of Science Education and Research Thiruvananthapuram (IISER-TVM) in 2014. He received his BS-MS dual degree in 2019, majoring in Physics with a minor in Mathematics.

He started his doctoral studies at the Department of Physics and Astronomy, Louisiana State University in 2019. In August 2020, he started his doctoral research with Dr. Mark M. Wilde, then Associate Professor in the Department of Physics and Astronomy, Louisiana State University.

Aby then transferred to the School of Applied and Engineering Physics, Cornell University in August 2022 with Dr. Mark M. Wilde, now Associate Professor, School of Electrical and Computer Engineering, Cornell University. He continued his doctoral research. He completed his A-Exam in September 2023.

This document is dedicated to Amma and Appa.

ACKNOWLEDGEMENTS

I would like to thank Prof. Mark M. Wilde for his continued support at both Louisiana State University (LSU) and Cornell University. He has been instrumental in my growth as a scholar and scientist. Through my discussions with Mark, I have learned how to approach research problems with care and precision and that no detail is too small. He has always been supportive, especially when my research projects, as they often do, fail to materialize into anything worthy of publication. He has always encouraged me to do better at everything research related, be it writing manuscripts, presenting my work, or research in general.

I would also like to thank Prof. Peter McMahon and Prof. Jayadev Acharya for agreeing to be part of my select committee here at Cornell and their invaluable advice throughout my PhD journey. I would also like to thank Prof. Hwang Lee, Prof. Kenneth Schafer, and Prof. Shuangqing Wei for being in my select committee at LSU.

I'm especially thankfully to Prof. Peter Bierhorst, Vincent Russo, Eneet Kaur, and Soorya Rethinasamy for being such amazing collaborators. Working with them has been a true delight. I can't thank them enough for the hours they spent pouring over my drafts and always being encouraging with feedback. I'm especially thankful to Soorya for creating the figures in Chapter 2. My papers would not be the same without Ignatius W. Primaatmaja, Charles C.-W. Lim, and Ashutosh Marwah.

I acknowledge funding from Air Force Office of Scientific Research Award Nos. FA9550-20-1-0067 and FA8750-23-2-0031, and National Science Foundation

under Grant No. 1907615. I acknowledge support from the Department of Physics and Astronomy at LSU, the School of Electrical and Computer Engineering, and the School of Applied and Engineering Physics at Cornell. I would like to thank all the professors and undergraduates who made my experience as a teaching assistant extremely fulfilling.

It goes without saying that my time as a doctoral student would have been quite dull and lifeless without: Stav Haldar, Anshumitra Baul, Akhil Bhardwaj, Karunya Shirali, Prerna Agarwal, Soorya Rethinasamy, Lauren Hingle, Vishal Singh, Dhrumil Patel, Hemant Mishra, Theshani Nuradha, Kaiyuan Ji, Aidan Sims, Vyjayanthimala, and Ninja Panther. I want to thank you all for the amazing memories, research discussions, and for being amazing friends. Speaking of friends, I'm endlessly grateful to Aparna Vinod, Akshai J Pillai, Nadi Dixit, and Swathi Harikrishnan for being just the absolute best of friends since forever. To my mother, my father, and my sister, words cannot express my gratitude.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

It has always been a little hard to wrap one's head around entanglement, be it bipartite or multipartite. The implications of the existence of entangled states have been a subject of interest since the introduction of the EPR paradox [4]. We got a better understanding of entanglement through Bell's theorem [5], which provided us with the theoretical tools necessary to develop experiments to test whether entanglement could be explained by classical physics. Such a test was first performed using the Clauser-Horne-Shimony-Holt inequality [6]. Such experiments contributed greatly to our understanding of quantum mechanics and earned Alain Aspect, John Clauser, and Anton Zeilinger the Nobel Prize for Physics in 2022.

Over the years, we have understood bipartite entanglement a lot more, but our understanding of multipartite entanglement is just catching up. Part of the incentive to understand multipartite entanglement comes from the rise of quantum networks. Potential uses for quantum networks include quantum computers connected together for distributed computing tasks [7, 8], a collection of quantum sensors that implement a joint measurement on a system of interest [9, 10, 11, 12], or a number of distant nodes that transmit quantum states among themselves [13, 14]. To realize the full potential of quantum networks, the efficient production and distribution of multipartite entanglement is essential [15]. Hence, a thorough understanding of multipartite entanglement is essential for the development of future

applications of quantum technologies.

1.1 Preliminaries

We begin by recalling some important definitions that will be used throughout this thesis. They are as follows.

Definition 1 *The quantum state of a system A is described by a density operator, ρ_A, which is a unit trace, positive semi-definite operator acting on the Hilbert space $\mathcal{H}_A$.*

The set of all linear operators acting on $\mathcal{H}_A$ is denoted by $L(\mathcal{H}_A)$. We shall denote the identity operator as $\mathbb{I}_A$. The set of all density operators acting on $\mathcal{H}_A$ is denoted by $D(\mathcal{H}_A)$.

Definition 2 *A quantum channel $\mathcal{N}_{A\to B} : L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ is a completely positive trace preserving linear map characterized by a set of finitely many Kraus operators, $\{K_x\}_{x\in\mathcal{X}}$, such that*

$$\mathcal{N}_{A\to B}(Y_A) \coloneqq \sum_{x\in\mathcal{X}} K_x Y_A K_x^\dagger \tag{1.1}$$

for every linear operator $Y_A \in L(\mathcal{H}_A)$, where K_x is a positive semi-definite operator for all $x \in \mathcal{X}$ and $\sum_{x\in\mathcal{X}} K_x^\dagger K_x = \mathbb{I}_A$.

Definition 3 *A measurement of a quantum system of A is described by a positive operator-valued measure (POVM) $\{\Pi_x\}_{x\in\mathcal{X}}$, where Π_x is a positive semi-definite operator for all $x \in \mathcal{X}$ and $\sum_{x\in\mathcal{X}} \Pi_x = \mathbb{I}_A$.*

A physical observable O has a corresponding Hermitian operator acting on the underlying Hilbert space. O has a spectral decomposition as follows:

$$O = \sum_{\lambda \in \text{spec}(O)} \lambda \, \Pi_\lambda \tag{1.2}$$

where spec(O) is the set of distinct eigenvalues of O and Π_λ is a POVM element corresponding to λ. A measurement of O is described by the POVM $\{\Pi_\lambda\}_{\lambda \in \text{spec}(O)}$. The expected value $\langle O \rangle$ of the observable O when the state is ρ is given by

$$\langle O \rangle \coloneqq \text{Tr}[O\rho] = \sum_{\lambda \in \text{spec}(O)} \lambda \ \text{Tr}[\rho \, \Pi_\lambda]. \tag{1.3}$$

A binary observable is an observable with exactly two distinct eigenvalues. Common examples of binary observables are the 2x2 Pauli matrices, σ_x, σ_y, and σ_z, with eigenvalues +1 and –1.

Definition 4 *A quantum instrument is a collection of completely positive trace non-increasing maps* $\{\mathcal{E}_x\}_{x \in \mathcal{X}}$ *where*

$$\mathcal{E}^x(\rho) \coloneqq \frac{E_x \rho \, E_x^\dagger}{\text{Tr}[E_x \rho \, E_x^\dagger]}, \tag{1.4}$$

E_x *is a positive semi-definite operator for all* $x \in \mathcal{X}$ *and* $\sum_{x \in \mathcal{X}} E_x^\dagger E_x = \mathbb{I}$.

Now, we move on to discussing the basics of multipartite entanglement and introducing the problems we address via this thesis.

1.2 Multipartite Entanglement

To discuss multipartite entanglement, we need to start by defining bipartite entanglement. To this end, we must recall what a separable or unentangled state is. A bipartite quantum state σ_{AB} of two spatially separated systems A and B is separable (unentangled) if it can be written as a probabilistic mixture of product states [16]:

$$\sigma_{AB} \coloneqq \sum_{x\in\mathcal{X}} p(x)\, \psi_A^x \otimes \phi_B^x, \tag{1.5}$$

where $\{p(x)\}_{x\in\mathcal{X}}$ is a probability distribution, and ψ_A^x and ϕ_B^x are pure states. The idea here is that the correlations between A and B can be fully attributed to a classical, inaccessible random variable with probability distribution $\{p(x)\}_{x\in\mathcal{X}}$. Any bipartite state that is not a separable state is an entangled state.

Similarly to how we need bipartite separable states to define bipartite entanglement, we need to understand multipartite separable states to understand multipartite entanglement. For simplicity, we shall refer to a multipartite state consisting of M parties an M-partite state. An M-partite state $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M}) \equiv \mathcal{D}(\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_M})$ is fully separable if it can be written as

$$\rho_{A_1\cdots A_M} = \sum_{x\in\mathcal{X}} p(x)\, \psi_{A_1}^{x,1} \otimes \cdots \otimes \psi_{A_M}^{x,M} \tag{1.6}$$

where $\psi_{A_i}^{x,i}$ is a pure state for every $x \in \mathcal{X}$ and $i \in \{1,\ldots,M\}$ and $\{p(x)\}_{x\in\mathcal{X}}$ is a probability distribution. Moving forward, M-SEP will denote the set of all $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ such that $\rho_{A_1\cdots A_M}$ is fully separable.

Unlike in the bipartite scenario where an entangled state is simply one that is not separable, the definition of a multipartite entangled state is a bit more nuanced. To highlight this nuance, we will look at two examples of states consisting of just three parties. First, consider the following state:

$$\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \otimes \frac{|0\rangle_C + |1\rangle_C}{\sqrt{2}}. \tag{1.7}$$

It is clear that such a state cannot be written in the form described in (1.6) and one could argue that it is a tripartite entangled state. Let us split the three systems into two groups, say AB and C. We call such a splitting a bipartition. The state above is separable on the bipartition AB and C. Now, consider the state,

$$\frac{|000\rangle_{ABC} + |111\rangle_{ABC}}{\sqrt{2}}. \tag{1.8}$$

It is clear that such a state cannot be written in form described in (1.6). Moreover, regardless of the bipartition, the state shared is not separable. We call such states genuinely tripartite entangled.

In general, one could split the M parties of a multipartite state into $k \leq M$ groups. This is called a k-partition. An M-partite state is said to be k-separable if, on some k-partition, $k \leq M$, the state is separable. An M-partite state is genuinely multipartite entangled if the state is not k-separable for all $k \leq M$.

No discussion about entanglement can be complete without an overview of Local Operations and Classical Communication (LOCC) channels. A channel $\mathcal{L}^{\rightarrow}_{A_1 \ldots A_M \rightarrow A'_1 \ldots A'_M}$ is said to one-way LOCC channel from A_1 to $A_2 \ldots A_M$ if it can be

written as

$$\mathcal{L}^{\rightarrow}_{A_1\ldots A_M\to A'_1\ldots A'_M} := \sum_{x\in\mathcal{X}} \mathcal{E}^x_{1,A_1\to A'_1}\otimes \mathcal{N}^x_{2,A_2\to A'_2}\otimes\cdots\otimes\mathcal{N}^x_{M,A_M\to A'_M} \tag{1.9}$$

where $x \in \mathcal{X}$ is a classical message publicly communicated to all parties, $\mathcal{E}^x_1$ is a quantum instrument and $\mathcal{N}^x_i$ is a quantum channel for all $x \in \mathcal{X}$ and $i \in \{2,\ldots,M\}$ [17]. We can define one-way LOCC from any A_i to the other parties similarly. An LOCC channel $\mathcal{L}_{A_1\ldots A_M\to A'_1\ldots A'_M}$ is then just a composition of finitely many one-way LOCC channels. LOCC channels are important to our discussion about entanglement because such channels cannot be used to produce entangled states or increase the amount of entanglement shared between distant parties [18].

Though above definitions of the bipartite and multipartite entanglement are straightforward to write down, but it is a different matter to formulate an algorithm to decide if a general state is separable; in fact, it has been proven to be computationally difficult in a variety of frameworks [19, 20, 21, 22, 23]. Intuitively, deciding the answer requires performing a search over all possible probabilistic decompositions of the state, and there are too many possibilities to consider. Regardless, determining whether a general state ρ_{AB} is separable or entangled, known as the separability problem, is a fundamental problem of interest relevant to various fields of physics, including condensed matter [24, 25, 26], quantum gravity [27, 28, 29, 30, 31], quantum optics [32], and quantum key distribution [33, 34]. In quantum information science, entanglement is the core resource in several basic quantum information processing tasks [33, 35, 36], making the separability problem essential in this field as well.

Part of the challenge in using entangled states for various tasks is that they are hard to produce and maintain faithfully on any physical platform. The utility of entangled states drops off dramatically the further they are from being perfectly or maximally entangled. Therefore, assessing the quality of entangled states produced becomes an important task, thus motivating the problem of quantifying entanglement [13, 37, 38, 18], in addition to deciding whether entanglement is present. We tackle the task of deciding whether a state is entangled in Chapter 2 of this thesis.

1.3 Device Independence

A problem that is related to the separability problem is the issue of testing whether the state shared between two distant parties is the maximally entangled state, i.e.,

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.10}$$

We can use the CHSH game [6] to do this. Consider two distant parties, Alice and Bob, who share a bipartite state and can perform two measurements on their share of the bipartite state. We denote Alice's choice of measurement by $x \in \{0, 1\}$ and their outcomes by $a \in \{0, 1\}$. Similarly, we denote Bob's choice of measurement by $y \in \{0, 1\}$ and their outcomes by $b \in \{0, 1\}$. In each round of the game, Alice and Bob receive their shares of the bipartite state. We choose x and y independently and uniformly at random, perform the corresponding measurement, and record the outcomes a and b. After all the rounds of the game, they use public communi-

cation to share all values of a, b, x, and y and calculate the probability with which $\text{win}(a,b,x,y) = 1$, where $\text{win}(a,b,x,y)$ is defined as follows:

$$\text{win}(a,b,x,y) = \begin{cases} 0, & \text{if } a \oplus b \neq x \wedge y \\ 1, & \text{if } a \oplus b = x \wedge y \end{cases}, \tag{1.11}$$

$\oplus$ is the binary XOR operation, and $\wedge$ is the binary AND operation. If the bipartite state Alice and Bob share is a separable state, the winning probability can be 3/4 at most. On the other hand, if Alice and Bob share a maximally entangled state, then the maximum winning probability is $(2+\sqrt{2})/4 \approx 0.85$. If all systems involved are qubits, then the measurement choices that achieve the maximum winning probability are, for Alice, σ_x basis and σ_z basis, and for Bob, $\sigma_x + \sigma_z$ basis and $\sigma_x - \sigma_z$ basis. Here σ_x and σ_x are the 2 x 2 Pauli matrices.

For the CHSH game to be a test for the maximally entangled state, the winning probability of $(2+\sqrt{2})/4$ would need to imply that the underlying state is a maximally entangled state. This is indeed true. It has been shown that if the maximum winning probability is achieved then the underlying state is indeed the maximally entangled state, up to local isometries [39, 40]. In addition, the measurements applied to achieve this winning probability are equivalent to the qubit basis measurement mentioned above [39, 40]. Both of these results put together are known as self testing of the maximally entangled state.

An implication of self testing is that Alice and Bob, without know anything about the state they share or the measurement they are applied on the state, they can infer both the state and measurement applied from the winning probability

of the CHSH game. They need not trust any claim about the state being distributed or the measurements being applied. This is the principle behind device-independence. In the general M-partite scenario, device-independence looks like this. Suppose that all parties $A_1, \ldots, A_M$ are given a share of a multipartite quantum state $\rho_{A_1 \cdots A_M}$, which is distributed to them by a possibly unknown entity. Each party also has access to a black box with which they can interact classically. For each classical input, the corresponding black box applies a positive operator-valued measure (POVM) on its respective share of the multipartite state. After the application of the POVM, the box outputs a classical value that is recorded by the corresponding participant. The parties can use the results of the measurements to complete certain tasks of their choosing. If they use only the inputs and outputs from the black box to complete their task, they will have completed the task independent of the underlying physical realization of the measurement and states shared among them.

For the M-partite device independent protocols, we are looking to self-test the Greenberger–Horne–Zeilinger (GHZ) state. The tripartite GHZ state is defined as follows:

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}}. \tag{1.12}$$

There are several multipartite generalizations of the CHSH game. In this work, we will look at two generalizations in particular: parity-CHSH game [3] and Mermin–Ardehali–Belinskii–Klyshko (MABK) inequality [41, 42, 43].

The parity-CHSH game [3] is defined using a winning condition very similar to

that of the CHSH inequality (1.11). As before, we denote Alice's and Bob's choice of measurement by $x, y \in \{0, 1\}$ and their outcomes by $a, b \in \{0, 1\}$, respectively. We denote Charlie's choice of measurement by $z = 1$ and their outcomes by $c \in \{0, 1\}$. The winning condition, $\text{win}(a, b, c, x, y, z)$, is defined as follows:

$$\text{win}\,(a, b, c, x, y, z) = \begin{cases} 0, & \text{if } a \oplus b \neq x \wedge (y \oplus c) \\ 1, & \text{if } a \oplus b = x \wedge (y \oplus c). \end{cases} \tag{1.13}$$

The probability of $\text{win}(a, b, c, x, y, z) = 1$ is equal to $\cos^2(\pi/8) \approx 0.85$ if the underlying state shared by Alice, Bob, and Charlie is the GHZ state, as defined in (1.12).

The MABK inequality [41, 42, 43] is defined as follows. Let x_i denote an input to the i-th measurement device, and let a_i denote the outcome of a measurement, where $i \in \{1, \ldots, M\}$ and M is the number of parties involved. We can then define the MABK inequality as follows.

Definition 5 *Let $\hat{O}_0^i$ and $\hat{O}_1^i$ be binary observables for all $i \in [M]$. The M-partite MABK operator, $\mathcal{K}_M$, is defined by the following recursion relation:*

$$\mathcal{K}_M := \frac{1}{2}\mathcal{F}(\mathcal{K}_{M-1}, \overline{\mathcal{K}}_{M-1}, \hat{O}_0^M, \hat{O}_1^M), \tag{1.14}$$

$$\mathcal{K}_2 := \frac{1}{2}\mathcal{F}(\hat{O}_0^1, \hat{O}_1^1, \hat{O}_0^2, \hat{O}_1^2), \tag{1.15}$$

where $\overline{\mathcal{K}}_{M-1}$ is obtained from $\mathcal{K}_{M-1}$ by exchanging $\hat{O}_0^i$ and $\hat{O}_1^i$ for all $i \in [M]$ and

$$\mathcal{F}(\hat{B}_0, \hat{B}_1, \hat{C}_0, \hat{C}_1) := \hat{B}_0 \otimes \left(\hat{C}_0 + \hat{C}_1\right) + \hat{B}_1 \otimes \left(\hat{C}_0 - \hat{C}_1\right). \tag{1.16}$$

The M-partite MABK inequalities are then defined for all $M \geq 2$ as

$$2^{\frac{4-M}{2}} \left|\text{Tr}\left[\mathcal{K}_M \rho_{\hat{A}_{[M]}}\right]\right| \leq 2^{\frac{m-M+3}{2}}, \quad m \in [M]. \tag{1.17}$$

The MABK inequalities are such that a violation of the inequalities for $m = 1$ proves that at least two parties are entangled, the violation of the inequalities for $m = M - 1$ proves genuine M-partite entanglement, and the case where $m = M$ gives an upper bound (tight) on what is achievable by quantum mechanics. In this work, we are interested in $m = M - 1$ and $m = M$, which correspond to

$$\beta_M := 2^{\frac{4-M}{2}} \left| \mathrm{Tr}\left[\mathcal{K}_M \rho_{\hat{A}_{[M]}} \right] \right| \in [2, 2\sqrt{2}]. \tag{1.18}$$

The CHSH inequality corresponds to

$$\beta_2 := 2 \left| \mathrm{Tr}\left[\mathcal{K}_2 \rho_{\hat{A}_{[2]}} \right] \right| \in [2, 2\sqrt{2}]. \tag{1.19}$$

For our purposes, we need to turn the MABK inequality into a game. This can be done using the procedure outlined in [44]. By unraveling the recursion in (1.14)–(1.15), we can rewrite the M-MABK operator as

$$\mathcal{K}_M = 2^{-2\lfloor \frac{M}{2} \rfloor} \sum_{x \in \{0,1\}^M} (-1)^{f(x)} \bigotimes_{i \in [M]} \hat{O}^i_{x_i}, \tag{1.20}$$

where $x_i \in \{0, 1\}$ is the ith bit of x and $f : \{0, 1\}^M \to \{0, 1, \perp\}$ is a function such that $(-1)^\perp = 0$ by convention.

For the MABK game, the M parties have two measurement settings each, denoted by $x_i \in \{0, 1\}$, and all measurements have two possible outcomes, denoted by $a_i \in \{0, 1\}$. Then the winning condition for the MABK game is as follows [45]:

$$\mathrm{win}(x_{[M]}, a_{[M]}) := \begin{cases} 1, & \text{if } \bigoplus_{i=1}^M a_i = f(x_{[M]}) \\ 0, & \text{else} \end{cases}, \tag{1.21}$$

where f is defined by the M-MABK operator in (1.20). The minimum and maximum winning probabilities when the underlying state is genuinely multipartite entangled are respectively as follows [45]:

$$p_{\min} := 2^{2\lfloor \frac{M}{2} \rfloor - M - 1} + 2^{\lfloor \frac{M}{2} \rfloor - \frac{M}{2} - 2}, \tag{1.22}$$

$$p_{\max} := 2^{2\lfloor \frac{M}{2} \rfloor - M - 1} + 2^{\lfloor \frac{M}{2} \rfloor - \frac{M}{2} - \frac{3}{2}}. \tag{1.23}$$

Note that when M is even,

$$p^e_{\min} = \frac{3}{4} \quad \text{and} \quad p^e_{\max} = \frac{2 + \sqrt{2}}{4}. \tag{1.24}$$

Similarly when M is odd,

$$p^o_{\min} = \frac{2 + \sqrt{2}}{8} \quad \text{and} \quad p^o_{\max} = \frac{1}{2}. \tag{1.25}$$

Now that we have seen that we can test for multipartite entanglement by making minimal assumptions on the state preparation or the measurement device at hand, it is natural to ask if there are any tasks we can complete without changing the minimal assumptions too much. The answer, of course, is yes. Here, we discuss two such tasks: quantum conference key agreement, in Chapter 4 and certification of multipartite distillable entanglement, in Chapter 3. In the following section, we provide a brief introduction to quantum conference key agreement and entanglement distillation.

1.4 Conference Key Agreement and Entanglement Distillation

Quantum conference key agreement (QCKA) is the generalization of the task of quantum key distribution (QKD) to more than two parties [46] (see [47] for a review). In QKD, the task is to share perfectly correlated, uniformly random secret key between two parties. In QCKA, the task is to share perfectly correlated, uniformly random secret between all M parties involved, where $M \geq 3$. The ideal conference key for the tripartite scenario can be expressed mathematically as follows:

$$\Phi_{L_A L_B L_C E} = 2^{-k} \sum_{l=1}^{2^k} |l\rangle\langle l|_{L_A} \otimes |l\rangle\langle l|_{L_B} \otimes |l\rangle\langle l|_{L_C} \otimes \omega_E, \tag{1.26}$$

where ω_E is the state possessed by the eavesdropper, which is independent of the key shared between the three parties, and k is the length of the conference key.

There are a wide variety of protocols to generate conference key agreement using quantum resources. All such protocols rely on the inherent correlations present in multipartite states, such as the GHZ state (1.12). Examples include the multiparty six-state protocol [46, 48], multiparty BB84 protocol [49], and prepare-and-measure implementations [46, 49]. In Chapter 4, we will focus on bounds on device-independent conference key agreement [3, 50].

For many information theoretic tasks, be it conference key agreement or teleportation, entanglement is a prerequisite. But, as mentioned in earlier, entanglement is difficult to produce and maintain. Many protocols require very specific entangled states, such the maximally entangled state (1.10) or the GHZ state (1.12).

For now, let us look at only the bipartite scenario. If, due to some decoherence process, we were left with some copies of a less-than-ideal entangled state, can we use these copies to "distill" maximally entangled state, $|\Phi^+\rangle$.

More precisely, we want to transform the state ρ_{AB} into a maximally entangled state between Alice and Bob with a Schmidt rank of d, which can be written as follows:

$$\left|\Phi^+\right\rangle_{\hat{A}\hat{B}} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{\hat{A}} |i\rangle_{\hat{B}} \,. \tag{1.27}$$

While performing such a transformation, we cannot allow for all possible quantum channels. This leads to trivial results, as the preparation of the maximally entangled state would also be allowed. Hence, we restricted to performing only local operations and classical communication (LOCC) channels. We shall denote an LOCC channel as $\mathcal{L}_{AB\to\hat{A}\hat{B}}$. The error in this transformation is quantified by the distillation error, expressed as:

$$p_{\text{err}}(\mathcal{L};\rho_{AB}) \coloneqq 1 - F\left(\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{\hat{A}\hat{B}}, \mathcal{L}_{AB\to\hat{A}\hat{B}}(\rho_{AB})\right) \tag{1.28}$$

$$= 1 - \left\langle\Phi^+\right|_{\hat{A}\hat{B}} \mathcal{L}_{AB\to\hat{A}\hat{B}}(\rho_{AB}) \left|\Phi^+\right\rangle_{\hat{A}\hat{B}} \tag{1.29}$$

An entanglement distillation protocol for ρ_{AB} is defined by the pair $(d, \mathcal{L})$, where $d \in \mathbb{N}$ and $\mathcal{L}$ is an LOCC channel. Further, an entanglement distillation protocol for ρ_{AB} is called a (d, ε) protocol, $\varepsilon \in [0, 1]$, if $p_{\text{err}}(\mathcal{L};\rho_{AB}) \leq \varepsilon$.

The one-shot ε-distillable entanglement is the largest d that can be extracted from ρ_{AB} among all (d, ε) protocols. Formally, the one-shot ε-distillable entangle-

ment of ρ_{AB}, denoted by $E_D^{\varepsilon}(\rho_{AB})$, is defined as

$$E_D^{\varepsilon}(\rho_{AB}) = \sup_{(d,\mathcal{L})} \{\log_2 d : p_{\text{err}}(\mathcal{L};\rho_{AB}) \leq \varepsilon\}, \tag{1.30}$$

where the optimization is over all $d \geq 1$ and all LOCC channels $\mathcal{L}_{AB\to\hat{A}\hat{B}}$ and d is the dimension of both $\hat{A}$ and $\hat{B}$. The asymptotic distillable entanglement is defined in terms of the following limit:

$$E_D(\rho_{AB}) \coloneqq \inf_{\varepsilon\in(0,1)} \liminf_{n\to\infty} \frac{1}{n} E_D^{\varepsilon}(\rho_{AB}^{\otimes n}). \tag{1.31}$$

In Chapter 3, we generalize these notions to the general M-partite setting and discuss how one can certify multipartite distillable entanglement.

1.5 Introduction to Variational Quantum Algorithms

A variational quantum algorithm (VQA) is an optimization technique can be realized on today's quantum computers. The general structure of VQAs allows them to be used for a wide-variety of applications and to be tailored to run on various kinds of quantum computer [51]. Let's briefly review the general structure of a VQA.

To begin, we find a loss function $\mathcal{L}$ that encodes the solution of the problem. Then, pick an ansatz i.e. a set of quantum operations that are parameterized by a set of continuous or discrete parameters, Θ, that can be optimized over. Using the quantum computer, we estimate $\mathcal{L}(\Theta)$. Then, we use a classical optimizer to

update Θ so as to find

$$\Theta^* = \arg\min_{\Theta} \mathcal{L}(\Theta). \tag{1.32}$$

This quantum-classical loop is what allows VQAs to tackle a variety of optimization problems. However, VQAs cannot be broadly applied to any sort of optimization. The loss function $\mathcal{L}(\Theta)$ must be one that can be estimated on today's noisy intermediate scale quantum computers [51].

As an example, consider the problem of finding the ground state of a given Hamiltonian $\mathcal{H}$. The task is to find a pure state such that $|\psi\rangle$ such that

$$|\psi\rangle = \arg\min_{|\phi\rangle} \langle\phi| \mathcal{H} |\phi\rangle . \tag{1.33}$$

We can choose an ansatz that approximates the set of all possible states by picking a suitable set of unitary circuits $U(\Theta)$, parameterized by Θ and apply it to some initial state, say $|0\rangle$. Then, we can use a quantum computer to estimate the energy of the state $\langle 0| U^\dagger(\Theta)\mathcal{H}U(\Theta) |0\rangle = \langle\phi(\Theta)| \mathcal{H} |\phi(\Theta)\rangle$. Then, we use a classical optimizer to update Θ so as to find

$$\Theta^* = \arg\min_{\Theta} \langle\phi(\Theta)| \mathcal{H} |\phi(\Theta)\rangle . \tag{1.34}$$

The minimum energy calculated using the ansatz $U(\Theta)$ will always be greater than the true minimum energy or,

$$\min_{|\phi\rangle} \langle\phi| \mathcal{H} |\phi\rangle \leq \min_{\Theta} \langle\phi(\Theta)| \mathcal{H} |\phi(\Theta)\rangle . \tag{1.35}$$

This is due to fact that, as Θ is varied, $U(\Theta)$ can reach only a subset of all possible unitary operations and hence $U(\Theta) |0\rangle$ can only express a subset of all possible states.

The structure of the loss function $\mathcal{L}(\Theta)$ amenable to VQAs is similar to (1.33). The loss functions that VQAs can optimize are either expectations of quantum operators or function of expectations of quantum operators [51]. This is because the current noisy intermediate-scale quantum computers only allow for the estimation of such loss functions.

The choice of ansatz can also be tailored to the quantum computer at one's disposal [51]. The ansatz may also be chosen such that it respects any symmetry that is inherent to the problem being considered [52, 53]. Any ansatz being considered will subject to a trade-off between the set of quantum states that it can express and the amount of training required to optimize the loss function [54, 55]. These problems are also often encountered in classical optimization.

Another commonly encountered issue with variational quantum algorithms is the emergence of barren plateaus or vanishing gradients as the number of qubits increases [56, 54]. However, recent results have shown that this problem can be mitigated by switching from a global reward function to a local reward function [57].

We will use variational quantum algorithms as part of our test for separability in Chapter 2.

CHAPTER 2

SCHRÖDINGER AS A QUANTUM PROGRAMMER: ESTIMATING ENTANGLEMENT VIA STEERING

2.1 Introduction

As we discussed in Chapter 1, Section 1.2, we want to test whether a given state is entangled and to quantify its entanglement content experimentally. A rudimentary approach employs state tomography to reconstruct the density matrix and check whether the matrix represents a state that is entangled [58, 59]. However, the computational complexity of this method scales exponentially with the number of qubits, thus prohibiting its use on larger states of interest. With the rapid development of quantum computers of increasing size, it is already infeasible to perform tomography to estimate the density matrices describing the states of these computers. It is even more daunting to address the separability problem using various well-known one-sided entanglement tests [60, 61, 62, 63]. This leaves us to seek out alternative methods for addressing the separability problem, and one forward-thinking direction is to employ a quantum computer to do so [21, 22, 23, 64].

An approach for addressing the separability problem, which we employ here, involves the quantum steering effect, originally discovered by Schrödinger [65, 66]. The idea of steering is that if two distant systems are entangled, distinct prob-

abilistic ensembles of states can be prepared on one system by performing distinct measurements on the other system. To describe this phenomenon more precisely, we can employ some elementary notions from quantum mechanics. Let ψ_{CD} be a pure state of two distant quantum systems C and D, and let $\rho_C = \mathrm{Tr}_D[\psi_{CD}]$ be the reduced state of the system C. Then by performing a measurement on the system D, it is possible to realize a probabilistic ensemble $\{(p(z), \psi_C^z)\}_z$ of pure states on the system C that satisfies $\rho_C = \sum_z p(z)\psi_C^z$. Moreover, for each possible probabilistic decomposition of ρ_C, a measurement acting on D can realize this decomposition. Steering has been a topic of interest in recent years, with applications to quantum key distribution [67, 68], quantum optics [69, 70], and the foundations of quantum mechanics [71, 72].

As suggested above, we can make a non-trivial link between the separability problem and steering, which offers a quantum mechanical method for approaching the former. To see it, recall that a purification of the separable state σ_{AB} in (1.5) is a pure state φ_{RAB} that satisfies $\mathrm{Tr}_R[\varphi_{RAB}] = \sigma_{AB}$, and consider that one such choice of the state vector $|\varphi\rangle_{RAB}$ in this case is as follows:

$$|\varphi\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{p(x)}\, |x\rangle_R \otimes |\psi^x\rangle_A \otimes |\phi^x\rangle_B, \tag{2.1}$$

where $\{|x\rangle_R\}_{x\in\mathcal{X}}$ is an orthonormal basis. Purifications are not unique, but all other purifications of σ_{AB} are related to the one in (2.1) by the action of a unitary operation on the reference system R [73]. By inspecting (2.1), we see that the systems A and B can be steered into the probabilistic ensemble $\{(p(x), \psi_A^x \otimes \phi_B^x)\}_{x\in\mathcal{X}}$ of product states by performing the projective measurement $\{|x\rangle\langle x|_R\}_{x\in\mathcal{X}}$ on the reference sys-

tem R of φ_{RAB}. This leads to an idea for testing separability in the general case. If a purification of a general state ρ_{AB} is available and the state ρ_{AB} is indeed separable, then one can a) try to find the unitary that realizes the purification in (2.1) and b) perform the measurement $\{|x\rangle\langle x|_R\}_{x\in\mathcal{X}}$ on the reference system R. After receiving the outcome x, one can finally test whether the reduced state is a product state.

As we will see in more detail later, the basic idea outlined above is at the heart of our method to test whether a state is separable. Additionally, this approach leads to a quantum algorithm and complexity-theoretic statements for quantifying the amount of entanglement in a state. We thus provide a meaningful connection between steering, entanglement, quantum algorithms, and quantum computational complexity theory, which has not been observed hitherto.

In this chapter, we expand on the abovementioned idea to develop various separability tests using the quantum steering effect. Our separability test for mixed states consists of a distributed quantum computation involving two parties: a computationally unbounded server, called a prover, which can, in principle, perform any quantum computation imaginable, and a computationally limited client, called a verifier, which can perform time-efficient quantum computations (see Figure 2.2). We prove Theorems 1 and 2, which state that the acceptance probabilities of our algorithms, in the ideal case, are directly related to a bonafide entanglement measure, the fidelity of separability. We also employ concepts from quantum computational complexity theory [74, 75] to understand how difficult this test is to perform. Our second contribution results from a modification of our sepa-

rability test. In an attempt to design a practical algorithm, we replace the prover with a combination of parameterized unitary circuits and classical optimization techniques to perform the necessary computation. This results in a variational quantum steering algorithm (VQSA) that approximates the aforementioned separability test (see Figure 2.3). The concept of quantum steering is again at the heart of our VQSA, just like the test for separability that it approximates. Interestingly, we prove that the acceptance probability of both tests is related to an entanglement measure called fidelity of separability [37, 38]. We also generalize our separability test and VQSA to the multipartite setting, using appropriate definitions of multipartite separability.

Next, we report the results of simulations of the VQSA on a quantum simulator and find that they show favorable convergence properties. In light of the limited scale and error tolerance of near-term quantum computers, we develop semidefinite programs (SDPs) to approximate the fidelity of separability using positive-partial-transpose (PPT) conditions [60, 61] and k-extendibility [62, 63] to benchmark the results obtained from our VQSA. As variational quantum algorithms (VQAs), in general, are prone to encountering barren plateaus [56], we also explore how we can mitigate this issue for our algorithms by making use of the ideas presented in [57].

Our approach is distinct from recent work on quantum algorithms for estimating entanglement. For example, VQAs have been used to address this problem by estimating the Hilbert–Schmidt distance [76], by creating a zero-sum game

using parameterized unitary circuits [77], by employing symmetric extendibility tests [64], by estimating logarithmic negativity [78], and using the positive map criterion [78]. VQAs have also been used to estimate the geometric measure of entanglement of multiqubit pure states [79]. The work of [80] is the closest related to ours, but the test used there requires two copies of the state of interest and controlled swap operations for each run of the algorithm, while our VQSA does not require either. In contrast, we introduce a paradigm for VQAs involving parameterized mid-circuit measurements, which is the core of our method for estimating entanglement, and we suspect that this approach will be helpful in future work for a wide variety of VQAs. Furthermore, as we show in Theorems 1 and 2, the acceptance probabilities of our algorithms, in the ideal case, are directly related to a bona fide entanglement measure, the fidelity of separability.

2.2 Quantum Interactive Proof for Fidelity of Separability

To gain intuition about the separability test for mixed states, let us formulate a simple test for the separability of pure states. From (1.5), we can see that a pure bipartite state φ_{AB} is separable if it can be written in product form, as

$$\varphi_{AB} = \psi_A \otimes \phi_B, \tag{2.2}$$

where ψ_A and ϕ_B are pure states. The test we develop below is important because it will reappear as part of the test for separability in the general case, along with quantum steering. Additionally, our approach slightly differs from the standard

approach for testing entanglement of pure states, which employs two copies of the state in a swap test [81, 82, 23]. Instead, our approach requires only a single copy of the state.

Our pure-state separability test consists of a distributed quantum computation involving a prover and a verifier (see Figure 2.1). The computation starts with the verifier preparing the pure state ψ_{AB}. The prover sends the verifier the pure state $\phi_{A'}$ in register A'. (We note that the prover can send a mixed state; however, the maximum acceptance probability of the test is achieved by a pure state. Hence, without loss of generality, the prover should send a pure state.) The verifier then performs the standard swap test [83, 84] on A and A' and accepts if the measurement outcome is zero. In the standard model of quantum computational complexity [74, 75], the prover attempts to get the verifier to accept the swap test with as high a probability as possible. Thus, in this scenario, the prover selects $\phi_{A'}$ to maximize the overlap between the reduced stated $\psi_A := \mathrm{Tr}_B[\psi_{AB}]$ and $\phi_{A'}$. The maximum acceptance probability is then equal to

$$\begin{aligned}
&\max_{\phi} \mathrm{Tr}[(\Pi^{\mathrm{sym}}_{A'A} \otimes I_B)(\phi_{A'} \otimes \psi_{AB})] \\
&= \frac{1}{2}\left(1 + \max_{\phi} \mathrm{Tr}[F_{A'A}(\phi_{A'} \otimes \psi_A)]\right) \qquad (2.3) \\
&= \frac{1}{2}\left(1 + \max_{\phi} \mathrm{Tr}[\phi_A \psi_A]\right) = \frac{1}{2}\left(1 + \|\psi_A\|_\infty\right), \qquad (2.4)
\end{aligned}$$

where $F_{A'A}$ is the unitary swap operator acting on systems A' and A, the projector $\Pi^{\mathrm{sym}}_{A'A} := \frac{1}{2}\left(I_{A'A} + F_{A'A}\right)$ projects onto the symmetric subspace of A' and A, and $\|\psi_A\|_\infty$ is the spectral norm of the reduced state ψ_A (equal to its largest eigenvalue). Since $\|\psi_A\|_\infty = 1$ if and only if ψ_A is a pure state and this occurs if and only if ψ_{AB} is a

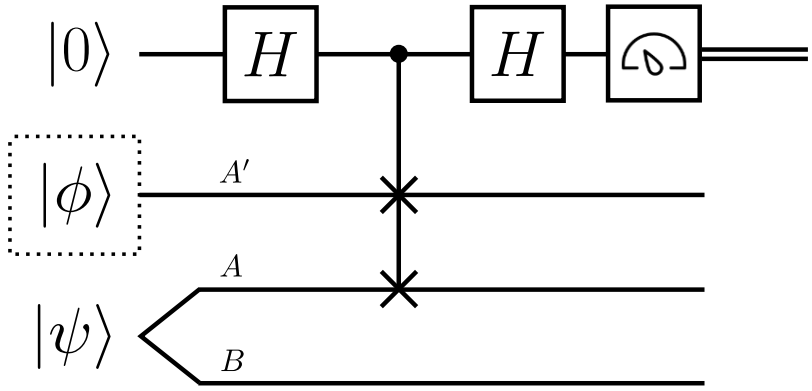


Figure 2.1: Pure-state separability test: The verifier has the pure state ψ_{AB} of interest. The prover (indicated by the dotted box) sends the verifier a pure state $\phi_{A'}$, who then performs the standard swap test on systems A' and A. As mentioned in (2.4), the acceptance probability is equal to $\frac{1}{2}(1 + \|\psi_A\|_\infty)$.

product state, it follows that the maximal acceptance probability is equal to one if and only if ψ_{AB} is a product state.

We now introduce our test for the separability of mixed states. Recall that a bipartite state is separable or unentangled if it can be written in the form given in (1.5), where $|\mathcal{X}| \leq \text{rank}(\sigma_{AB})^2$ [16, 85].

Our separability test for mixed states consists of a distributed quantum computation involving a prover and a verifier. The computation (depicted in Figure 2.2) begins with the verifier preparing a purification ψ_{RAB} of ρ_{AB}. The verifier sends the system R to a quantum prover, whom, in our model, we restrict to performing entanglement-breaking channels. The prover thus performs an entanglement-breaking channel on the reference system R and sends a system A'

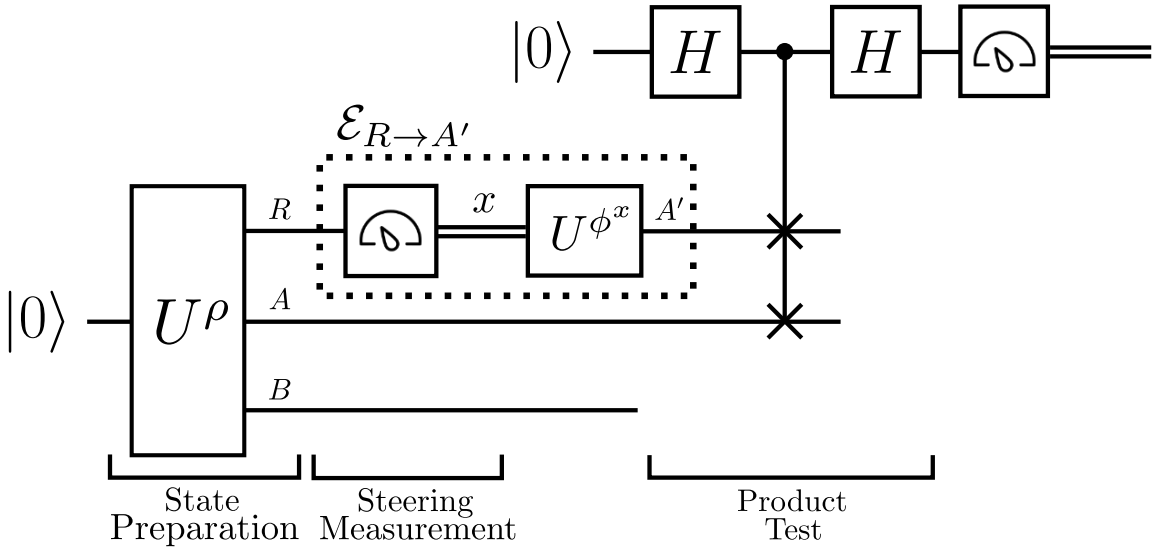


Figure 2.2: Test for separability of mixed states. The verifier uses a unitary circuit U^ρ to produce the state ψ_{RAB}, which is a purification of ρ_{AB}. The prover (indicated by the dotted box) applies an entanglement-breaking channel $\mathcal{E}_{R\to A'}$ on R by measuring the rank-one POVM $\{\mu_R^x\}_x$ and then, depending on the outcome x, prepares a pure state from the set $\{\phi_{A'}^x\}_x$. The final state is sent to the verifier, who performs a swap test. Theorem 1 states that the maximum acceptance probability of this interactive proof is equal to $\frac{1}{2}(1 + F_s(\rho_{AB}))$, i.e., a simple function of the fidelity of separability.

to the verifier. An entanglement-breaking channel $\mathcal{E}_{R\to A'}$ can always be written as a measure-and-prepare channel [86], as follows:

$$\mathcal{E}_{R\to A'}(\cdot) = \sum_{x\in\mathcal{X}} \mathrm{Tr}[\mu_R^x(\cdot)]\, \phi_{A'}^x, \tag{2.5}$$

where $\{\mu_R^x\}_{x\in\mathcal{X}}$ is a rank-one positive operator-valued measure (POVM) and $\{\phi_{A'}^x\}_{x\in\mathcal{X}}$ is a set of pure states. (Due to the above measure-and-prepare decomposition of an entanglement-breaking channel, we can alternatively think of the prover as be-

ing split into two provers, a first who is allowed to perform a general quantum operation, followed by the communication of classical data to a second prover, who then is allowed to perform a general operation before communicating quantum data to the verifier. However, we proceed with the single-prover terminology in what follows.) By performing the measurement portion of the entanglement-breaking channel, the prover has, in essence, steered the verifier's systems A and B to a certain probabilistic ensemble of pure states. After steering the verifier's system, the prover sends system A' to the verifier using the preparation portion of the entanglement-breaking channel. The verifier finally performs a swap test on systems A and A' and accepts if and only if the measurement outcome of the swap test is zero. The standard model in quantum computational complexity theory [74, 75] is that the prover is always trying to get the verifier to accept the computation: in this scenario, the prover steers the verifier's systems A and B to an ensemble that has maximum overlap with a product-state ensemble and then sends an appropriate state to pass the swap test with the highest probability possible.

The maximum acceptance probability of the distributed quantum computation detailed above is equal to

$$\max_{\mathcal{E}\in \mathrm{EB}_{R\to A'}} \mathrm{Tr}\left[\left(\Pi^{\mathrm{sym}}_{A'A} \otimes I_{RB}\right) \mathcal{E}_{R\to A'}\left(\psi_{RAB}\right)\right], \tag{2.6}$$

where $\Pi^{\mathrm{sym}}_{A'A}$ is the projector onto the symmetric subspace of the A' and A systems, and $\mathrm{EB}_{R\to A'}$ denotes the set of all entanglement-breaking channels with input system R and output system A'. We state in Theorem 1 below that the maximum

acceptance probability in (2.6) can be expressed as a simple function of the fidelity of separability of ρ_{AB}, the latter defined as [37, 38]

$$F_s(\rho_{AB}) \coloneqq \max_{\sigma_{AB} \in \mathrm{SEP}(A:B)} F(\rho_{AB}, \sigma_{AB}), \tag{2.7}$$

where $\mathrm{SEP}(A:B)$ denotes the set of separable states shared between Alice and Bob and $F(\rho, \sigma) \coloneqq \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1^2$ is the fidelity of the states ρ and σ [87]. The fidelity of separability is also known as the maximum separable fidelity [21, 22, 23]. We now state two important properties of $F_s(\rho_{AB})$.

Proposition 1 ([88]) *For a state ρ_{AB}, the following formula holds*

$$F_s(\rho_{AB}) = \max_{\{(p(x), \psi_{AB}^x)\}_x} \left\{ \sum_x p(x) F_s(\psi_{AB}^x) : \rho_{AB} = \sum_x p(x) \psi_{AB}^x \right\}, \tag{2.8}$$

where the pure-state ensemble $\{(p(x), \psi_{AB}^x)\}_x$ satisfies $\sum_x p(x)\psi_{AB}^x = \rho_{AB}$, all ψ_{AB}^x are pure, and

$$F_s(\psi_{AB}) = \max_{|\phi\rangle_A, |\varphi\rangle_B} |\langle \psi|_{AB} |\phi\rangle_A \otimes |\varphi\rangle_B|^2. \tag{2.9}$$

Proposition 2 ([88]) *For a bipartite state ρ_{AB}, the following equality holds*

$$F_s(\rho_{AB}) = \max_{\{(p(x), \psi_{AB}^x)\}_x} \left\{ \sum_x p(x) \left\| \psi_A^x \right\|_\infty : \rho_{AB} = \sum_x p(x) \psi_{AB}^x \right\}. \tag{2.10}$$

With these definitions and properties, we state the first key theoretical result of this chapter:

Theorem 1 *For a pure state ψ_{RAB}, the following equality holds:*

$$\max_{\mathcal{E} \in \mathrm{EB}_{R \to A'}} \mathrm{Tr}\left[\left(\Pi_{A'A}^{\mathrm{sym}} \otimes I_{RB} \right) \mathcal{E}_{R \to A'} (\psi_{RAB}) \right] = \frac{1 + F_s(\rho_{AB})}{2}, \tag{2.11}$$

where $F_s(\rho_{AB})$ is the fidelity of separability of the state $\rho_{AB} = \mathrm{Tr}_R[\psi_{RAB}]$.

Proof. Recall that an entanglement-breaking channel can be rewritten as [86]

$$\mathcal{E}_{R\to A'}(\cdot) = \sum_x \mathrm{Tr}[\mu_R^x(\cdot)]\phi_{A'}^x, \tag{2.12}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A'}^x\}_x$ is a set of pure states. Then we find, for fixed $\mathcal{E}_{R\to A'}$, that

$$\mathrm{Tr}[\Pi_{A'A}^{\mathrm{sym}}\mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1}{2}\mathrm{Tr}[(I_{A'A} + F_{A'A})\mathcal{E}_{R\to A'}(\psi_{RAB})] \tag{2.13}$$

$$= \frac{1}{2}\left(1 + \mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]\right). \tag{2.14}$$

So let us work with the expression $\mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})]$. Consider that

$$\mathrm{Tr}[F_{A'A}\mathcal{E}_{R\to A'}(\psi_{RAB})] = \mathrm{Tr}\left[F_{A'A}\sum_x \mathrm{Tr}_R[\mu_R^x\psi_{RAB}]\otimes\phi_{A'}^x\right] \tag{2.15}$$

$$= \mathrm{Tr}\left[F_{A'A}\sum_x p(x)\psi_{AB}^x\otimes\phi_{A'}^x\right] \tag{2.16}$$

$$= \mathrm{Tr}\left[F_{A'A}\sum_x p(x)\psi_{A}^x\otimes\phi_{A'}^x\right] \tag{2.17}$$

$$= \sum_x p(x)\langle\phi^x|_A\psi_A^x|\phi^x\rangle_A, \tag{2.18}$$

where

$$p(x) \coloneqq \mathrm{Tr}[\mu_R^x\psi_{RAB}], \tag{2.19}$$

$$\psi_{AB}^x \coloneqq \frac{1}{p(x)}\mathrm{Tr}_R[\mu_R^x\psi_{RAB}]. \tag{2.20}$$

Thus, the acceptance probability for a fixed entanglement-breaking channel is given by

$$\mathrm{Tr}[\Pi_{A'A}^{\mathrm{sym}}\mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1}{2}\left(1 + \sum_x p(x)\langle\phi^x|_A\psi_A^x|\phi^x\rangle_A\right). \tag{2.21}$$

After optimizing over every element of $\mathrm{EB}_{R\to A'}$, which denotes the set of all entanglement-breaking channels with input system R and output system A', and realizing that optimizing over measurements in $\mathcal{E}_{R\to A'}$ induces a pure-state decomposition of ρ_{AB} and optimizing over preparation channels in $\mathcal{E}_{R\to A'}$ gives the spectral norm of ψ_A^x, we arrive at the claimed formula for the acceptance probability, when combined with (2.8) and (2.10):

$$\max_{\mathcal{E}\in\mathrm{EB}_{R\to A'}} \mathrm{Tr}[(\Pi_{A'A}^{\mathrm{sym}} \otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] = \frac{1 + F_s(\rho_{AB})}{2}. \tag{2.22}$$

This concludes the proof. ■

With this theorem, we have established a separability test for mixed states. We can now discuss the implementation of our separability test for mixed states on today's quantum computers.

2.3 Variational Quantum Steering Algorithm for Fidelity of Separability

We want to point out two important aspects of our separability test from Section 2.2. First, note that, in the real world, no computationally unbounded quantum prover is available to provide the ideal states required for the tests. The other important point is that the swap test at the end of the computation essentially leads to a measure of overlap between the state of the verifier's system and the state provided by the prover.

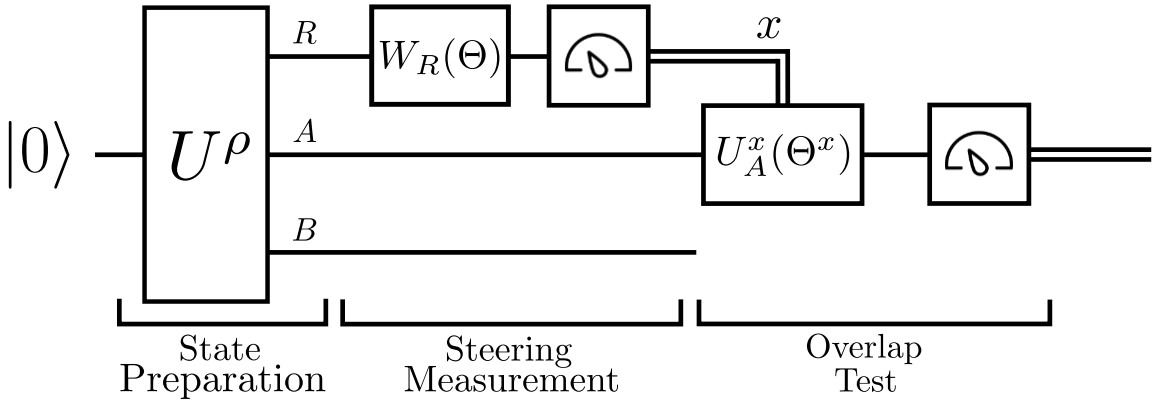


Figure 2.3: Quantum part of the VQSA to estimate the fidelity of separability $F_s(\rho_{AB})$. The unitary circuit U^ρ prepares the state ψ_{RAB}, which is a purification of ρ_{AB}. The parameterized circuit $W_R(\Theta)$ acts on R to evolve ψ_{RAB} to another purification of ρ_{AB}. The following measurement, labeled "steering measurement," steers the systems AB to be in a pure state ψ_{AB}^x if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuit $U_A^x(\Theta^x)$ and the subsequent measurement accepts with a maximum probability of $F_s(\rho_{AB})$.

Taking both these points into consideration, we modify the computational scenario in Figure 2.2 to a) measure the necessary overlaps directly and b) make use of quantum variational techniques [51] (parameterized unitary circuits and classical optimization of parameters) to approximate the actions of a computationally unbounded prover. The resulting procedure also tests and quantifies the separability of a given state by estimating its fidelity of separability. This procedure is a different quantum variational technique called a variational quantum steering algorithm (VQSA). As can be seen in Figure 2.3, quantum steering is at the core of the VQSA via the use of a parameterized mid-circuit measurement.

Our VQSA is structured as follows. Let ρ_{AB} denote the state for which we want to estimate the fidelity of separability, and let ψ_{RAB} be a purification of it, which results from the action of the unitary operator U^{ρ} on the all-zeros pure state $|0\rangle\langle 0|$. Once we have ψ_{RAB}, we can attempt to access all possible pure-state decompositions $\{(p(x), \psi^x_{AB})\}_{x\in\mathcal{X}}$ of ρ_{AB} by acting on the system R with unitary operations. We use the first parameterized unitary $W_R(\Theta)$. To ensure that we have a sufficient number of measurement outcomes (to cover the possible case when $|\mathcal{X}| = \text{rank}(\rho_{AB})^2$), we can prepare some ancillary qubits in the all-zeros state of a system R' and act with W on R and R'. However, without loss of generality, these extra qubits can be grouped as part of an overall reference system, relabeled as R.

After the action of $W_R(\Theta)$, the reference system is measured in the standard basis, and based on the outcome x, the post-measurement state of the system AB is a pure state ψ^x_{AB}. We then estimate the maximum eigenvalue of the reduced state ψ^x_A: this can be accomplished by performing a parameterized unitary $U^x_A(\Theta^x)$, based on the outcome x, on the reduced state ψ^x_A, measuring all qubits of A in the computational basis, and accepting if the all-zeros outcome occurs.

Using a hybrid quantum-classical optimization loop, we can maximize the acceptance probability to estimate the value of the fidelity of separability. The quantum part of this VQSA is summarized in Figure 2.3.

Theorem 2 *If the parameterized unitary circuits involved in the quantum part of the VQSA, summarized in Figure 2.3, can express all possible unitary operators of their re-*

spective systems, then the maximum acceptance probability of the quantum circuit is equal to $F_s(\rho_{AB})$.

Proof. To prove the above statement, let us track the state of the VQSA at the points indicated in Figure 2.4.

- At Step (1), the unitary U^ρ prepares the pure state ψ_{RAB}. This is a specific initial purification of ρ_{AB}.
- At Step (2), we apply the parameterized unitary circuit $W_R(\Theta)$ to ψ_{RAB}. Expanding $W_R(\Theta)|\psi^\rho\rangle_{RAB}$ in terms of the standard basis $\{|x\rangle\}_x$ leads to

$$W_R(\Theta)|\psi\rangle_{RAB} = \sum_{x\in\mathcal{X}} \sqrt{q(x)}|x\rangle_R|\varphi^x\rangle_{AB}. \tag{2.23}$$

- At Step (3), the measurement outcome x occurs with probability $q(x)$, and the state vector of registers A and B becomes $|\varphi^x\rangle_{AB}$.
- At Step (4), depending on the measurement outcome x, we apply the parameterized unitary circuit $U_A^x(\Theta^x)$ to register A. The state vector is now $U_A^x(\Theta^x)|\varphi^x\rangle_{AB}$.
- At Step (5), we trace over B and measure A in the standard basis. We accept when we get the all-zeros outcome. The acceptance probability is then equal to

$$\sum_{x\in\mathcal{X}} q(x)\,\langle 0|\,U_A^x(\Theta^x)\varphi_A^x\,(U_A^x)^\dagger\,|0\rangle = \sum_{x\in\mathcal{X}} q(x)\,\langle\phi^x|_A\varphi_A^x|\phi^x\rangle_A, \tag{2.24}$$

  where we have defined $|\phi^x\rangle_A := \left(U_A^x\right)^\dagger|0\rangle$.

- Maximizing the acceptance probability corresponds to maximization over the parameters of $W_R(\Theta)$ and $U_A^x(\Theta^x)$.
- Maximization over the parameters of W_R is a maximization over all possible pure-state decompositions of ρ_{AB}.
- Maximization over the parameters of $U_A^x(\Theta^x)$ is a maximization of $\langle \phi^x | \varphi_A^x | \phi^x \rangle$, which yields the value $\left\| \varphi_A^x \right\|_\infty$.
- The maximum acceptance probability is equal to

$$\max_{\{(p(x),\psi_{AB}^x)\}_x} \left\{ \sum_x p(x) \left\| \varphi_A^x \right\|_\infty : \rho_{AB} = \sum_x p(x) \psi_{AB}^x \right\}, \tag{2.25}$$

  which is in turn equal to $F_s(\rho_{AB})$, by (2.8) and (2.10).

This concludes the proof. ■

This proves that the maximum acceptance probability equals $F_s(\rho_{AB})$ if the parameterized unitary circuits express all possible unitary operators acting on their respective systems. However, we note that any ansatz employed for the parameterized unitary circuits has limited expressibility. As such, the maximum acceptance probability obtained via the VQSA, in principle, will also be closer to the actual value of $F_s(\rho_{AB})$ if we use a more expressive ansatz.

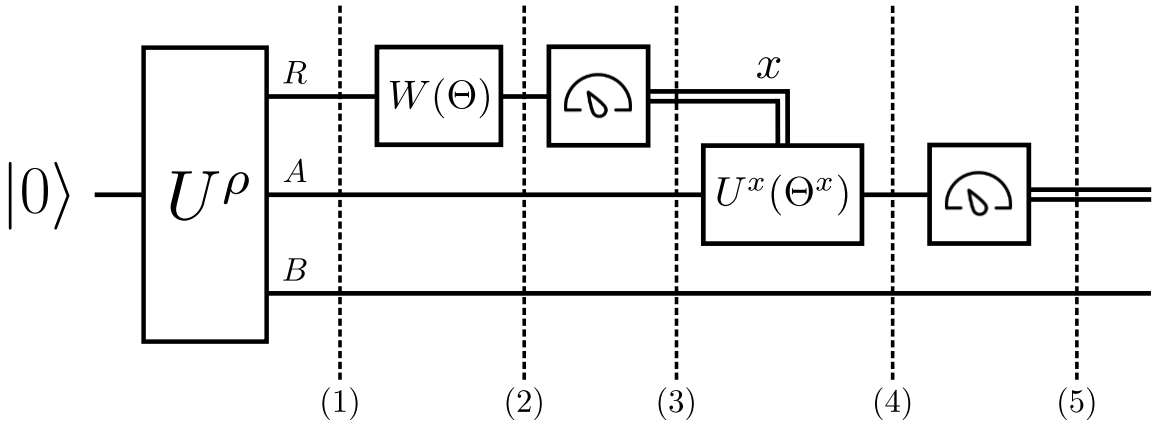


Figure 2.4: VQSA to estimate the fidelity of separability $F_s(\rho_{AB})$. The unitary circuit U^ρ produces the state ψ_{RAB}, which is a purification of ρ_{AB}. The parameterized circuit $W_R(\Theta)$ acts on R to evolve ψ_{RAB} to another pure-state decomposition of ρ_{AB}. The following measurement steers the system AB to be in a pure state ψ^x_{AB} if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuit $U^x_A(\Theta^x)$ and the subsequent measurement estimates $\left\|\psi^x_A\right\|_\infty$.

2.4 Generalization to Multipartite Fidelity of Separability

We now generalize our VQSA to measure the fidelity of separability of multipartite states in the following fashion.

A multipartite state $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M}) \equiv \mathcal{D}(\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_M})$ is separable if it can be written as

$$\rho_{A_1\cdots A_M} = \sum_{x\in\mathcal{X}} p(x)\psi^{x,1}_{A_1} \otimes \cdots \otimes \psi^{x,M}_{A_M} \tag{2.26}$$

where $\psi^{x,i}_{A_i}$ is a pure state for every $x \in \mathcal{X}$ and $i \in \{1,\ldots,M\}$. Let M-SEP denote the set of all $\rho_{A_1\cdots A_M} \in \mathcal{D}(\mathcal{H}_{A_1\cdots A_M})$ such that $\rho_{A_1\cdots A_M}$ is separable.

For the multipartite case of the distributed quantum computation, the verifier prepares a purification $\psi^{\rho}_{RA_1\cdots A_M}$ of $\rho_{A_1\cdots A_M}$. The prover applies a multipartite entanglement-breaking channel on R, which can be written as:

$$\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\cdot) = \sum_{x\in\mathcal{X}} \mathrm{Tr}[\mu^x_R(\cdot)]\left(\phi^{x,1}_{A'_1}\otimes\cdots\otimes\phi^{x,M-1}_{A'_{M-1}}\right), \tag{2.27}$$

where $\{\mu^x_R\}_x$ is a rank-one POVM and $\{\phi^{x,i}_{A'_i}\}_{x,i}$ is a set of pure states. The prover sends systems $(A^{M-1})' \equiv A'_1\cdots A'_{M-1}$ to the verifier. (Here again, we can think of the prover as actually being split into M provers, a first who performs the measurement $\{\mu^x_R\}_x$ and communicates the outcome x to $M-1$ other provers, the ith of whom prepares the state $\phi^{x,i}_{A'_i}$ and sends it to the verifier, for all $i\in\{1,\ldots,M-1\}$.) Finally, the verifier performs a collective swap test on these systems and the systems $A_1\cdots A_M$, as depicted in Figure 2.5. The acceptance probability of this distributed quantum computation is given by

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}}\mathcal{E}_{R\to(A^{M-1})'}(\psi_{RA^{M-1}})], \tag{2.28}$$

where $\Pi^{\mathrm{sym}}_{(A^{M-1})'A^{M-1}}$ is the projection onto the symmetric subspace of systems $(A^{M-1})'$ and A^{M-1} and EB_{M-1} denotes the set of multipartite entanglement-breaking channels defined in (2.27). This leads to the following theorem, which generalizes Theorem 1 to the multipartite case:

Theorem 3 *For a pure state $\psi_{RA^M}\equiv\psi_{RA_1\cdots A_M}$, the following equality holds:*

$$\max_{\mathcal{E}\in\mathrm{EB}_{M-1}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{(A^{M-1})'(A^{M-1})}\mathcal{E}_{R\to A'_1\cdots A'_{M-1}}(\psi_{RA^M})] = \frac{1}{2}\left(1+F_s(\rho_{A_1\cdots A_M})\right), \tag{2.29}$$

where the multipartite fidelity of separability is defined as

$$F_s(\rho_{A_1\cdots A_M}) := \max_{\sigma_{A_1\cdots A_M}\in M-\mathrm{SEP}} F(\rho_{A_1\cdots A_M},\sigma_{A_1\cdots A_M}). \tag{2.30}$$

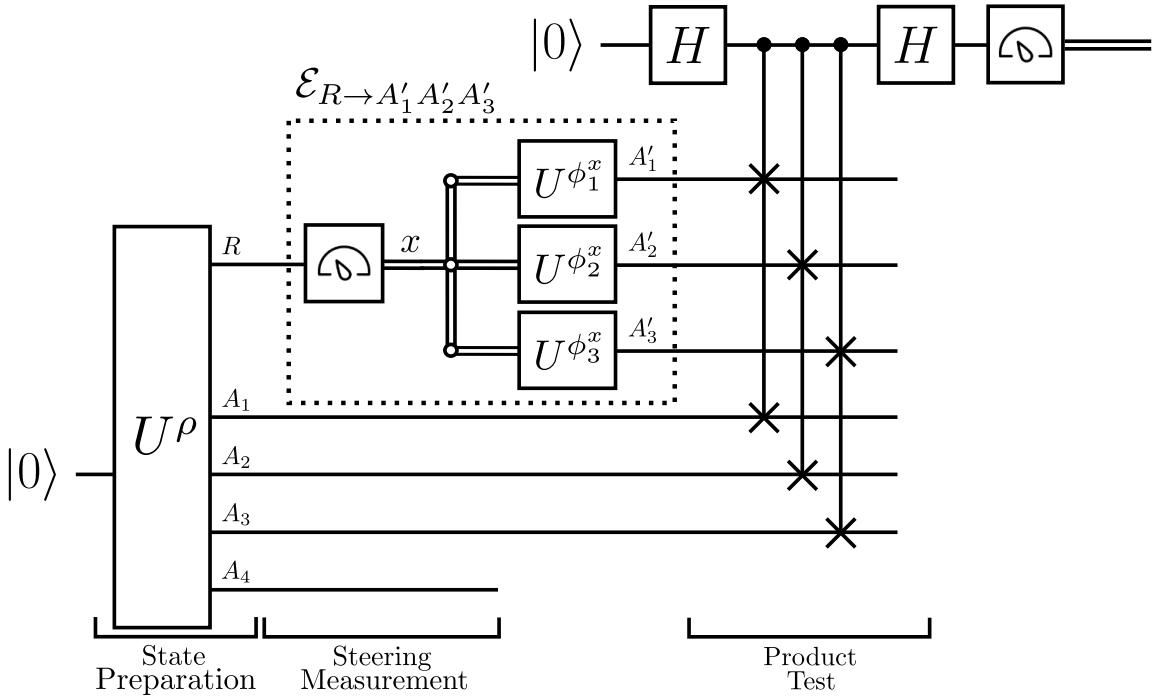


Figure 2.5: Test for separability of multipartite mixed states. The verifier uses a unitary circuit U^ρ to produce the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The prover (indicated by the dotted box) applies an entanglement-breaking channel $\mathcal{E}_{R\to A_1'A_2'A_3'}$ on R by measuring the rank-one POVM $\{\mu_R^x\}_x$ and then, depending on the outcome x, prepares a state from the set $\{\phi_{A_1'}^{x,1} \otimes \phi_{A_2'}^{x,2} \otimes \phi_{A_3'}^{x,3}\}_x$. The final state is sent to the verifier, who performs a collective swap test. Theorem 3 states that the maximum acceptance probability of this interactive proof is equal to $\frac{1}{2}(1 + F_s(\rho_{A_1A_2A_3A_4}))$, i.e., a simple function of the multipartite fidelity of separability.

Proof. The circuit diagram is given in Figure 2.5. The verifier prepares a purification $\psi^\rho_{RA_1\cdots A_M}$ of $\rho_{A_1\cdots A_M}$. The prover applies a multipartite entanglement-breaking

channel on R, which can be written as

$$\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\cdot) = \sum_x \operatorname{Tr}[\mu_R^x(\cdot)]\left(\phi_{A_1'}^{x,1}\otimes\cdots\otimes\phi_{A_{M-1}'}^{x,M-1}\right), \tag{2.31}$$

where $\{\mu_R^x\}_x$ is a rank-one POVM and $\{\phi_{A_i'}^{x,i}\}_{x,i}$ is a set of pure states. The prover sends the systems $(A^{M-1})' = A_1'\cdots A_{M-1}'$ to the verifier. Now, the verifier performs a collective swap test on $A_1\cdots A_M$, as depicted in the final part of the circuit diagram in Figure 2.5. The acceptance probability of this interactive proof system is thus given by

$$\max_{\mathcal{E}\in\mathrm{EB}} \operatorname{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\mathcal{E}_{R\to(A_1\cdots A_{M-1})'}(\psi_{RA_1\cdots A_M})], \tag{2.32}$$

where

$$\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} := \frac{1}{2}\left(I_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} + F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}\right) \tag{2.33}$$

is the projector onto the symmetric subspace of A' and A and $F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}}$ is a tensor product of individual swaps $F_{A_i'A_i}$, for $i\in\{1,\ldots,M-1\}$. That is,

$$F_{(A_1\cdots A_{M-1})'A_1\cdots A_{M-1}} = \bigotimes_{i=1}^{M-1} F_{A_i'A_i}. \tag{2.34}$$

Then we find, for fixed $\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}$, that

$$\begin{aligned}
&\operatorname{Tr}[\Pi^{\mathrm{sym}}_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] \\
&= \frac{1}{2}\operatorname{Tr}[(I_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})} + F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})})\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA_1\cdots A_M})] &(2.35)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\mathcal{E}_{R\to A_1'\cdots A_{M-1}'}(\psi_{RA^M})] &(2.36)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x \operatorname{Tr}[\mu_R^x(\psi_{RA^M})]\phi_{A_1'}^{x,1}\otimes\cdots\otimes\phi_{A_{M-1}'}^{x,M-1}\right], &(2.37)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}\left[F_{(A_1\cdots A_{M-1})'(A_1\cdots A_{M-1})}\sum_x p(x)(\psi_{A_1\cdots A_M}^x)\phi_{A_1'}^{x,1}\otimes\cdots\otimes\phi_{A_{M-1}'}^{x,M-1}\right], &(2.38)
\end{aligned}$$

$$= \frac{1}{2} + \frac{1}{2} \sum_x p(x) \operatorname{Tr}\left[\left(\phi^{x,1}_{A_1} \otimes \cdots \otimes \phi^{x,M-1}_{A_{M-1}} \right) \psi^x_{A_1 \cdots A_{M-1}} \right], \tag{2.39}$$

where

$$p(x) := \operatorname{Tr}[\mu^x_R \psi_{RA^M}], \tag{2.40}$$

$$\psi^x_{A_1 \cdots A_M} := \frac{1}{p(x)} \operatorname{Tr}_R[\mu^x_R \psi_{RA^M}]. \tag{2.41}$$

For a given x, let us simplify $F_s(\varphi_{A_1 \cdots A_M})$ as defined in (2.30),

$$F_s(\varphi_{A_1 \cdots A_M}) = \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left| \langle \varphi |_{A_1 \cdots A_M} |\phi^1\rangle_{A_1} \otimes \cdots \otimes |\phi^M\rangle_{A_M} \right|^2 \tag{2.42}$$

$$= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^M} \left| \langle \phi^1 |_{A_1} \otimes \cdots \otimes \langle \phi^M |_{A_M} |\varphi\rangle_{A_1 \cdots A_M} \right|^2 \tag{2.43}$$

$$= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \left\| \langle \phi^1 |_{A_1} \otimes \cdots \otimes \langle \phi^{M-1} |_{A_{M-1}} \otimes I_{A_M} |\varphi\rangle_{A^M} \right\|_2^2 \tag{2.44}$$

$$= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \operatorname{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1} \otimes \cdots \otimes |\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}} \otimes I_{A_M}) \varphi_{A_1 \cdots A_M}] \tag{2.45}$$

$$= \max_{\{|\phi^i\rangle_{A_i}\}_{i=1}^{M-1}} \operatorname{Tr}[(|\phi^1\rangle\langle\phi^1|_{A_1} \otimes \cdots \otimes |\phi^{M-1}\rangle\langle\phi^{M-1}|_{A_{M-1}}) \varphi_{A_1 \cdots A_{M-1}}]. \tag{2.46}$$

The first two equalities are from the definition and a rewriting. The third equality follows from the variational characterization of the Euclidean norm of a vector. Noting the form in (2.46) and applying the maximization over entanglement-breaking channels of the form described in (2.27) to (2.39), we arrive at the desired claim in (2.29). ■

We can then use the generalized test of separability of mixed states to develop a VQSA for the multipartite case. See Figure 2.6. This involves replacing the collective swap test in Figure 2.5 with an overlap measurement, similar to how we got Figure 2.3 from Figure 2.2.

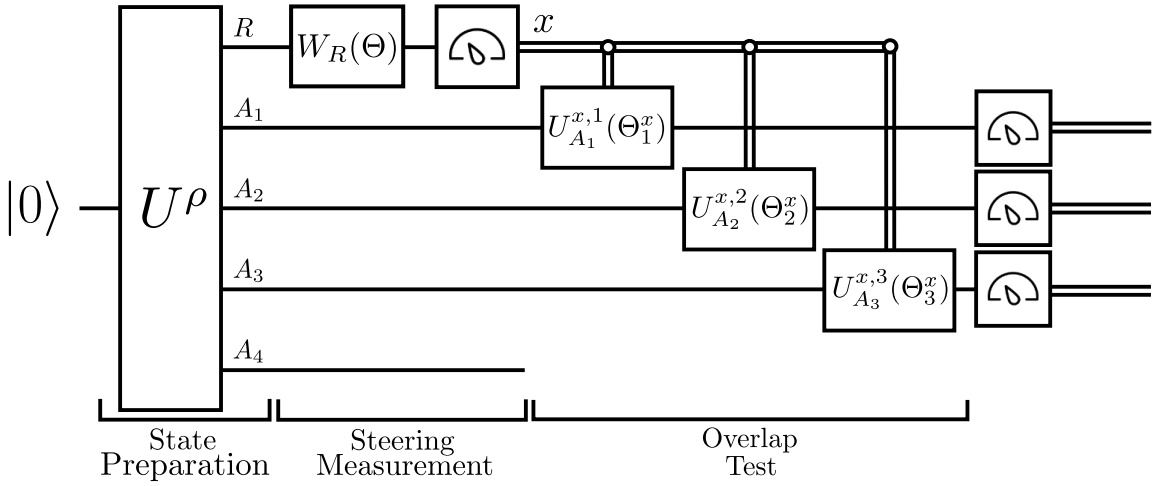


Figure 2.6: VQSA to estimate the multipartite fidelity of separability $F_s(\rho_{A_1A_2A_3A_4})$. The unitary circuit U^ρ prepares the state $\psi_{RA_1A_2A_3A_4}$, which is a purification of $\rho_{A_1A_2A_3A_4}$. The parameterized circuit $W_R(\Theta)$ acts on R to evolve the state to another purification of $\rho_{A_1A_2A_3A_4}$. The following measurement, labeled "steering measurement," steers the remaining systems to be in a state $\psi^x_{A_1A_2A_3A_4}$ if the measurement outcome x occurs. Conditioned on the outcome x, the final parameterized circuits $U^{x,1}_{A_1}(\Theta^x_1)$, $U^{x,2}_{A_2}(\Theta^x_2)$, and $U^{x,3}_{A_3}(\Theta^x_3)$ are applied, and the subsequent measurement accepts with a maximum probability of $F_s(\rho_{A_1A_2A_3A_4})$.

2.5 Benchmarking Semidefinite Programs

Since our algorithms will be running on near-term quantum computers with limited scale and error tolerance, we develop semidefinite programs (SDPs) to benchmark the results from our VQSA because the ideal outcomes can be estimated classically for small numbers of qubits. Our benchmarks $\widetilde{F}^1_s(\rho_{AB}, k)$ and $\widetilde{F}^2_s(\rho_{AB}, k)$ are based on the positive partial transpose (PPT) and k-extendibility hierarchy. We

present the details in subsections 2.5.1 and 2.5.2.

2.5.1 First Benchmarking SDP $\widetilde{F}_s^1$

In this subsection, we detail the derivation of our first benchmarking SDP $\widetilde{F}_s^1$, based on the SDP for fidelity [89]. Let ρ_{AB} and σ_{AB} be bipartite states. The SDP for the root fidelity $\sqrt{F}(\rho_{AB}, \sigma_{AB})$, which makes use of Uhlmann's theorem [87], is as follows:

$$\sqrt{F}(\rho_{AB}, \sigma_{AB}) = \max_{X_{AB} \in \mathcal{L}(\mathcal{H}_{AB})} \left\{ \operatorname{Re}[\operatorname{Tr}[X_{AB}]] : \begin{bmatrix} \rho_{AB} & X_{AB} \\ X_{AB}^\dagger & \sigma_{AB} \end{bmatrix} \geq 0 \right\}, \tag{2.47}$$

where $\mathcal{L}(\mathcal{H}_{AB})$ is the set of all linear operators acting on the Hilbert space $\mathcal{H}_{AB}$.

We would ideally like to include a maximization over the set of all separable states, but it is well known to be computationally challenging to optimize over this set [19, 20]. Furthermore, it is not generally possible to characterize the set of separable states using semi-definite constraints [90]. Instead, we approximate the set by constraining σ_{AB} to have a positive partial transpose (PPT) [60, 61] and be k-extendible [62, 63], since all separable states satisfy these constraints. Let $\widetilde{F}_s^1(\rho_{AB})$

denote the resulting quantity, the square root of which is defined as follows:

$$\sqrt{\widetilde{F}_s^1}(\rho_{AB},k) := \max_{\substack{X_{AB}\in\mathcal{L}(\mathcal{H}_{AB}),\\ \sigma_{AB^k}\geq 0}} \left\{ \begin{array}{c} \operatorname{Re}[\operatorname{Tr}[X_{AB}]] : \\ \begin{bmatrix} \rho_{AB} & X_{AB} \\ X_{AB}^\dagger & \sigma_{AB_1} \end{bmatrix} \geq 0, \\ \operatorname{Tr}[\sigma_{AB^k}] = 1, \\ \sigma_{AB^k} = \mathcal{P}_{B^k}(\sigma_{AB^k}), \\ T_{B_{1\cdots j}}(\sigma_{AB_{1\cdots j}}) \geq 0 \quad \forall j \in \{1,\ldots,k\} \end{array} \right\}, \tag{2.48}$$

where $B^k \equiv B_1 \cdots B_k$, the notation T_R denotes the partial transpose map acting on the system R, and $\mathcal{P}_{B^k}$ denotes the channel that performs a uniformly random permutation of systems B_1 through B_k.

Proposition 3 *The following bound holds for a bipartite state ρ_{AB}:*

$$F_s(\rho_{AB}) \leq \widetilde{F}_s^1(\rho_{AB},k) \leq 1 - \left[\sqrt{1-F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)} \right]^2. \tag{2.49}$$

Proof. Due to the containment discussed above, note that

$$F_s(\rho_{AB}) \leq \widetilde{F}_s^1(\rho_{AB},k). \tag{2.50}$$

An opposite bound on $\widetilde{F}_s^1(\rho_{AB},k)$ in terms of $F_s(\rho_{AB})$ is as follows:

$$\sqrt{1-F_s(\rho_{AB})} \leq \sqrt{1-\widetilde{F}_s^1(\rho_{AB},k)} + 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)}, \tag{2.51}$$

which can be rewritten as in (2.49):

$$\widetilde{F}_s^1(\rho_{AB},k) \leq 1 - \left[\sqrt{1-F_s(\rho_{AB})} - 2\sqrt{\frac{|B|^2}{k}\left(1-\frac{|B|^2}{k}\right)} \right]^2. \tag{2.52}$$

It is a consequence of [91, Theorem II.7′], the triangle inequality for sine distance [92], and the Fuchs-van-de-Graaf inequalities [93]. Indeed, consider that,

$$\widetilde{F}_s^1(\rho_{AB}, k) = \max_{\sigma_{AB} \in \text{EXT-PPT}_k} F(\rho_{AB}, \sigma_{AB}) \tag{2.53}$$

$$\leq \max_{\sigma_{AB} \in \text{EXT}_k} F(\rho_{AB}, \sigma_{AB}), \tag{2.54}$$

where EXT-PPT$_k$ denotes the set of σ_{AB} being optimized over in (2.48) and EXT$_k$ is the set of k-extendible states. Now recall that for all $\omega_{AB}^k \in \text{EXT}_k$ (see [91, Theorem II.7′] and also just above [91, Theorem II.2] for their norm convention)

$$\min_{\sigma_{AB} \in \text{SEP}(A:B)} \frac{1}{2} \left\| \omega_{AB}^k - \sigma_{AB} \right\|_1 \leq \frac{2\,|B|^2}{k}, \tag{2.55}$$

the sine distance obeys the triangle inequality [92]:

$$\sqrt{1 - F(\omega, \tau)} \leq \sqrt{1 - F(\omega, \xi)} + \sqrt{1 - F(\xi, \tau)}, \tag{2.56}$$

and the Fuchs-van-de-Graaf inequality [93]:

$$1 - \sqrt{F}(\omega, \tau) \leq \frac{1}{2} \left\| \omega - \tau \right\|_1, \tag{2.57}$$

where ω, τ, and ξ are states. If $\frac{1}{2} \left\| \omega - \tau \right\|_1 \leq \varepsilon$, the latter implies that

$$1 - \sqrt{F}(\omega, \tau) \leq \varepsilon \;\Leftrightarrow\; \sqrt{1 - F(\omega, \tau)} \leq \sqrt{\varepsilon\,(2 - \varepsilon)}. \tag{2.58}$$

Letting σ_{AB}^k be an optimal choice in (2.54) and σ'_{AB} an optimal choice for $\min_{\sigma_{AB} \in \text{SEP}(A:B)} \frac{1}{2} \left\| \omega_{AB}^k - \sigma_{AB} \right\|_1$, this implies that

$$\min_{\sigma_{AB} \in \text{SEP}(A:B)} \sqrt{1 - F(\rho_{AB}, \sigma_{AB})} \leq \sqrt{1 - F(\rho_{AB}, \sigma'_{AB})} \tag{2.59}$$

$$\leq \sqrt{1 - F(\rho_{AB}, \sigma_{AB}^k)} + \sqrt{1 - F(\sigma'_{AB}, \sigma_{AB}^k)} \tag{2.60}$$

$$\leq \sqrt{1 - F(\rho_{AB}, \sigma_{AB}^{k})} + 2\sqrt{\frac{|B|^2}{k}\left(1 - \frac{|B|^2}{k}\right)}. \tag{2.61}$$

Rearranging and applying (2.53)–(2.54), we arrive at the claimed inequality in (2.51). ■

2.5.2 Second Benchmarking SDP $\widetilde{F}_s^2$

In this subsection, we detail the derivation of our second benchmarking SDP $\widetilde{F}_s^2$, which is an SDP that approximates (2.6) in the main text. Consider a version of the distributed quantum computation that led to (2.6) where, instead of restricting the prover to only entanglement-breaking channels, we insist that the prover sends back k systems labeled as $A_1 \cdots A_k$. Then, the verifier randomly selects one of the k systems and performs a swap test on the A system of the state ψ_{RAB}. This random selection is conducted so that the prover output is effectively reduced to that of an approximate entanglement-breaking channel. Note that the resulting interactive proof is in QIP(2). More specifically, the acceptance probability of this interactive proof system is given by

$$\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \operatorname{Tr}[\Pi_{A'A}^{\mathrm{sym}} \overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})], \tag{2.62}$$

where

$$\overline{\mathcal{P}}_{R\to A'} := \frac{1}{k}\sum_{i=1}^{k} \operatorname{Tr}_{A_1^{k\prime}\setminus A_i} \circ \mathcal{P}_{R\to A'_1\cdots A'_k}, \tag{2.63}$$

and $\mathcal{P}$ is an arbitrary channel. Observing that $\overline{\mathcal{P}}_{R\to A'}$ is a k-extendible channel [94, 95, 96, 97], it follows that

$$\max_{\mathcal{P}_{R\to A'_1\cdots A'_k}} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\overline{\mathcal{P}}_{R\to A'}(\psi_{RAB})] = \max_{\mathcal{E}^k_{R\to A'}\in \mathrm{EXT}_k} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\mathcal{E}^k_{R\to A'}(\psi_{RAB})], \tag{2.64}$$

where EXT_k denotes the set of k-extendible channels. These are defined by $\mathcal{E}^k_{R\to A'}(\rho_{SR}) \in \mathrm{EXT}_k(S:A')$ for every input state ρ_{SR}, where $\mathrm{EXT}_k(S:A')$ denotes the set of k-extendible states. Hence, the quantity in (2.64) is an upper bound on (2.6), and it is given by the following SDP:

$$\max_{\Gamma^{\mathcal{E}^k}_{RA'^k}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\,\mathrm{Tr}_R[T_R(\psi_{RAB})\Gamma^{\mathcal{E}^k}_{RA'_1}]] : \\ \mathrm{Tr}_{A'^k}[\Gamma^{\mathcal{E}^k}_{RA'^k}] = I_R, \\ \Gamma^{\mathcal{E}^k}_{RA'^k} = \mathcal{P}_{A'^k}(\Gamma^{\mathcal{E}^k}_{RA'^k}) \end{array} \right\}, \tag{2.65}$$

where $\Gamma^{\mathcal{E}^k}_{RA'}$ is the Choi operator of $\mathcal{E}^k$ and $\mathcal{P}_{A'^k}$ is the channel that randomly permutes the systems A'^k. We can add further PPT constraints to this SDP, which is still an upper bound on (2.6) and leads to our second benchmark $\widetilde{F}^2_s(\rho_{AB},k)$:

$$\frac{1}{2}(1+\widetilde{F}^2_s(\rho_{AB},k)) := \max_{\Gamma^{\mathcal{E}^k}_{RA'^k}\geq 0} \left\{ \begin{array}{c} \mathrm{Tr}[\Pi^{\mathrm{sym}}_{A'A}\,\mathrm{Tr}_R[T_R(\psi_{RAB})\Gamma^{\mathcal{E}^k}_{RA'_1}]] : \\ \mathrm{Tr}_{A'^k}[\Gamma^{\mathcal{E}^k}_{RA'^k}] = I_R, \\ \Gamma^{\mathcal{E}^k}_{RA'^k} = \mathcal{P}_{A'^k}(\Gamma^{\mathcal{E}^k}_{RA'^k}), \\ T_{A'_{1\cdots j}}(\Gamma^{\mathcal{E}^k}_{RA'^k}) \geq 0 \quad \forall j \in \{1,\ldots,k\} \end{array} \right\} \tag{2.66}$$

where the map T_R is the partial transpose map acting on the system R.

The following theorem indicates how $\widetilde{F}^2_s$ approximates $F_s(\rho_{AB})$.

Proposition 4 *The following bound holds for a bipartite state ρ_{AB}:*

$$F_s(\rho_{AB}) \leq \widetilde{F}^2_s(\rho_{AB},k) \leq F_s(\rho_{AB}) + \frac{4\,|A|^3\,|B|}{k}. \tag{2.67}$$

Proof. Since every entanglement-breaking channel is k-extendible, we trivially find that

$$\frac{1+F_s(\rho_{AB})}{2} = \max_{\mathcal{E}\in\text{EB}} \text{Tr}[(\Pi^{\text{sym}}_{A'A}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] \tag{2.68}$$

$$\leq \max_{\mathcal{E}^k_{R\to A'}\in\text{EXT-PPT}_k} \text{Tr}[(\Pi^{\text{sym}}_{A'A}\otimes I_{RB})\mathcal{E}^k_{R\to A'}(\psi_{RAB})] \tag{2.69}$$

$$= \frac{1+\widetilde{F}^2_s(\rho_{AB},k)}{2}, \tag{2.70}$$

where EXT-PPT$_k$ denotes the set of channels satisfying the constraints in (2.66). Consider the following bound for a k-extendible state ω^k_{AB} [91, Theorem II.7′] (see also just above [91, Theorem II.2] for their norm convention):

$$\min_{\sigma_{AB}\in\text{SEP}(A:B)} \frac{1}{2}\left\|\omega^k_{AB}-\sigma_{AB}\right\|_1 \leq \frac{2|B|^2}{k}. \tag{2.71}$$

We can use it and the result of [98, Lemma 7] to conclude that

$$\min_{\mathcal{E}\in\text{EB}} \frac{1}{2}\left\|\mathcal{E}^k-\mathcal{E}\right\|_\diamond \leq \frac{2|R|\,|A'|^2}{k}. \tag{2.72}$$

Then consider that, for every fixed choice of $\mathcal{E}^k_{R\to A'} \in$ EXT-PPT$_k$, there exists an entanglement-breaking channel $\mathcal{E}$ satisfying

$$\frac{1}{2}\left\|\mathcal{E}^k-\mathcal{E}\right\|_\diamond \leq \frac{2|R|\,|A'|^2}{k}. \tag{2.73}$$

Then we find that

$$\text{Tr}[(\Pi^{\text{sym}}_{A'A}\otimes I_{RB})\mathcal{E}^k_{R\to A'}(\psi_{RAB})]$$

$$\leq \text{Tr}[(\Pi^{\text{sym}}_{A'A}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] + \frac{2|R|\,|A'|^2}{k} \tag{2.74}$$

$$\leq \max_{\mathcal{E}\in\text{EB}} \text{Tr}[(\Pi^{\text{sym}}_{A'A}\otimes I_{RB})\mathcal{E}_{R\to A'}(\psi_{RAB})] + \frac{2|R|\,|A'|^2}{k} \tag{2.75}$$

$$= \frac{1 + F_s(\rho_{AB})}{2} + \frac{2\,|R|\,|A'|^2}{k}. \tag{2.76}$$

Since the inequality holds for every $\mathcal{E}^k_{R\to A'} \in \text{EXT-PPT}_k$, it follows that

$$\max_{\mathcal{E}^k_{R\to A'} \in \text{EXT-PPT}_k} \text{Tr}[(\Pi^{\text{sym}}_{A'A} \otimes I_{RB})\mathcal{E}^k_{R\to A'}(\psi_{RAB})] \leq \frac{1 + F_s(\rho_{AB})}{2} + \frac{2\,|R|\,|A'|^2}{k}. \tag{2.77}$$

This concludes the proof after recalling that $|R| \leq |A||B|$, observing that $|A| = |A'|$, and performing some simple algebra. ■

Remark 4 *Although the correction term in the upper bound in Proposition 4 decreases with increasing k, it is clear that, for it to become arbitrarily small, k needs to be larger than $|A|^3|B|$, which is exponential in the number of qubits for the state ρ_{AB}. Thus, this approach does not lead to an efficient method for placing the fidelity of separability estimation problem in QIP(2) or even QIP.*

2.6 Examples

We now present an example simulation of our VQSA to demonstrate that it can estimate the fidelity of separability. For our first example, we take the state of interest ρ_{AB} to be a (3/4,1/4) probabilistic mixture of two maximally entangled states, $|\Phi^+\rangle = \sqrt{1/2}(|00\rangle + |11\rangle)$ and $|\Phi^-\rangle = \sqrt{1/2}(|00\rangle - |11\rangle)$, so that

$$\rho_{AB} = \frac{3}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{1}{4}|\Phi^-\rangle\langle\Phi^-|. \tag{2.78}$$

Systems R, A, and B of the purification of ρ_{AB} contain one qubit each. See Figure 2.7 for the results. We use the benchmarks and VQSA to estimate the fidelity

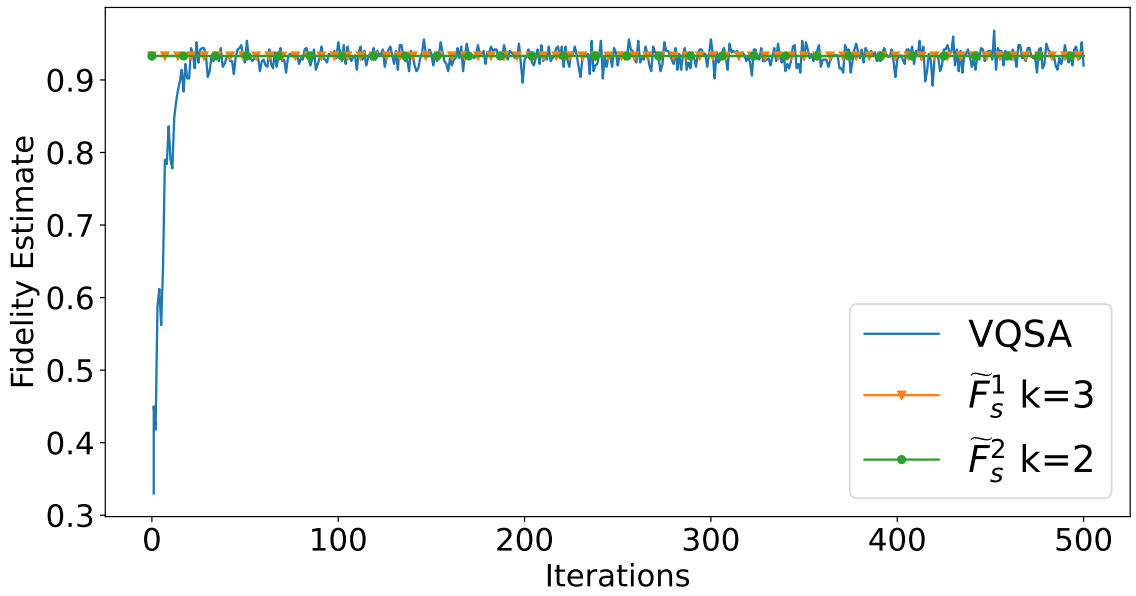


Figure 2.7: Fidelity of separability calculated for a (3/4,1/4) classical mixture of $|\Phi^+\rangle$ and $|\Phi^-\rangle$ using our VQSA (blue line). The algorithm converges to 0.93, which agrees with the value obtained using the benchmarks $\widetilde{F}_s^1$ and $\widetilde{F}_s^2$.

of separability as ≈ 0.93. We evaluate these benchmarks for different levels of the k-extendibility hierarchy. See Section 2.7 for more examples and Section 2.9.1 for details about the code we developed.

As a second example, we consider a state consisting of four qubits. Let us consider the four-qubit state $|\psi\rangle$ defined as follows:

$$\frac{1}{\sqrt{2}}\left(|0\rangle_{A_1}|0\rangle_{A_2}|0\rangle_{B_1}|0\rangle_{B_2} + |1\rangle_{A_1}|1\rangle_{A_2}|1\rangle_{B_1}|1\rangle_{B_2}\right), \tag{2.79}$$

where A consists of two qubits A_1 and A_2 and B consists of two qubits B_1 and B_2. We then pass A_1 and A_2 through a qubit depolarizing channel defined as $\mathcal{D}_p(\rho) :=$

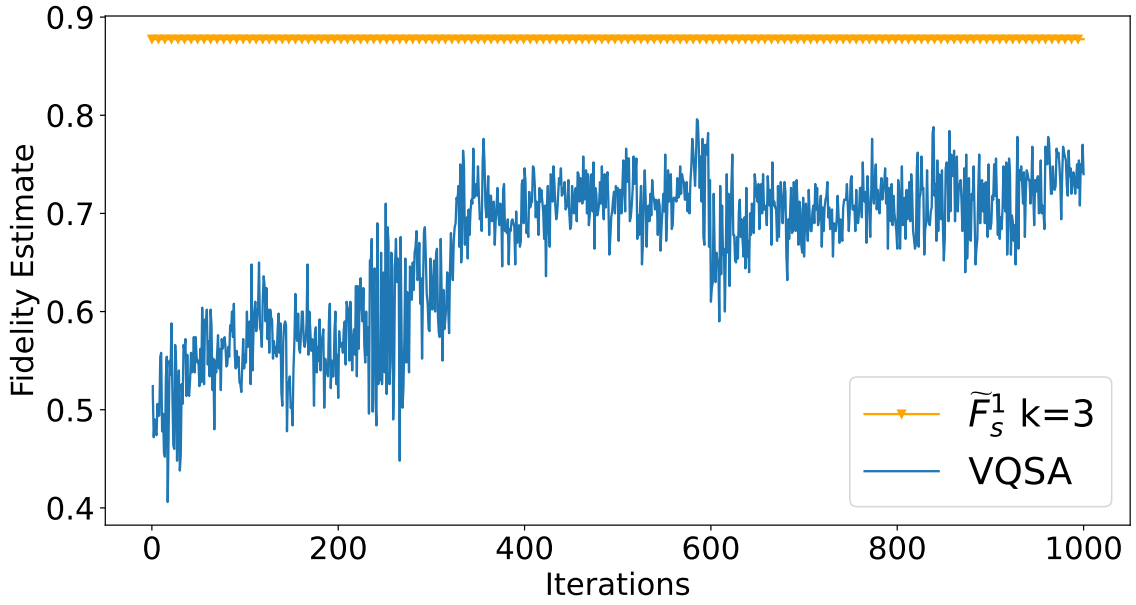


Figure 2.8: Fidelity of separability calculated for the state $\tilde{\rho}_{AB}$ as specified in (2.80) using our VQSA (blue line) and $\widetilde{F}_s^1$ (orange line).

$(1-p)\rho + p\mathbb{I}/2$ where $p = 0.7$. So, the final state under consideration can be written as

$$\tilde{\rho}_{AB} := (\mathcal{D}_{p,A_1} \otimes \mathcal{D}_{p,A_2} \otimes \mathbb{I}_{B_1} \otimes \mathbb{I}_{B_2})(|\psi\rangle\langle\psi|)\,. \tag{2.80}$$

We can then use our VQSA to estimate the fidelity of separability for $\tilde{\rho}_{AB}$ and compare the result against the previous SDP benchmarks. See Figure 2.8 for the results.

2.6.1 Local Reward Function

An essential issue with variational quantum techniques, such as VQAs, is the emergence of barren plateaus or vanishing gradients as the number of qubits increases [56]. However, recent results have shown that this problem can be mitigated by switching from a global reward function to a local reward function [57]. In our case, a global reward function is one in which we measure all the qubits that constitute the system A, as done in the approach discussed in Theorem 2. An example of a local reward function involves selecting a qubit in the system A at random to measure in the computational basis and recording the outcome, accepting if the result equals zero. Our proposed local reward function can be used to obtain upper and lower bounds on our initial global reward function, following the approach of [99, Appendix C]. Local functions have also been used recently to avoid barren plateaus in VQAs when estimating the geometric measure of entanglement for pure states [100].

We develop a local reward function as an alternative to the global reward function considered above, i.e., the acceptance probability in Theorem 2. The acceptance probability in Theorem 2 can be considered a global reward function because it corresponds to the probability of measuring zero in every register. As indicated in [57], it is helpful to employ a local reward function to mitigate the barren plateau problem [56], which plagues all variational quantum algorithms.

Let us define the local and global reward functions. Let Z_i be the event of

measuring zero in the i-th register. We then set the local reward function to be the probability of measuring zero in a register chosen uniformly at random; that is, it is given by the following:

$$L \equiv \frac{1}{n} \sum_i \Pr(Z_i) \,. \tag{2.81}$$

The event of measuring all zeros is given by $\bigcap_i Z_i$, and the probability that this event occurs is $G \equiv \Pr(\bigcap_i Z_i)$, which is what we used in Theorem 2 as the global reward function.

We are interested in determining inequalities related to the global and local reward functions, and the following analysis employs the same ideas used in [99, Appendix C]. Using DeMorgan's laws, we find that

$$\Pr\left(\bigcap_i Z_i\right) = \Pr\left(\left(\bigcup_i Z_i^c\right)^c\right) = 1 - \Pr\left(\bigcup_i Z_i^c\right). \tag{2.82}$$

We can then use the union bound to conclude that

$$\Pr\left(\bigcap_i Z_i\right) = 1 - \Pr\left(\bigcup_i (Z_i)^c\right) \geq 1 - \sum_i \Pr((Z_i)^c) \,. \tag{2.83}$$

Finally, consider that

$$\begin{aligned} G &= \Pr\left(\bigcap_i Z_i\right) && (2.84)\\ &\geq 1 - \sum_i \Pr(Z_i^c) && (2.85)\\ &= \sum_i \Pr(Z_i) - (n-1) && (2.86)\\ &= nL - (n-1) && (2.87)\\ &= n(L-1) + 1. && (2.88) \end{aligned}$$

We can also derive an upper bound on the global reward function in terms of the local reward function. Recall the following inequality, which holds for every set $\{A_1, A_2, \ldots, A_n\}$ of events:

$$\Pr\left(\bigcup_i A_i\right) \geq \frac{1}{n} \sum_i \Pr(A_i)\,. \tag{2.89}$$

Setting $A_i = Z_i^c$, we get

$$\Pr\left(\bigcup_i Z_i^c\right) \geq \frac{1}{n} \sum_i \Pr(Z_i^c)\,. \tag{2.90}$$

Using DeMorgan's laws, we obtain the desired upper bound as follows:

$$G = \Pr\left(\bigcap_i Z_i\right) \leq 1 - \frac{1}{n} \sum_i (1 - \Pr(Z_i)) \tag{2.91}$$

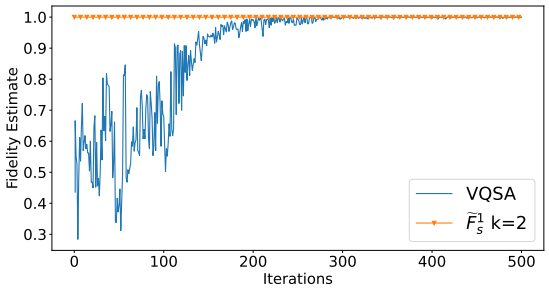
$$= \frac{1}{n} \sum_i \Pr(Z_i) = L. \tag{2.92}$$

In summary, we have established the following bounds:

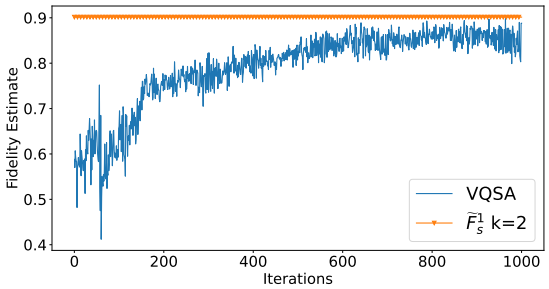
$$n(L-1) + 1 \leq G \leq L, \tag{2.93}$$

so that $G = 1$ if and only if $L = 1$. Since we always have $G \in [0, 1]$, the lower bound is only nontrivial if L is sufficiently large, i.e., if $L \geq 1 - \frac{1}{n}$.

We provide simulations of the local reward function in Section 2.7, indicating that the local reward function can also be used to estimate the fidelity of separability of a given state.



(a) Fidelity of separability calculated for a random product state using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.



(b) Fidelity of separability calculated for a random entangled state using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.

Figure 2.9: Fidelity of separability estimated using the local reward function of the VQSA and benchmarked by $\widetilde{F}_s^1$.

2.7 Further Simulations and Details

For our simulations, we use the Qiskit Aer simulator and Qiskit's Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer to perform the classical optimization. The jitters in the fidelity values between iterations of the VQSA can be attributed to the shot noise in estimating the acceptance probability using the Qiskit Aer simulator, as well as the fact that the SPSA optimizer we have used to perform the classical optimization is itself a stochastic algorithm.

The input states and parameterized unitaries were generated using the hardware efficient ansatz (HEA) [101] for all the simulations in our work. The HEA consists of several layers, each composed of two parameters per qubit per layer, specifying rotations about the x- and y-axes. After each layer of rotations is a series of neighboring qubit CNOT gates. When using the HEA to generate the input

states, we keep the rotation angles fixed, thus leading to a fixed input state. For the parameterized unitaries, the rotation angles are parameters and are optimized over.

In Figure 2.9(a), we report simulation results after generating a random bipartite product state, with each partition containing two qubits. We remove all the CNOT gates from the HEA that generates the input state ρ to guarantee a product state. We calculated the fidelity of separability using both the local reward function of the VQSA and the benchmark $\widetilde{F}_s^1$, the latter discussed in Section 2.5.1.

In Figure 2.9(b), we do the same for a random bipartite state with the partitions A and B containing two qubits and one qubit, respectively, and three qubits in the reference system.

We generated all parameterized unitary circuits in the following fashion. We used the Qiskit Aer simulator and Qiskit's Simultaneous Perturbation Stochastic Approximation (SPSA) optimizer to perform the classical optimization. All other details can be found in Table 2.1. The local reward function of the VQSA requires more classical processing (like picking a qubit at random to measure) and seems to require more iterations to reach the correct value. However, these downsides are outweighed by the fact that it is less susceptible to the emergence of barren plateaus. More details about the local cost function can be found in Section 2.6.1.

Figure	No. of Qubits	State ρ_{AB}	Layer Count
2.7	$R = 2, A = 1, B = 1$	$(3/4)\|\Phi^+\rangle\langle\Phi^+\| + (1/4)\|\Phi^-\rangle\langle\Phi^-\|$	W_R no. of layers = 2 U_A^x no. of layers = 2
2.8	$R = 4, A = 2, B = 2$	$(\mathcal{D}_{p,A_1} \otimes \mathcal{D}_{p,A_2} \otimes \mathbb{I}_B)(\|\psi\rangle\langle\psi\|)$ $\|\psi\rangle = \frac{1}{\sqrt{2}}(\|0\rangle_{A_1}\|0\rangle_{A_2}\|00\rangle_B + \|1\rangle_{A_1}\|1\rangle_{A_2}\|11\rangle_B)$	W_R no. of layers = 4 U_A^x no. of layers = 4
2.9(a)	$R = 3, A = 2, B = 2$	Random product state using HEA [101]	W_R no. of layers = 4 U_A^x no. of layers = 4
2.9(b)	$R = 3, A = 2, B = 2$	Random entangled state using HEA [101]	W_R no. of layers = 4 U_A^x no. of layers = 4

Table 2.1: Details of all VQSA simulations.

2.8 Quantum Computational Complexity Considerations

Our final result is regarding the computational complexity of estimating the fidelity of separability $F_s(\rho_{AB})$. The complexity-theoretic approach allows us to classify the separability problem based on its computational difficulty. Analyses of this form can be effectively conducted within the framework of quantum computational complexity theory [74, 75].

In the paradigm of complexity theory [102], a complexity class is a set of computational problems that require similar resources to solve. If a complexity class A is contained within another class B, then some problems in B could require more computational resources than problems in A. To effectively characterize the difficulty of a class of problems, we pick a problem that is representative of the class or complete for the class. A problem h is considered complete for a complexity

class A if h is contained in the class and the ability to solve the problem h can be extended efficiently to solve every other problem in A.

To tackle the question posed about the computational complexity of estimating the fidelity of separability, we define $\mathrm{QIP}_{\mathrm{EB}}(2)$ to be the complexity class containing problems that can be solved using a prover restricted to applying only entanglement-breaking channels, which processes a quantum message received from the verifier and sends back a quantum message to the verifier. Thus, estimating the fidelity of separability of a given state then falls within $\mathrm{QIP}_{\mathrm{EB}}(2)$, as seen from Figure 2.2. To fully characterize this novel complexity class, we provide a complete problem for it. We establish that, given quantum circuits to generate a channel $\mathcal{N}_{A\to B}$ and a state ρ_B, estimating the following quantity is complete for $\mathrm{QIP}_{\mathrm{EB}}(2)$:

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x,\\ \rho_B=\sum_x p(x)\psi_B^x}} \sum_x p(x) F(\psi_B^x, \mathcal{N}_{A\to B}(\varphi_A^x)), \tag{2.94}$$

where $\{(p(x),\psi^x)\}_x$ is a pure-state ensemble and $\{\varphi^x\}_x$ is a set of pure states.

2.8.1 Complexity Class $\mathrm{QIP}_{\mathrm{EB}}(2)$

In this subsection, we establish a complete problem for $\mathrm{QIP}_{\mathrm{EB}}(2)$, and then we interpret this problem in Remark 7. See [74, 75] for further background on quantum computational complexity theory. Let us first define the complexity class $\mathrm{QIP}_{\mathrm{EB}}(2)$. Let $A = \left(A_{\mathrm{yes}}, A_{\mathrm{no}}\right)$ be a promise problem, and let $a, b : \mathbb{N} \to [0,1]$ and p be polynomial functions. The verifier V is described by a polynomial-time generated family

of quantum circuits. The prover P is a family of arbitrary entanglement-breaking channels that naturally interface with a given verifier. Then $A \in \mathrm{QIP}_{\mathrm{EB}}(2)(a,b)$ if there exists a two-message verifier with the following properties:

1. Completeness: For all $x \in A_{\mathrm{yes}}$, there exists a prover P that causes the verifier V to accept x with probability at least $a(|x|)$.
2. Soundness: For all $x \in A_{\mathrm{no}}$, every prover P causes the verifier V to accept x with probability at most $b(|x|)$.

In the above, acceptance is defined as obtaining the outcome one upon measuring the decision-qubit register.

Problem 5 *Given are circuits to generate a channel $\mathcal{N}_{G\to S}$ and a state ρ_S. Fix α and β such that $0 \leq \alpha < \beta \leq 1$. Decide which of the following holds:*

$$\textit{Yes:} \quad f(\mathcal{N}_{G\to S}, \rho_S) \geq \beta, \tag{2.95}$$

$$\textit{No:} \quad f(\mathcal{N}_{G\to S}, \rho_S) \leq \alpha, \tag{2.96}$$

where

$$f(\mathcal{N}_{G\to S}, \rho_S) := \max_{\{(p(x),\psi^x)\}_x, \{\varphi^x\}_x} \left\{ \sum_x p(x) F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)) : \sum_x p(x)\psi_S^x = \rho_S \right\} \tag{2.97}$$

with the optimization being over every pure-state decomposition of ρ_S as $\sum_x p(x)\psi_S^x = \rho_S$. Also, $\{\varphi^x\}_x$ is a set of pure states.

Theorem 6 *Problem 5 is a complete problem for* $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Proof. The main idea behind the proof is to show that the acceptance probability of a general $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem can precisely be written as $f(\mathcal{N}_{G\to S}, \rho_S)$. This implies that an arbitrary $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem can be reduced to an instance of Problem 5, and we argue at the end how this also implies that Problem 5 can be reduced to an instance of a problem in $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Consider a general interactive proof system in $\mathrm{QIP}_{\mathrm{EB}}(2)$ that begins with the verifier preparing a bipartite pure state ψ_{RS}, followed by the system R being sent to the prover, which subsequently performs an entanglement-breaking channel. The verifier then performs a unitary $V_{R'S\to DG}$ and projects onto the $|1\rangle\langle 1|$ state of the decision qubit. Indeed, the acceptance probability is given by

$$\max_{\mathcal{E}\in\mathrm{EB}} \mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}_{R'S\to DG}(\mathcal{E}_{R\to R'}(\psi_{RS}))], \tag{2.98}$$

where $\mathcal{V}_{R'S\to DG}$ is the unitary channel corresponding to the unitary operator $V_{R'S\to DG}$. By reasoning similar to that in (2.12), (2.19), and (2.20), we find that

$$\mathcal{E}_{R\to R'}(\psi_{RS}) = \sum_x p(x)\phi^x_{R'} \otimes \psi^x_S, \tag{2.99}$$

so that the acceptance probability is equal to

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi^x_S = \psi_S}} \mathrm{Tr}\left[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\left(\sum_x p(x)\phi^x_{R'} \otimes \psi^x_S\right)\right]$$

$$= \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\\ \sum_x p(x)\psi^x_S = \psi_S}} \sum_x p(x)\,\mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\,(\phi^x_{R'} \otimes \psi^x_S)]\,, \tag{2.100}$$

where we have used the shorthand $\mathcal{V} \equiv \mathcal{V}_{R'S\to DG}$. Consider that, for all x,

$$\mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)\mathcal{V}\,(\phi^x_{R'} \otimes \psi^x_S)] = \|\langle 1|_D \otimes I_G)V|\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S\|_2^2 \tag{2.101}$$

$$= \max_{|\varphi^x\rangle_G} |\langle 1|_D \otimes \langle \varphi^x|_G) V |\phi^x\rangle_{R'} \otimes |\psi^x\rangle_S|^2 \tag{2.102}$$

$$= \max_{|\varphi^x\rangle_G} \mathrm{Tr}\Big[V^\dagger (|1\rangle\langle 1|_D \otimes |\varphi^x\rangle\langle\varphi^x|_G) V \phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S \Big] \tag{2.103}$$

$$= \max_{|\varphi^x\rangle_G} \mathrm{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G) \phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S], \tag{2.104}$$

where the isometric channel $\mathcal{W}_{G\to R'S}$ is defined as

$$\mathcal{W}_{G\to R'S}(\cdot) \coloneqq (V_{R'S\to DG})^\dagger (|1\rangle\langle 1|_D \otimes (\cdot)_G) V_{R'S\to DG}, \tag{2.105}$$

and the corresponding isometry $W_{G\to R'S}$ as $W_{G\to R'S} \coloneqq (V_{R'S\to DG})^\dagger |1\rangle_D$. Then, the acceptance probability is given by

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\phi^x\}_x,\{\varphi^x\}_x}} \left\{ \begin{array}{c} \sum_x p(x) \mathrm{Tr}\Big[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G) \phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S\Big] : \\ \sum_x p(x) \psi^x_S = \psi_S \end{array} \right\}. \tag{2.106}$$

Since the optimization over $\phi^x_{R'}$ is arbitrary, we can also write

$$\max_{|\phi^x\rangle_{R'}} \mathrm{Tr}[\mathcal{W}_{G\to R'S}(|\varphi^x\rangle\langle\varphi^x|_G) \phi^x_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S]$$

$$= \max_{|\phi^x\rangle_{R'}} |\langle \phi^x|_{R'} \otimes \langle \psi^x|_S W_{G\to R'S} |\varphi^x\rangle_G|^2 \tag{2.107}$$

$$= \| I_{R'} \otimes \langle \psi^x|_S W_{G\to R'S} |\varphi^x\rangle_G \|_2^2 \tag{2.108}$$

$$= \Big(\langle \varphi^x|_G (W_{G\to R'S})^\dagger I_{R'} \otimes |\psi^x\rangle_S \Big) (I_{R'} \otimes \langle \psi^x|_S W_{G\to R'S} |\varphi^x\rangle_G) \tag{2.109}$$

$$= \langle \varphi^x|_G (W_{G\to R'S})^\dagger (I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S) W_{G\to R'S} |\varphi^x\rangle_G \tag{2.110}$$

$$= \mathrm{Tr}\Big[(I_{R'} \otimes |\psi^x\rangle\langle\psi^x|_S) W_{G\to R'S} |\varphi^x\rangle\langle\varphi^x|_G (W_{G\to R'S})^\dagger \Big] \tag{2.111}$$

$$= \mathrm{Tr}[|\psi^x\rangle\langle\psi^x|_S \mathcal{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)], \tag{2.112}$$

where we define the channel $\mathcal{N}_{G\to S}$ as

$$\mathcal{N}_{G\to S}(\cdot) \coloneqq \mathrm{Tr}_{R'}[(V_{R'S\to DG})^\dagger (|1\rangle\langle 1|_D \otimes (\cdot)_G) V_{R'S\to DG}]. \tag{2.113}$$

Then, we find that the acceptance probability is given by

$$\max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x)\operatorname{Tr}[|\psi^x\rangle\langle\psi^x|_S \mathcal{N}_{G\to S}(|\varphi^x\rangle\langle\varphi^x|_G)] = \max_{\substack{\{(p(x),\psi^x)\}_x,\{\varphi^x\}_x\\ \sum_x p(x)\psi_S^x=\psi_S}} \sum_x p(x) F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)). \tag{2.114}$$

This concludes the proof of the first part.

To see how this implies that Problem 5 can be realized in $\mathrm{QIP}_{\mathrm{EB}}(2)$, note that the circuit preparing the state ρ_S prepares a purification and traces over the reference system, and the circuit to generate $\mathcal{N}_{G\to S}$ is realized by adjoining an environment system in the state $|0\rangle\langle 0|$, performing a unitary, and tracing over the environment. So we let the verifier prepare the purification of ρ_S and this plays the role of ψ_{RS} above, and the channel $\mathcal{N}_{G\to S}$ can be realized precisely as in (2.113) with appropriate substitutions. ■

Remark 7 *The quantity in* (2.97) *can be interpreted as follows: Given a channel* $\mathcal{N}$ *and a source state* ρ*, calculate the largest average ensemble fidelity attainable in reproducing the source at the output of the channel. This means it is necessary to find the ensemble decomposition* $\{(p(x),\psi^x)\}_x$ *of* ρ *as well as a set* $\{\varphi^x\}_x$ *of encoding states that lead to the largest ensemble fidelity (and this is what is left to the prover). This criterion is similar to one used in Schumacher data compression [103], but this seems more similar to the setting of the source-channel separation theorem [104], in which the goal is to transmit an information source over a quantum channel. The channel* $\mathcal{N}$ *here could consist of a fixed encoding* $\mathcal{E}$*, noisy channel* $\mathcal{M}$*, and fixed decoding* $\mathcal{D}$*, (i.e.,* $\mathcal{N} = \mathcal{D}\circ\mathcal{M}\circ\mathcal{E}$*) and then the goal is to test how well a given fixed scheme* $(\mathcal{E},\mathcal{D})$ *can communicate a source* ρ *over a*

channel $\mathcal{M}$, according to the ensemble fidelity criterion.

Remark 8 *We can write the expression in (2.97) alternatively as*

$$\text{Eq. (2.97)} = \max_{\substack{\{(p(x),\psi^x)\}_x, \\ \sum_x p(x)\psi_S^x = \rho_S}} \sum_x p(x) \left\| (\mathcal{N}_{G\to S})^\dagger(\psi_S^x) \right\|_\infty , \tag{2.115}$$

where $(\mathcal{N}_{G\to S})^\dagger$ is the Hilbert–Schmidt adjoint of the channel $\mathcal{N}_{G\to S}$. Employing the abbreviations $\psi_S^x \equiv |\psi^x\rangle\langle\psi^x|_S$ and $\varphi_G^x \equiv |\varphi^x\rangle\langle\varphi^x|_G$, this follows because

$$\begin{aligned}
&\max_{\substack{\{(p(x),\psi^x)\}_x, \\ \{\varphi^x\}_x, \\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x) \operatorname{Tr}[\psi_S^x \mathcal{N}_{G\to S}(\varphi_G^x)] \\
&= \max_{\substack{\{(p(x),\psi^x)\}_x, \\ \{\varphi^x\}_x, \\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x) \operatorname{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] &(2.116)\\
&= \max_{\substack{\{(p(x),\psi^x)\}_x, \\ \{\varphi^x\}_x, \\ \sum_x p(x)\psi_S^x = \psi_S}} \sum_x p(x) \max_{\{\varphi^x\}_x} \operatorname{Tr}[(\mathcal{N}_{G\to S})^\dagger(\psi_S^x)\varphi_G^x] &(2.117)\\
&= \max_{\substack{\{(p(x),\psi^x)\}_x, \\ \sum_x p(x)\psi_S^x = \rho_S}} \sum_x p(x) \left\| (\mathcal{N}_{G\to S})^\dagger(\psi_S^x) \right\|_\infty . &(2.118)
\end{aligned}$$

If we define the function

$$g_{\mathcal{N}}(\rho) := \left\| (\mathcal{N}_{G\to S})^\dagger(\rho_S) \right\|_\infty , \tag{2.119}$$

then the function in (2.115) is known as the concave closure of $g_{\mathcal{N}}(\rho)$ and has been studied in other contexts in quantum information theory [105, Section 2]. It has an interesting dual formulation, as demonstrated in [105, Eq. (15)]. Given the observation in (2.115), we can thus conclude that, given circuits to realize the channel $\mathcal{N}$ and state ρ, estimating the concave closure of the function $g_{\mathcal{N}}(\rho)$ within additive error is a complete problem for $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Remark 9 *Employing the reasoning from Remark 8, we find that the acceptance probability in (2.22) is equal to the concave closure of the following function:*

$$f(\rho_{AB}) := \left\| \Pi^{\text{sym}}_{AA'} (\rho_{AB} \otimes I_{A'}) \Pi^{\text{sym}}_{AA'} \right\|_\infty , \tag{2.120}$$

where we used the fact that the state ρ_S from Remark 8 is ρ_{AB} and the map $\mathcal{N}_{G\to S}$ from Remark 8 is

$$\mathcal{N}(\sigma_{AA'B}) = \text{Tr}_{A'}[\Pi^{\text{sym}}_{AA'} \sigma_{AA'B} \Pi^{\text{sym}}_{AA'}], \tag{2.121}$$

with adjoint

$$\mathcal{N}^\dagger(\omega_{AB}) = \Pi^{\text{sym}}_{AA'} (\omega_{AB} \otimes I_{A'}) \Pi^{\text{sym}}_{AA'}. \tag{2.122}$$

Observe that the map $\rho_{AB} \mapsto \Pi^{\text{sym}}_{AA'} (\rho_{AB} \otimes I_{A'}) \Pi^{\text{sym}}_{AA'}$ is proportional to that used in a $1 \to 2$ universal cloning machine [106, Eq. (17)]. If ρ_{AB} is pure, so that we write it as ψ_{AB}, then the following inequality holds:

$$\left\| \Pi^{\text{sym}}_{AA'} (\psi_{AB} \otimes I_{A'}) \Pi^{\text{sym}}_{AA'} \right\|_\infty \leq \left\| \Pi^{\text{sym}}_{AA'} \right\|_\infty \| \psi_{AB} \otimes I_{A'} \|_\infty \left\| \Pi^{\text{sym}}_{AA'} \right\|_\infty \leq 1, \tag{2.123}$$

where we applied the multiplicativity of the spectral norm. Thus, the concave closure of $f(\rho_{AB})$ satisfies $f(\rho_{AB}) \in [0, 1]$. Furthermore, from Lemma 1 below, we know that

$$\left\| \Pi^{\text{sym}}_{AA'} (\psi_{AB} \otimes I_{A'}) \Pi^{\text{sym}}_{AA'} \right\|_\infty = \frac{1}{2} \left(1 + \| \psi_A \|_\infty \right), \tag{2.124}$$

showing the consistency of the claim just above (2.120) with Theorem 1 and Eqs. (2.8) and (2.10) in the main text. If ρ_{AB} is a pure product state, so that we can write it as $\rho_{AB} = \phi_A \otimes \varphi_B$, then we have that

$$\left\| \Pi^{\text{sym}}_{AA'} (\phi_A \otimes \varphi_B \otimes I_{A'}) \Pi^{\text{sym}}_{AA'} \right\|_\infty = \left\| \Pi^{\text{sym}}_{AA'} (\phi_A \otimes I_{A'}) \Pi^{\text{sym}}_{AA'} \right\|_\infty , \tag{2.125}$$

and the spectral norm on the right-hand side of (2.125) *is achieved by choosing the vector* $|\phi\rangle_A \otimes |\phi\rangle_{A'}$*, so that*

$$\begin{aligned}
&(\langle\phi|_A \otimes \langle\phi|_{A'})\Pi^{\mathrm{sym}}_{AA'}(\phi_A \otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}(|\phi\rangle_A \otimes |\phi\rangle_{A'}) \\
&= (\langle\phi|_A \otimes \langle\phi|_{A'})(\phi_A \otimes I_{A'})(|\phi\rangle_A \otimes |\phi\rangle_{A'}) \qquad (2.126)\\
&= 1. \qquad (2.127)
\end{aligned}$$

Lemma 1 *For a pure state* ψ_{AB}*, the following equality holds:*

$$\left\|\Pi^{\mathrm{sym}}_{AA'}(\psi_{AB} \otimes I_{A'})\Pi^{\mathrm{sym}}_{AA'}\right\|_\infty = \frac{1}{2}\left(1 + \|\psi_A\|_\infty\right), \qquad (2.128)$$

where $\psi_A \equiv \mathrm{Tr}_B[\psi_{AB}]$*.*

Proof. Consider that

$$\begin{aligned}
&\left\|\left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})\left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right)\right\|_\infty \\
&\qquad = \left\|(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})\left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})\right\|_\infty . \qquad (2.129)
\end{aligned}$$

Now consider that

$$\begin{aligned}
&(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})\left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}) \\
&= (|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})\left(\frac{I_{AA'} + F_{AA'}}{2} \otimes I_B\right)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}) \qquad (2.130)\\
&= \frac{1}{2}(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}) + \frac{1}{2}(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})(F_{AA'} \otimes I_B)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}) . \qquad (2.131)
\end{aligned}$$

Then writing the Schmidt decomposition of $|\psi\rangle_{AB}$ as $|\psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}|i\rangle_A|i\rangle_B$, we find that

$$(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})(F_{AA'} \otimes I_B)(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'})$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} \left(|\psi\rangle\langle i|_A \langle i|_B \otimes |j\rangle\langle j|_{A'}\right) \left(F_{AA'} \otimes I_B\right) \left(|i'\rangle_A |i'\rangle_B \langle\psi|_{AB} \otimes |j'\rangle\langle j'|_{A'}\right) \tag{2.132}$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} \left(|\psi\rangle\langle i|_A \langle i|_B \otimes |j\rangle\langle j|_{A'}\right) \left(|j'\rangle_A |i'\rangle_B \langle\psi|_{AB} \otimes |i'\rangle\langle j'|_{A'}\right) \tag{2.133}$$

$$= \sum_{i,i',j,j'} \sqrt{\lambda_i \lambda_{i'}} |\psi\rangle\langle i|j'\rangle_A \langle i|i'\rangle_B \langle\psi|_{AB} \otimes |j\rangle\langle j|i'\rangle\langle j'|_{A'} \tag{2.134}$$

$$= \sum_i \lambda_i |\psi\rangle\langle\psi|_{AB} \otimes |i\rangle\langle i|_{A'} \tag{2.135}$$

$$= |\psi\rangle\langle\psi|_{AB} \otimes \sum_i \lambda_i |i\rangle\langle i|_{A'} \tag{2.136}$$

$$= |\psi\rangle\langle\psi|_{AB} \otimes \psi_{A'}. \tag{2.137}$$

Then

$$\begin{aligned} &\left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \\ &= \frac{1}{2} \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) + |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \psi_{A'} \qquad (2.138) \\ &= |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \left(I_{A'} + \psi_{A'}\right), \qquad (2.139) \end{aligned}$$

and we conclude that

$$\begin{aligned} &\left\| \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \left(|\psi\rangle\langle\psi|_{AB} \otimes I_{A'}\right) \left(\Pi^{\mathrm{sym}}_{AA'} \otimes I_B\right) \right\|_\infty \\ &= \left\| |\psi\rangle\langle\psi|_{AB} \otimes \frac{1}{2} \left(I_{A'} + \psi_{A'}\right) \right\|_\infty \qquad (2.140) \\ &= \frac{1}{2} \left(1 + \|\psi_{A'}\|_\infty\right) \qquad (2.141) \\ &= \frac{1}{2} \left(1 + \|\psi_A\|_\infty\right). \qquad (2.142) \end{aligned}$$

This concludes the proof. ■

2.8.2 Placement of $\mathbf{QIP}_{\mathrm{EB}}(2)$

By placing the problem of estimating the fidelity of separability in the class $\mathrm{QIP}_{\mathrm{EB}}(2)$, we establish results that link quantum steering and the separability problem to quantum computational complexity theory. Furthermore, we show that the complexity class $\mathrm{QIP}_{\mathrm{EB}}(2)$ contains QAM [107] and QSZK [108]. It also follows, as a direct generalization of the hardness results from [21, 22], that the problem of estimating the fidelity of separability is hard for QSZK and NP. All of the aforementioned complexity classes are considered to be, in the worst case, out of reach of the capabilities of efficient quantum computers. See Figure 2.10 for a detailed diagram. However, following the approach of [109], we can try to solve some instances of problems in these classes using parameterized circuits and VQAs.

2.8.3 $\mathbf{QAM} \subseteq \mathbf{QIP}_{\mathrm{EB}}(2)$

First, recall that QAM consists of the verifier selecting a classical letter x uniformly at random, sending the choice to the prover, who then sends back a pure state ψ_x to the verifier, who finally performs an efficient measurement to decide whether to accept the computation [107]. Note that QAM contains QMA [107].

To see the containment $\mathrm{QAM} \subseteq \mathrm{QIP}_{\mathrm{EB}}(2)$, consider that the verifier's first circuit in $\mathrm{QIP}_{\mathrm{EB}}(2)$ can consist of preparing a random classical bitstring in a system R.

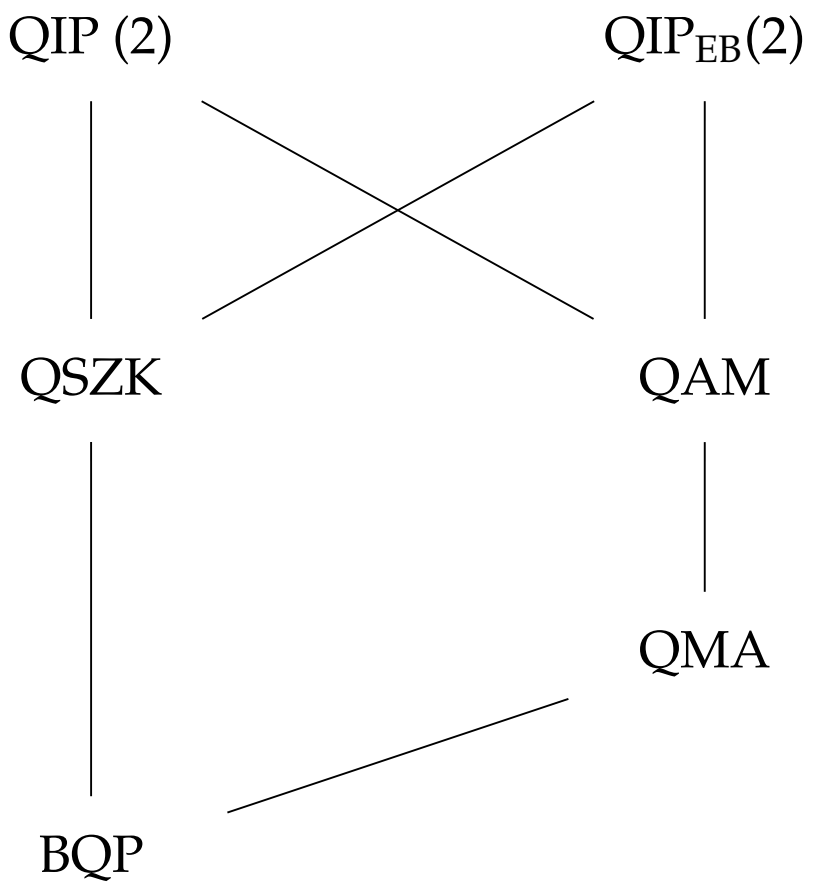


Figure 2.10: Placement of QIP$_{EB}$(2) relative to other known complexity classes. The complexity classes are organized such that if a class is connected to a class above it, the complexity class placed lower is a subset of the class above. For example, QIP$_{EB}$(2) is a superset of both QSZK and QAM.

The verifier sends system R to the prover. Then, the prover's action amounts to preparing some state that gets returned to the verifier. The rest of the protocol then simulates a QAM protocol.

2.8.4 QSZK $\subseteq$ QIP$_{\text{EB}}(2)$

Quantum statistical zero-knowledge (QSZK) consists of all problems that can be solved by the interaction between a quantum verifier and a quantum prover, such that the verifier accumulates statistical evidence about the answer to a decision, but does not learn anything other than the answer by interacting with the prover [110, 108]. A complete problem for this class is quantum state distinguishability, in which the goal is to decide whether two states ρ_0 and ρ_1, generated by quantum circuits, are far or close in trace distance [110]. This is a nice problem for understanding the basics of the QSZK complexity class: the interaction begins with the verifier picking one of the states uniformly at random, recording the choice as a bit x, and then sending the chosen state ρ_x to the prover over a quantum channel. The prover can then perform the optimal Helstrom measurement [111, 112] to distinguish the states, which has success probability equal to

$$p_{\text{succ}} \coloneqq \frac{1}{2}\left(1 + \frac{1}{2}\left\|\rho_0 - \rho_1\right\|_1\right). \tag{2.143}$$

The Helstrom measurement leads to a decision bit y, which the prover sends back to the verifier over a quantum channel (here, a single classical bit channel would suffice). The verifier then accepts if $x = y$, and the probability that this happens is

equal to p_{succ}. By repeating this protocol a polynomial number of times and invoking the error-reduction protocol from [110], it follows that the verifier can make the completeness and soundness probabilities exponentially close to one and zero, respectively, to have essentially zero error probability in the final decision about whether the states are near or far in trace distance. Finally, the interaction has a "zero knowledge" aspect because the verifier only learns the bit of the prover and nothing about how to distinguish the states.

Since quantum state distinguishability is a complete problem for QSZK and the interaction described above can be performed in $\text{QIP}_{\text{EB}}(2)$, the containment $\text{QSZK} \subseteq \text{QIP}_{\text{EB}}(2)$ follows.

2.9 Conclusion and Discussion

In this chapter, we detailed a distributed quantum computation to test the separability of a quantum state that, at its core, uses quantum steering. This test demonstrated a link between quantum steering and the separability problem. The acceptance probability of this distributed quantum computation is directly related to an entanglement measure known as the fidelity of separability. Using the test's structure, we also showed computational complexity-theoretic results and established a link between quantum steering, quantum algorithms, and quantum computational complexity. By replacing the prover with a parameterized circuit, we modified this distributed quantum computation to develop our variational quan-

tum steering algorithm (VQSA), a novel kind of variational quantum algorithm that uses quantum steering to address the problem of estimating the fidelity of separability. This algorithm allows for the direct estimation of the fidelity of separability without the need for state tomography and subsequent approximate tests on separability. Our algorithm is not unitary due to the mid-circuit measurement on system R and the consequent conditional operation applied on system A. This is an important distinction from most VQAs, which do not use a parameterized mid-circuit measurement. We also discuss multipartite generalizations of both our separability test and VQSA. Finally, we simulated our VQSA using the noisy Qiskit Aer simulator [113], which showed favorable convergence trends and was compared against two classical SDP benchmarks.

Our VQSA has applications beyond entanglement quantification on a single quantum computer. We can also think of our VQSA as a distributed variational quantum algorithm for measuring the entanglement of a bipartite state. See [114, 115, 116] for previous instances of distributed VQAs. Indeed, our algorithm can be executed over a quantum network, in which each node has quantum and classical computers capable of performing VQAs. The initial part of the algorithm distributes R to Rob, A to Alice, and B to Bob, who are all in distant locations. Then, Rob performs the parameterized measurement and sends the outcome over a classical channel to Alice, who performs another parameterized measurement. They can repeat this process to assess the quality of the entanglement between Alice and Bob. This interpretation is even more interesting regarding quantum networks for the multipartite case, in which the classical data gets broadcast from

Rob to all the other nodes except the last one.

VQSAs can tackle other problems involving quantum steering, like maximizing the pure-state decompositions of quantum states. This technique may also be helpful in estimating other entanglement measures that involve optimizing over the set of separable states. By applying the insights of [88, Appendix A] and our approach here, it is clear that VQSAs will also help estimate maximal fidelities associated with other resource theories, such as the resource theory of coherence [117]. More broadly, we suspect that the paradigm of parameterized mid-circuit measurements and distributed variational quantum algorithms will help address other computational problems of interest in quantum information science and physics, given recent advances in experimental implementations [118, 119, 120, 121].

2.9.1 Software

All of our Python source files are available with the arXiv posting of [122]. We performed all simulations using the noisy Qiskit Aer simulator. The Picos Python package [123] was used to invoke the CVXOPT solver [124] for solving the SDPs, and the toqito Python package [125] was used for carrying out specific operations on the matrices representing quantum systems.

CHAPTER 3

DEVICE-INDEPENDENT CERTIFICATION OF MULTIPARTITE DISTILLABLE ENTANGLEMENT

3.1 Introduction

Quantum networks may become a reality within the near future and have the potential to open up several avenues of applications. Potential uses for quantum networks include quantum computers connected together for distributed computing tasks [7, 8], a collection of quantum sensors that implement a joint measurement on a system of interest [9, 10, 11, 12], or a number of distant nodes that transmit quantum states among themselves [13, 14, 47]. To realize the full potential of quantum networks, the efficient production and distribution of multipartite entanglement is essential [15].

To distribute multipartite entanglement over large distances, one can choose two basic approaches. The first approach involves distributing bipartite entanglement between each of the nodes and then using local operations and classical communication to convert the global state into a desired multipartite state [126, 127]. The alternate method involves producing the multipartite state of interest at a single location [128] and distributing the resulting state via quantum channels to the intended recipients. Whichever procedure one might employ, it is important to study the associated success probability and quality of entanglement yielded by

these procedures.

This point raises the question: how can we certify or guarantee that a minimum amount of entanglement is produced by a certain procedure or method? This question becomes more interesting when we recall that quantum networks may have components based on different architectures: for example, superconducting qubits for computing [129, 130, 131], trapped ions [132] or solid-state qubits [133] for memory, photons for communication [128], and so on. Hence, we need to adopt a framework of certification that is independent of the constituent parts of the quantum network, thus bringing us to device-independent (DI) protocols.

The general interest in DI protocols [134, 135] stems from the fact that one can test and verify the amount of entanglement in a state using only classical inputs and outputs, along with classical communication. DI protocols are based on various self-testing results [39, 136, 137, 138], the first of which were developed in [39]. (See [139] for a review.) Most importantly, such protocols are agnostic to the underlying mechanics and specifics of the state being tested. As such, and relevant to the present chapter, DI protocols are suitable for the certification of multipartite entanglement in quantum networks, especially ones that contain elements with dissimilar underlying technologies.

There has been a lot of recent interest in device-independent protocols involving more than two parties, including investigations into Bell-type inequalities [140, 141] and their application toward DI conference key agreement, involv-

ing achievable rates [3, 50] and upper bounds on key-agreement rates [142, 143]. However, little attention has been paid toward the device-independent certification of multipartite distillable entanglement. Multipartite entanglement distillation is an important step to ensure that we are using states that are as close as possible to ideal states.

In this chapter, we provide a lower bound on the certifiable rate of one-shot multipartite distillable entanglement in a device-independent setting. The multipartite Greenberger–Horne–Zeilinger (GHZ) state is the basic entanglement resource that is critical to maximizing the utility of quantum networks for applications like quantum sensing [9, 10, 11, 12], multi-party quantum communication [13, 14, 47], and distributed quantum computation [7, 8]. It is vital to distill GHZ states from less-than-perfect multipartite states that are available to the parties in a quantum network, while using only minimal additional resources like local operations and classical communication (LOCC). To maximize the utility of every copy of an available multipartite state, we need to look at the one-shot distillable entanglement of the state shared by the quantum network. The device-independent setting means that all the conclusions are drawn from only the classical inputs and outputs of the protocol, along with the assumption of the completeness and correctness of quantum mechanics [39, 136, 137]. In other words, the conclusions hold true regardless of the precise inner workings of the experimental devices.

In more detail, we extend DI entanglement distillation certification from the

bipartite scenario [144] to the multipartite scenario. In what follows, we first give a detailed description and definition of what we mean by DI multipartite entanglement distillation. In Section 3.2, we define a DI, M-partite entanglement distillation certification protocol, which consists of completeness and soundness conditions. In Section 3.3, we provide a detailed description of a proposed protocol. Our proposed protocol is centered around the Mermin–Ardehali–Belinskii–Klyshko (MABK) inequality [41, 42, 43], which is critical to proving the completeness condition. We show in Section 3.4 that the proposed protocol is complete. Thereafter, in Section 3.5, we proceed to proving that it is sound, by making use of the entropy accumulation theorem [145] and the structure of the MABK inequality [45].

3.2 Definitions and Setup

In this section, we provide several definitions that we use throughout the rest of the chapter, including the GHZ orthonormal basis, the one-shot multipartite distillable entanglement of a multipartite quantum state, an entanglement distillation certification protocol, and basic entropies.

Definition 6 *The GHZ orthonormal basis for the set of M-qubit states is composed of the following 2^M states:*

$$|\psi_{v,u}\rangle := \frac{1}{\sqrt{2}}\left[|0,u\rangle + (-1)^v|1,\bar{u}\rangle\right], \tag{3.1}$$

where $v \in \{0,1\}$, *while* $u \in \{0,1\}^{M-1}$ *and* $\bar{u} = \mathbf{1} \oplus u$ *are* $M-1$ *bit strings, with* $\mathbf{1}$ *the all-ones bit vector of size* $M-1$.

The one-shot multipartite distillable entanglement of a state quantifies the amount of multipartite entanglement that we can distill from a single copy of the state. It is defined formally as follows:

Definition 7 (Multipartite distillable entanglement) *Let* $\varepsilon \in [0,1]$. *The one-shot distillable M-partite entanglement* $E_D^{\varepsilon}(\rho_{A_{[M]}})$ *of a multipartite state* $\rho_{A_{[M]}} \equiv \rho_{A_1 \cdots A_M}$ *is defined as*

$$E_D^{\varepsilon}(\rho_{A_{[M]}}) \coloneqq \sup_{\substack{d \in \mathbb{N}, \\ \mathcal{L} \in \mathrm{LOCC}}} \left\{ \log_2 d : F\left(\mathcal{L}_{A_{[M]} \to \hat{A}_{[M]}}(\rho), \Phi^d_{\hat{A}_{[M]}} \right) \geq 1 - \varepsilon \right\}, \tag{3.2}$$

where the optimization is over every LOCC channel $\mathcal{L}_{A_{[M]} \to \hat{A}_{[M]}}$, *the fidelity is defined as* $F(\rho, \sigma) \coloneqq \left\| \sqrt{\rho}\, \sqrt{\sigma} \right\|_1^2$, *and* $\Phi^d_{\hat{A}_{[M]}} \equiv |\Phi^d\rangle\langle\Phi^d|_{\hat{A}_{[M]}}$ *is an M-party, rank-d GHZ state, with*

$$|\Phi^d_{\hat{A}_{[M]}}\rangle \coloneqq \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{A_1} \cdots |i\rangle_{A_M}. \tag{3.3}$$

The asymptotic distillable entanglement is defined in terms of the following limit:

$$E_D(\rho_{A_{[M]}}) \coloneqq \inf_{\varepsilon \in (0,1)} \liminf_{n \to \infty} \frac{1}{n} E_D^{\varepsilon}(\rho^{\otimes n}_{A_{[M]}}). \tag{3.4}$$

Since our goal is to quantify multipartite distillable entanglement in a device-independent setting, we want to be able to make statements about the aforementioned quantity that hold regardless of the physical systems involved. In other words, we want to bound this quantity in a device-independent setting.

Let us take a closer look at what this means. To begin with, suppose that all parties $A_1, \ldots, A_M$ are given a share of a multipartite quantum state $\rho_{A_1 \cdots A_M}$, which is distributed to them by a possibly unknown entity. Each party also has access to a black box with which they can interact classically. For each classical input, the corresponding black box applies a positive operator-valued measure (POVM) on its respective share of the multipartite state. After the application of the POVM, the box outputs a classical value that is recorded by the corresponding participant. The parties can use the results of the measurements to complete certain tasks of their choosing. If they use only the inputs and outputs from the black box to complete their task, they will have completed the task independent of the underlying physical realization of the measurement and states shared among them. This is the idea behind device independence.

We now define what we mean by a device-independent (DI) protocol for certifying a rate of one-shot distillable multipartite entanglement. Our definition for a DI M-partite entanglement distillation certification (DIMEC) protocol is based on the definition of a DI entanglement certification protocol in [144], defined therein for two parties.

Definition 8 (DIMEC protocol) *Let $n \in \mathbb{N}$, let ε_{smo}, ε_{snd}, $\varepsilon_{\text{cmp}} \in [0, 1]$, and let $r \geq 0$ be a threshold M-partite distillation rate. Furthermore, let $\mathcal{S}^{\text{honest}}$ be a set of "honest" states, each of which is denoted by ϕ^{honest}. Let $\mathcal{D}^{\text{honest}}$ be the set of "honest" measurement devices. Let $\mathcal{P}$ be a protocol employing only multipartite LOCC, which, upon being given a state $\sigma \in \mathcal{D}\big(\bigotimes_{i=1}^{M} \mathcal{H}_{A_i}^{\otimes n}\big)$, creates a state $\rho \in \mathcal{D}\big(\bigotimes_{i=1}^{M} \mathcal{H}_{A_i}^{\otimes n}\big)$. Let $\rho_{|\Omega}$ denote the final state*

conditioned on the protocol not aborting.

A protocol $\mathcal{P}$ is said to be a DI M-partite entanglement distillation certification (DIMEC) protocol if the following conditions hold:

1. *Noise tolerance (completeness): The probability that $\mathcal{P}$ aborts when applied on $\phi^{\text{honest}} \in \mathcal{S}^{\text{honest}}$ using a measurement device from $\mathcal{D}^{\text{honest}}$ is at most ε_{cmp}.*
2. *Entanglement certification (soundness): For every source σ and measurement device, either $E_D^{n,\varepsilon_{\text{snd}}}(\rho_{|\Omega}) \geq r$ or $\mathcal{P}$ aborts with probability greater than $1 - \varepsilon_{\text{smo}}$ when applied on σ.*

To design a protocol and show that it satisfies all the conditions in Definition 8, we need to use some information-theoretic quantities. Here we recall the definitions of von Neumann entropy, coherent information, and smooth conditional max-entropy.

Definition 9 *The von Neumann entropy $H(A)_\rho$ of a state ρ_A is defined as follows:*

$$H(A)_\rho := -\operatorname{Tr}[\rho_A \log_2 \rho_A]. \tag{3.5}$$

Definition 10 *The coherent information $I(A\rangle B)_\rho$ of a bipartite state ρ_{AB} is defined as follows:*

$$I(A\rangle B)_\rho := H(B)_\rho - H(AB)_\rho = -H(A|B)_\rho, \tag{3.6}$$

where $H(B)_\rho$ is the von Neumann entropy of $\rho_B = \operatorname{Tr}_A[\rho_{AB}]$ and $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$ is the quantum conditional entropy of the state ρ_{AB}.

Definition 11 ([146]) *The smooth conditional max-entropy of a bipartite state ρ_{AB} is defined for all $\varepsilon \in (0,1)$ as*

$$H_{\max}^{\varepsilon}(A|B)_{\rho} \coloneqq \inf_{\tilde{\rho} \in \mathcal{D}_{\leq}} H_{\max}(A|B)_{\rho}, \tag{3.7}$$

where

$$\mathcal{D}_{\leq} \coloneqq \{\omega \geq 0 : \mathrm{Tr}[\omega] \leq 1\}, \tag{3.8}$$

$\tilde{\rho}$ is such that $\sqrt{1 - F(\rho, \tilde{\rho})} \leq \varepsilon$, $H_{\max}(A|B)_{\rho} \coloneqq \sup_{\sigma_B} \log_2 F(\rho_{AB}, \mathbb{I}_A \otimes \sigma_B)$, and $F(\rho, \sigma) \coloneqq \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1^2$ is the fidelity.

3.3 Device-Independent Multipartite Entanglement Certification Protocol

Before introducing our proposed DIMEC protocol, first we need to discuss the MABK inequality [41, 42, 43]. Let x_i denote an input to the ith measurement device, and let a_i denote the outcome of a measurement, where $i \in \{1, \ldots, M\}$ and M is the number of parties involved. We can then define the MABK inequality as follows.

Definition 12 *Let $\hat{O}_0^i$ and $\hat{O}_1^i$ be binary observables for all $i \in [M]$. The M-partite MABK operator, $\mathcal{K}_M$, is defined by the following recursion relation:*

$$\mathcal{K}_M \coloneqq \frac{1}{2}\mathcal{F}(\mathcal{K}_{M-1}, \overline{\mathcal{K}}_{M-1}, \hat{O}_0^M, \hat{O}_1^M), \tag{3.9}$$

$$\mathcal{K}_2 \coloneqq \frac{1}{2}\mathcal{F}(\hat{O}_0^1, \hat{O}_1^1, \hat{O}_0^2, \hat{O}_1^2), \tag{3.10}$$

where $\overline{\mathcal{K}}_{M-1}$ *is obtained from* $\mathcal{K}_{M-1}$ *by exchanging* $\hat{O}_0^i$ *and* $\hat{O}_1^i$ *for all* $i \in [M]$ *and*

$$\mathcal{F}(\hat{B}_0, \hat{B}_1, \hat{C}_0, \hat{C}_1) := \hat{B}_0 \otimes \left(\hat{C}_0 + \hat{C}_1\right) + \hat{B}_1 \otimes \left(\hat{C}_0 - \hat{C}_1\right). \tag{3.11}$$

The M*-partite MABK inequalities are then defined for all* $M \geq 2$ *as*

$$2^{\frac{4-M}{2}} \left|\mathrm{Tr}\left[\mathcal{K}_M \rho_{\hat{A}_{[M]}}\right]\right| \leq 2^{\frac{m-M+3}{2}}, \quad m \in [M]. \tag{3.12}$$

The MABK inequalities are such that a violation of the inequalities for $m = 1$ proves that at least two parties are entangled, the violation of the inequalities for $m = M - 1$ proves genuine M-partite entanglement, and the case where $m = M$ gives an upper bound (tight) on what is achievable by quantum mechanics. In this work, we are interested in $m = M - 1$ and $m = M$, which correspond to

$$\beta_M := 2^{\frac{4-M}{2}} \left|\mathrm{Tr}\left[\mathcal{K}_M \rho_{\hat{A}_{[M]}}\right]\right| \in [2, 2\sqrt{2}]. \tag{3.13}$$

The CHSH inequality corresponds to

$$\beta_2 := 2 \left|\mathrm{Tr}\left[\mathcal{K}_2 \rho_{\hat{A}_{[2]}}\right]\right| \in [2, 2\sqrt{2}]. \tag{3.14}$$

For our purposes, we need to turn the MABK inequality into a game. This can be done using the procedure outlined in [44]. By unraveling the recursion in (3.9)–(3.10), we can rewrite the M-MABK operator as

$$\mathcal{K}_M = 2^{-2\lfloor \frac{M}{2} \rfloor} \sum_{x \in \{0,1\}^M} (-1)^{f(x)} \bigotimes_{i \in [M]} \hat{O}_{x_i}^i, \tag{3.15}$$

where $x_i \in \{0, 1\}$ is the ith bit of x and $f : \{0, 1\}^M \to \{0, 1, \perp\}$ is a function such that $(-1)^\perp = 0$ by convention.

For the MABK game, the M parties have two measurement settings each, denoted by $x_i \in \{0, 1\}$, and all measurements have two possible outcomes, denoted by $a_i \in \{0, 1\}$. Then the winning condition for the MABK game is as follows [45]:

$$\text{win}(x_{[M]}, a_{[M]}) := \begin{cases} 1, & \text{if } \bigoplus_{i=1}^{M} a_i = f(x_{[M]}) \\ 0, & \text{else} \end{cases}, \tag{3.16}$$

where f is defined by the M-MABK operator in (3.15). The minimum and maximum winning probabilities when the underlying state is genuinely multipartite entangled are respectively as follows [45]:

$$p_{\text{min}} := 2^{2\lfloor \frac{M}{2} \rfloor - M - 1} + 2^{\lfloor \frac{M}{2} \rfloor - \frac{M}{2} - 2}, \tag{3.17}$$

$$p_{\text{max}} := 2^{2\lfloor \frac{M}{2} \rfloor - M - 1} + 2^{\lfloor \frac{M}{2} \rfloor - \frac{M}{2} - \frac{3}{2}}. \tag{3.18}$$

Note that when M is even,

$$p^e_{\text{min}} = 3/4 \quad \text{and} \quad p^e_{\text{max}} = (2 + \sqrt{2})/4. \tag{3.19}$$

Similarly when M is odd,

$$p^o_{\text{min}} = (2 + \sqrt{2})/8 \quad \text{and} \quad p^o_{\text{max}} = 1/2. \tag{3.20}$$

Based on the MABK game defined above, we propose Protocol 1. There are two types of rounds in Protocol 1: a testing round, where the parties play the MABK game and record the result, and a storage round, where the parties simply store the state they receive in a quantum memory. At the beginning of each round, we choose between these types uniformly random. The main result of this chapter is that Protocol 1 is a DIMEC protocol, satisfying the requirements of Definition 8, and we state this result formally in Theorem 18.

Protocol 1: : DIMEC protocol based on the MABK game

Arguments:

$\mathcal{M}$ – untrusted measurement device, with inputs and outputs in the set $\{0, 1\}$

$n \in \mathbb{N}_+$ – number of rounds

γ – the probability of conducting a test

ω_{exp} – expected winning probability in the MABK game

$\delta_{\text{est}} \in (0, 1)$ – width of the statistical confidence interval for the estimation test

$A_{i,j}$ indicates a classical register belonging to the i-th party and j-th round.

1: For every round $j \in [n]$, do steps 2-10:

2: Let ϕ^j denote the multipartite state produced by the source in this round.

3: Set $A_{i,j}, X_{i,j}, W_j = \perp$ for all $i \in [M]$.

4: Choose $T_j = 1$ with probability γ and $T_j = 0$ with probability $1 - \gamma$.

5: If $T_j = 1$:

6: Choose inputs $X_{i,j} \in \{0, 1\}$ uniformly at random.

7: Measure ϕ^j using $\mathcal{M}$ with the inputs $X_{i,j}$ and record outputs $A_{i,j} \in \{0, 1\}$.

8: Set $W_j = 1$ if the MABK game is won and $W_j = 0$ otherwise.

9: If $T_j = 0$:

10: Keep ϕ^j in the registers $\bigotimes_{i=1}^{m} \hat{A}_{i,j}$.

11: Abort if $W := \sum_{j=1}^{n} \chi(T_j = 1)\, W_j < (\omega_{\text{exp}}\gamma - \delta_{\text{est}}) \cdot n$.

3.4 Completeness

In this section, we show that Protocol 1 is complete. To prove the completeness condition in Definition 8, we need to show that our protocol applied to an arbitrary $\phi^{\text{honest}} \in \mathcal{S}^{\text{honest}}$ aborts with only a small probability. We prove this result in the following theorem.

Theorem 10 *The following bound holds:*

$$\varepsilon_{\text{cmp}} \leq \exp\left(-2n\delta_{\text{est}}^2\right), \tag{3.21}$$

implying that the probability that Protocol 1 aborts for $\phi^{\text{honest}} \in \mathcal{S}^{\text{honest}}$ *is no larger than* $\exp\left(-2n\delta_{\text{est}}^2\right)$.

Proof. Protocol 1 aborts when W, the estimator for the MABK game winning probability, is not high enough. This happens when the MABK violation is not large or if the number of samples is not sufficiently large. Whenever $\phi^{\text{honest}} \in \mathcal{S}^{\text{honest}}$ and the rounds are independent and identically distributed (IID), i.e., an honest implementation, the sequence $\left(\chi(T_j = 1)\, W_j\right)_{j=1}$ is a sequence of IID random variables. Using Hoeffding's inequality [147], we conclude that

$$\varepsilon_{\text{cmp}} = \Pr\left(W \leq (\omega_{\text{exp}}\gamma - \delta_{\text{est}}) \cdot n\right) \leq e^{-2n\delta_{\text{est}}^2}, \tag{3.22}$$

completing the proof. ■

3.5 Soundness

In this section, we prove the soundness of Protocol 1. To do so, we need to show that the protocol ensures a minimum amount of multipartite distillable entanglement or aborts with high probability. First, we briefly discuss a protocol to distill multipartite entanglement from a mixed state. We will use this achievable rate of multipartite distillable entanglement to prove the soundness of Protocol 1.

Consider the following setting: a pure state $\psi_{A_1 \cdots A_M BR}$ is held by $M + 2$ parties, with the ith sender holding A_i, for $i \in \{1, \ldots, M\} =: [M]$, one receiver holding B, and a reference system holding R, which serves as a purifying system. Additionally, Alice-i and Bob share a maximally entangled state $\Phi(c_i)_{A'_i B'_i}$ of Schmidt rank $c_i \in \mathbb{N}$, and so the initial overall state is

$$\psi_{A_1 \cdots A_M BR} \otimes \Phi(c_1)_{A'_1 B'_1} \otimes \cdots \otimes \Phi(c_M)_{A'_M B'_M}. \tag{3.23}$$

Multiparty state merging is an LOCC protocol that transforms this initial state to

$$\psi_{\hat{A}_1 \cdots \hat{A}_M \hat{B} R} \otimes \Phi(d_1)_{A''_1 B''_1} \otimes \cdots \otimes \Phi(d_M)_{A''_M B''_M}, \tag{3.24}$$

such that all of the systems $\hat{A}_1 \cdots \hat{A}_M \hat{B}$ are in Bob's possession. (For details, see Section 6.3 of [148].) If $c_i > d_i$, then the protocol consumes $\log_2 c_i - \log_2 d_i$ ebits shared between A_i and B. If $c_i < d_i$, then the protocol produces $\log_2 d_i - \log_2 c_i$ ebits, which are shared between A_i and B (recall that the term "ebit" is synonymous with the standard Bell pair). If the protocol distills ebits between each Alice, $A_1 \cdots A_M$, and Bob B, then they can apply LOCC to convert several copies of their ebits into multipartite GHZ states.

For a one-shot realization of the entire process of using LOCC to convert $\psi_{A_1 \cdots A_M BR}$ into a GHZ state, we need only understand the one-shot behavior of the state merging step. The theorem needed for the state merging step is as follows:

Theorem 11 (Theorem 6.15 of [148]) *Given the setting above, quantum state merging can be achieved successfully, in the sense that the fidelity constraint in (3.2) holds, for* $\varepsilon = 8 \cdot 3^{M/2} \sqrt{\varepsilon'} \in (0, 1)$, *if for all* $K \subseteq [M]$ *such that* $K \neq \emptyset$,

$$\sum_{k \in K} (\log_2 d_k - \log_2 c_k) \leq -H_{\max}^{\varepsilon'}(A_K | A_{K^c} B)_\psi + 2 \log \varepsilon'. \tag{3.25}$$

Using the above theorem and the steps elucidated earlier, we conclude the following:

Theorem 12 (Theorem 9 of [149]) *Let* $\rho_{A_1 \cdots A_M}$ *be a state held by m parties. The following is an achievable rate for GHZ distillation under LOCC:*

$$\max_{k \in [M]} \left\{ \min_{K \subseteq [M] \setminus k} \frac{I(A_K \rangle A_{[M] \setminus K})_\rho}{|K|} \right\}, \tag{3.26}$$

where $I(A\rangle B)_\theta$ *is the coherent information of a state* θ_{AB}.

The statement above gives a bound only on the asymptotic rate of GHZ distillation from mixed states. For our purpose, we require a lower bound on $\frac{1}{n} E_D^{\varepsilon}(\rho_{A_{[M]}}^{\otimes n})$. The following proposition gives such a bound by making use of the developments of [148, 149].

Proposition 5 *Let $\rho_{A_1\cdots A_M}$ be held by m parties. Fix $\varepsilon' > 0$ such that $\varepsilon := 8 \cdot 3^{M/2} \sqrt{\varepsilon'} \in (0,1)$. Then the following is an achievable one-shot rate for GHZ distillation under LOCC; i.e.,*

$$\frac{1}{n} E_D^{\varepsilon}(\rho_{A_{[M]}}^{\otimes n}) \geq \max_{k \in [M]} \left\{ \min_{K \subseteq [M]\setminus k} \frac{-H_{\max}^{\varepsilon'}(A_K|A_{[M]\setminus K})_\rho}{|K|} \right\} + \frac{2\log \varepsilon'}{M-1}. \tag{3.27}$$

Proof. To achieve this one-shot rate, we can use the protocol outlined in [149, Theorem 9] but without time sharing. Time shared decoding is replaced with simultaneous decoding, as the former is not possible in the one-shot setting. We obtain achievable rates for the one-shot case by replacing coherent information in (3.26) with the conditional smooth max-entropy. This leaves us with an expression commensurate with (3.25) in Theorem 11. ■

3.5.1 Entropy Accumulation Theorem (EAT)

To certify that a minimum amount of multipartite entanglement can be distilled from the states left over at the end of n rounds of Protocol 1, we need to lower bound $-H_{\max}^{\varepsilon}\left(A_K^{\otimes n}|A_{[M]\setminus K}^{\otimes n}\right)_{\rho^{\otimes n}}$. Since this is a finite-length protocol, and we are interested in a smooth entropic quantity, we can use Entropy Accumulation Theory (EAT) to obtain a rate r in terms of the desired error constants. To apply EAT, one needs to define "EAT channels," which describe the sequential process under consideration, and max-tradeoff functions. In our case, the sequential process results from our protocol for the certification of multipartite entanglement distillation.

For a sequential process like our protocol, the most restrictive relation between the rounds is to assume that they are IID. However, such a restriction is arguably too strong for the device-independent scenario. Entropy accumulation theory allows for a more general relation between the rounds of our protocol. This is encapsulated in the following definition of EAT channels.

Definition 13 (EAT channels [145]) *An EAT channel $\mathcal{N}_j : R_{j-1} \to R_j O_j S_j W_j$, for $j \in [n]$, is a CPTP map, such that, for all $j \in [n]$:*

1. *W_j is a finite-dimensional classical system. S_j and R_j are arbitrary quantum systems.*
2. *Given an input state $\sigma_{R_{j-1}}$, the output state $\sigma_{R_j O_j S_j W_j} = \mathcal{N}_j\left(\sigma_{R_{j-1}}\right)$ has the property that one can perform a quantum instrument on the systems $O_j S_j$ (in the state $\sigma_{O_j S_j}$), obtain the classical register W_j, and discard it, without changing the state $\sigma_{O_j S_j}$. That is, for the instrument $\mathcal{T}_j : O_j S_j \to O_j S_j W_j$ describing the process of obtaining W_j from O_j and S_j, it holds that $(\mathrm{Tr}_{W_j} \circ \mathcal{T}_j)\left(\sigma_{O_j S_j}\right) = \sigma_{O_j S_j}$.*
3. *O_j is a finite-dimensional quantum system of dimension d_{O_j}.*

If the rounds are not IID, then we cannot consider a round of the protocol to be completely independent of the preceding rounds. In other words, we cannot use the additivity property of the quantities under consideration. To resolve this, entropy accumulation theory requires that a special function, associated with our protocol, be found. This special function is called the max-tradeoff function.

To define max-tradeoff functions, we need to clarify some notation, which we will use henceforth. Given a value $w = (w_1, \ldots, w_n) \in \mathcal{W}^n$, where $\mathcal{W}$ is a finite alphabet, we denote by freq_w the probability distribution over $\mathcal{W}$ defined by $\text{freq}_w(\tilde{w}) := \frac{|\{j \,|\, w_j = \tilde{w}\}|}{n}$ for $\tilde{w} \in \mathcal{W}$. If τ is a state classical on W, we write $\Pr[w]_\tau$ to denote the probability that τ assigns to w. Now, we move on to the definition of max-tradeoff functions.

Definition 14 (Max-tradeoff function [145]) *Let $\mathcal{N}_1, \ldots, \mathcal{N}_n$ be a family of EAT channels. Let $\mathcal{W}$ denote the common alphabet of $W_1, \ldots, W_n$. A concave [1] function $f_{\max}$ from the set of probability distributions p over $\mathcal{W}$ to the real numbers is called a max-tradeoff function for $\{\mathcal{N}_j\}_j$ if it satisfies*

$$f_{\max}(p) \geq \sup_{\sigma} \left\{ H\left(O_j \middle| S_j\right)_{\mathcal{N}_j(\sigma)} : \text{Tr}_{R_j O_j S_j}[\mathcal{N}_j(\sigma)] = p \right\}, \tag{3.28}$$

for all $j \in [n]$, where the supremum is taken over all input states of $\mathcal{N}_j$ for which the marginal on W_j of the output state is the probability distribution p.

The statement of the EAT, relevant for the smooth max-entropy, is given below (see [145, Theorem 4.4] and Eq. (A.2) of [150, Appendix A]).

Theorem 13 ([145, 150]) *Let $\mathcal{N}_j : R_{j-1} \to R_j O_j S_j W_j$ for $j \in [n]$ be a sequence of EAT channels as in Definition 13, $\tau_{OSW} = (\text{Tr}_{R_n} \circ \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1)(\tau_{R_0})$ the final state, Ω an event*

[1] Let $\hat{\Omega}$ be a set of frequencies defined via $\text{freq}_w(\tilde{w}) \in \hat{\Omega}$ if and only if $\tilde{w} \in \Omega$. We can consider concave functions, in contrast to affine ones [145], since the event Ω defined in the current work results in a convex set $\hat{\Omega}$.

defined over $\mathcal{W}^n$ *indicating acceptance,* $\Pr[\Omega]_\tau$ *the probability of acceptance given the underlying state* τ*, and* $\tau_{|\Omega}$ *the final state conditioned on* Ω*.*

Let $\varepsilon_{\text{smo}} \in (0,1)$*. For* $f_{\max}$ *a max-tradeoff function for* $\{\mathcal{N}_j\}_j$*, as in Definition 14, and all* $t \in \mathbb{R}$ *such that* $f_{\max}(\text{freq}_w) \leq t$ *for all* $w \in \mathcal{W}^n$ *for which* $\Pr[w]_{\tau_{|\Omega}} > 0$*, the following holds:*

$$H_{\max}^{\varepsilon_{\text{smo}}}(O|S)_{\tau_{|\Omega}} \leq nt + v\sqrt{n}\,, \tag{3.29}$$

where d_{O_i} *denotes the dimension of* O_i *and*

$$v := 2\left(\log_2(1+2d_{O_i}) + \lceil \|\nabla f_{\max}\|_\infty \rceil\right)\sqrt{1 - 2\log_2(\varepsilon_{\text{smo}} \cdot \Pr[\Omega]_\tau)}. \tag{3.30}$$

It has been shown that Theorem 13, the generalized entropy accumulation theorem, holds regardless of whether the sequence of channels $\{\mathcal{N}_j\}_j$ satisfies a Markov-chain condition [150, Appendix A]. Note that the original entropy accumulation theorem [145] does require such a Markov-chain condition.

3.5.2 EAT Channels

In this subsection, we prove that Protocol 1, for all $j \in [n]$, satisfies the conditions for EAT channels, $\mathcal{N}_j : R_{j-1} \to R_j O_j S_j W_j$ as outlined in Definition 13. This is a necessary condition for the application of the entropy accumulation theorem [145].

Consider Condition 1 of Definition 13. We can think of R_j as a source distributing the states across the network. As far we are concerned, it is an arbitrary

quantum system. W_j is the classical register associated with determining whether the MABK game has been won. W_j is finite dimensional, as it can take only three values. S_j consists of all the systems involved in the protocol, except for the system $\hat{A}_{[M'],j}$ for some $M' \in [M-1]$.

For Condition 2 of Definition 13, we can see that W_j is determined using only the classical values $A_{i,j}$ and $X_{i,j}$ and does not affect the classical and quantum registers.

Finally, we are left with Condition 3 of Definition 13. Checking these conditions is more involved. First, we note that Protocol 1 makes use of the MABK inequality, which involves two inputs and two outputs for all parties involved. This allows us to apply Jordan's lemma on every party. Now, we recall Jordan's lemma [151]:

Theorem 14 (Lemma 4.1 in [151]) *Let $\hat{O}_0$ and $\hat{O}_1$ be two Hermitian operators with eigenvalues -1 and $+1$. Then there exists a basis in which both operators are block diagonal, in blocks of dimension 2×2 at most.*

For each party A_i and for every round j, we can reduce the associated binary observables $\hat{O}_0^{i,j}$ and $\hat{O}_1^{i,j}$ to a block-diagonal form in a suitable local basis using Theorem 14. The block-diagonal form is as follows:

$$\hat{O}_0^{i,j} = \bigoplus_{d_{i,j}} O_0^{d_{i,j}} = \bigoplus_{d_{i,j}} \sigma_y^{d_{i,j}}, \tag{3.31}$$

$$\hat{O}_1^{i,j} = \bigoplus_{d_{i,j}} O_1^{d_{i,j}} \tag{3.32}$$

$$= \bigoplus_{d_{i,j}} \left(\cos\left(\alpha_{d_{i,j}}\right)\sigma_y^{d_{i,j}} + \sin\left(\alpha_{d_{i,j}}\right)\sigma_x^{d_{i,j}}\right). \tag{3.33}$$

Let $\Pi_{d_{i,j}}$ denote the projection onto the $d_{i,j}$th block. If we act with the projection $\Pi_{d_{i,j}}$ on $\rho_{\hat{A}_{[M],j}}$, then we obtain the index $d_{i,j}$ of the corresponding Jordan block. Hence, after the application of the projection, the system possessed by each party is a two-dimensional system. This is true of $\hat{A}_{i,j}$ especially, which satisfies Condition 3. After party i performs the measurement $\{\Pi_{d_{i,j}}\}_{d_{i,j}}$ for round j, for all $i \in [M]$, the post-measurement state is as follows:

$$\frac{\left(\bigotimes_{i=1}^M \Pi_{d_{i,j}}\right)\rho_{\hat{A}_{[M],j}}\left(\bigotimes_{i=1}^M \Pi_{d_{i,j}}\right)}{\mathrm{Tr}\left[\left(\bigotimes_{i=1}^M \Pi_{d_{i,j}}\right)\rho_{\hat{A}_{[M],j}}\right]} \otimes \left(\bigotimes_{i=1}^M |d_{i,j}\rangle\langle d_{i,j}|\right). \tag{3.34}$$

Note that the first M quantum registers on the left have been reduced to qubit registers.

Using these projections, we produce Protocol 2. Protocol 2 is a device-dependent version of Protocol 1 but has the same winning probability as Protocol 1. This is due the fact that, regardless of the value of T_j and for any $d_j = d_{1,j} \cdots d_{M,j}$, the underlying state can thought of as being in the following state [152, Theorem 1]:

$$\tilde{\rho}^{d_j} := \sum_{u \in \{0,1\}^{M-1}} \left[\lambda_{0,u}^{d_j} |\psi_{0,u}\rangle\langle\psi_{0,u}| + \lambda_{1,u}^{d_j} |\psi_{1,u}\rangle\langle\psi_{1,u}| + \mathbf{i} s_u^{d_j} \left(|\psi_{0,u}\rangle\langle\psi_{1,u}| - |\psi_{1,u}\rangle\langle\psi_{0,u}|\right)\right], \tag{3.35}$$

where $\mathbf{i}^2 = -1$, $s_u^{d_j}, \lambda_{0,u}^{d_j} \in [0,1]$, and $\psi_{0,u}, \psi_{1,u}$ are defined in Definition 6. Hence, the projective measurement detailed earlier will neither change the winning probability nor the amount of multipartite entanglement produced by the source. (This is

true for any two-input two-output, or $(M, 2, 2)$, full-correlator Bell inequality [152, Theorem 1], like the MABK inequality we consider here.)

We will use Protocol 2 only to make statements about the soundness of Protocol 1. First, we need to clarify some notation. As before, the index i will denote the party, and the index j will denote the round of the protocol. $\hat{A}_{[M][n]}$ refers to all the quantum registers $\hat{A}_{i,j}$ possessed by the respective parties at the end of the protocol before conditioning on the outcome of the protocol. $A_{[M][n]}$ refers to the classical registers $A_{i,j}$ containing the inputs of the protocol used by the parties in each round, regardless of the T_j of said rounds. $D_{[M][n]}$ contains the results of the Jordan block projection $D_{i,j}$ performed in each round of the protocol. $X_{[M][n]}$ refers to the classical registers containing output $X_{i,j}$ from all the rounds of the protocol. For convenience, we shall refer to $A_{[M][n]}$, $D_{[M][n]}$, and $X_{[M][n]}$ together as $(ADX)_{[M][n]}$. $\overline{W}$ and T refer to the classical registers containing W_j and T_j, respectively, from all the rounds of the protocol.

3.5.3 Max-Tradeoff Function

In this section, we obtain a max-tradeoff function that satisfies Definition 14. We are interested in finding an upper bound on the following quantity:

$$\sup_{\sigma} H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\,T_j\Big)_{\mathcal{N}_j(\sigma)}\,, \tag{3.36}$$

for all $j \in [n]$ and $M' \in [M-1]$, where the supremum is taken over all input states of $\mathcal{N}_j$ for which the marginal on W_j of the output state is the probability

Protocol 2: : DIMEC protocol based on the MABK game

Arguments:

$\mathcal{M}$ – untrusted measurement device, with inputs and outputs in the set $\{0, 1\}$

$n \in \mathbb{N}_+$ – number of rounds

γ – the probability of conducting a test

ω_{exp} – expected winning probability in the MABK game

$\delta_{\text{est}} \in (0, 1)$ – width of the statistical confidence interval for the estimation test

$A_{i,j}$ indicates a classical register belonging to the i-th party and j-th round.

1: For every round $j \in [n]$, do steps 2-11:
2: Let ϕ^j denote the multipartite state produced by the source in this round.
3: Set $A_{i,j}, X_{i,j}, W_j = \perp$ for all $i \in [M]$.
4: Choose $T_j = 1$ with probability γ and $T_j = 0$ with probability $1 - \gamma$.
5: If $T_j = 1$:
6: Choose inputs $X_{i,j} \in \{0, 1\}$ uniformly at random.
7: Measure ϕ^j using $\mathcal{M}$ with the inputs $X_{i,j}$ and record outputs $A_{i,j} \in \{0, 1\}$.
8: Set $W_j = 1$ if the MABK game is won and $W_j = 0$ otherwise.
9: If $T_j = 0$:
10: Apply projections described in (3.34).
11: Keep ϕ^j in the registers $\bigotimes_{i=1}^{m} \hat{A}_{i,j}$.
12: Abort if $W = \sum_{j=1}^{n} \chi(T_j = 1)\, W_j < (\omega_{\text{exp}}\gamma - \delta_{\text{est}})n$.

distribution p. Henceforth, we shall refer this set of states as

$$\Sigma_p := \left\{\sigma \,\middle|\, \mathcal{N}_j(\sigma)_{W_j} = p\right\}. \tag{3.37}$$

We will first simplify (3.36). Note that the following equality holds:

$$\sum_x p(x) H(A|B)_{\rho^x} = H(A|BX)_{\tilde{\rho}}, \tag{3.38}$$

where $\{p(x)\}_x$ is a probability distribution, $\{\rho^x_{AB}\}_x$ is a set of states, $\tilde{\rho}_{ABX} := \sum_x p(x)\rho^x_{AB} \otimes |x\rangle\langle x|$, and $\{|x\rangle\}_x$ is an orthonormal basis. Using this, we find that

$$\begin{aligned}\sup_{\sigma\in\Sigma_p} H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\,T_j\Big)_{\mathcal{N}_j(\sigma)} = \\ \sup_{\sigma\in\Sigma_p}\Big[\Pr(T_j=0) H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\Big)_{\mathcal{N}_j^0(\sigma)} \\ + \Pr(T_j=1) H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\Big)_{\mathcal{N}_j^1(\sigma)}\Big],\end{aligned} \tag{3.39}$$

where $\mathcal{N}_j^0(\sigma)$ corresponds to the state when $T_j = 0$, and $\mathcal{N}_j^1(\sigma)$ corresponds to the state when $T_j = 1$. Note that $T_j = 1$ corresponds to a round where we apply measurements to play the MABK game and each $\hat{A}_{i,j}$ is in a deterministic state for all $i \in [M]$. This implies that

$$H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\Big)_{\mathcal{N}_j^1(\sigma)} = 0. \tag{3.40}$$

Hence,

$$\begin{aligned}\sup_{\sigma\in\Sigma_p} H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\,T_j\Big)_{\mathcal{N}_j(\sigma)} = \\ (1-\gamma)\sup_{\sigma\in\Sigma_p} H\Big(\hat{A}_{[M'],j}\Big|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\Big)_{\mathcal{N}_j^0(\sigma)}.\end{aligned} \tag{3.41}$$

To calculate an upper bound on the above quantity, we will use the fact that the conditional entropy is concave [153]:

$$\sum_x p(x) H(A|B)_{\rho^x} \leq H(A|B)_{\bar{\rho}}, \tag{3.42}$$

where the notation is the same as in (3.38) and $\bar{\rho}_{AB} \coloneqq \sum_x p(x) \rho^x_{AB}$. We will also make use of the bipartition between systems represented by the vertical bar in (3.36), which means that we can make use of local operations with respect to this bipartition. Given a particular $D_{[M],j}$ at the end of the j-th round of Protocol 2, the state $\tilde{\rho}^{d_j}$ in (3.35) has a simple structure in the GHZ basis. We can rewrite the GHZ basis, from Definition 6, in the following fashion:

$$|\psi_{v,u,w}\rangle \equiv \frac{1}{\sqrt{2}} \left[|w, u\rangle + (-1)^v |\bar{w}, \bar{u}\rangle \right], \tag{3.43}$$

where $v \in \{0,1\}$, while $u \in \{0,1\}^{M-M'}$ and $\bar{u} = 1 \oplus u$ are $M - M'$ bit strings, and $w \in \{0,1\}^{M'}$ and $\bar{w} = 1 \oplus w$ are M' bit strings.

Within the partition denoted by u, we can choose one qubit to be the control qubit, u_1, and then apply CNOTs on all the other qubits. We apply a similar set of operations on the partition denoted by w with the first qubit containing w_1 as the control qubit. These operations transform the M-partite GHZ basis states into the following state:

$$\frac{1}{2} \left(|u_1, w_1\rangle + (-1)^v |\bar{u}_1, \bar{w}_1\rangle \right) \otimes |u_2 \cdots u_{M'}\rangle \otimes |w_2 \cdots w_{M-M'}\rangle, \tag{3.44}$$

where $u_i, w_i \in \{0,1\}$. The above state is a Bell-basis state between the control qubits containing u_1 and w_1. After the CNOTs, as described above, are applied on the

state $\tilde{\rho}^{d_j}$ in (3.35), there are still off-diagonal terms in the resulting state. To make the final state diagonal in the Bell basis, we use the following twirling channel [154]:

$$\mathcal{T}(\rho) = \frac{1}{4}\Big(\rho + (X\otimes X)\,\rho\,(X\otimes X) + (Y\otimes Y)\,\rho\,(Y\otimes Y) + (Z\otimes Z)\,\rho\,(Z\otimes Z)\Big). \tag{3.45}$$

Now that we have simplified the underlying state, we make the following observation about the MABK inequality.

Lemma 2 *An M-partite MABK inequality* (3.12) *is equivalent to the CHSH inequality within any bipartition consisting of M′ parties on one side and the M − M′ other parties on the other side such that, for some* $\hat{O}_0^{[M-M'+1]}$ *and* $\hat{O}_1^{[M-M'+1]}$,

$$\mathcal{K}_M = \frac{1}{2}\mathcal{F}\Big(\mathcal{K}_{M-M'}, \overline{\mathcal{K}}_{M-M'}, \hat{O}_0^{[M-M'+1]}, \hat{O}_1^{[M-M'+1]}\Big). \tag{3.46}$$

Proof. We know that, for all $M \geq 3$

$$\mathcal{K}_M = \frac{1}{2}\mathcal{K}_{M-1}\otimes\left(\hat{O}_0^M + \hat{O}_1^M\right) + \frac{1}{2}\overline{\mathcal{K}}_{M-1}\otimes\left(\hat{O}_0^M - \hat{O}_1^M\right), \tag{3.47}$$

and

$$\overline{\mathcal{K}}_M = \frac{1}{2}\overline{\mathcal{K}}_{M-1}\otimes\left(\hat{O}_0^M + \hat{O}_1^M\right) + \frac{1}{2}\mathcal{K}_{M-1}\otimes\left(\hat{O}_1^M - \hat{O}_0^M\right). \tag{3.48}$$

It is then clear that

$$\mathcal{K}_{M-1} = \frac{1}{2}\mathcal{K}_{M-2}\otimes\left(\hat{O}_0^{M-1} + \hat{O}_1^{M-1}\right) + \frac{1}{2}\overline{\mathcal{K}}_{M-2}\otimes\left(\hat{O}_0^{M-1} - \hat{O}_1^{M-1}\right), \tag{3.49}$$

Let

$$V_M := \left|\mathrm{Tr}\left[\mathcal{K}_M\,\rho_{\hat{A}_{[M]}}\right]\right| = \frac{1}{2}\left|\mathrm{Tr}\left[\left\{\mathcal{K}_{M-1}\otimes\left(\hat{O}_0^M + \hat{O}_1^M\right) + \overline{\mathcal{K}}_{M-1}\otimes\left(\hat{O}_0^M - \hat{O}_1^M\right)\right\}\rho_{\hat{A}_{[M]}}\right]\right|. \tag{3.50}$$

From [45, Theorem 2], we know be relabeling $\mathcal{K}_{M-1}$ as $\hat{O}_0^1$, $\overline{\mathcal{K}}_{M-1}$ as $\hat{O}_1^1$, $\hat{O}_0^M$ as $\hat{O}_0^2$, and $\hat{O}_1^M$ as $\hat{O}_1^2$, for $M' = 1$

$$V_M = \frac{1}{2}\left|\mathrm{Tr}\left[\mathcal{F}\left(\mathcal{K}_{M-1}, \overline{\mathcal{K}}_{M-1}, \hat{O}_0^M, \hat{O}_1^M\right)\rho_{\hat{A}_{[M]}}\right]\right|. \tag{3.51}$$

We need to show the same for $1 \leq M' \leq M-1$. Let us start with $M' = 2$. By substituting (3.49) in (3.47), we get

$$\begin{aligned}\mathcal{K}_M = &\frac{1}{4}\left(\mathcal{K}_{M-2}\otimes\left(\hat{O}_0^{M-1}+\hat{O}_1^{M-1}\right)+\overline{\mathcal{K}}_{M-2}\otimes\left(\hat{O}_0^{M-1}-\hat{O}_1^{M-1}\right)\right)\otimes\left(\hat{O}_0^M+\hat{O}_1^M\right)\\ &+\frac{1}{4}\left(\overline{\mathcal{K}}_{M-2}\otimes\left(\hat{O}_0^{M-1}+\hat{O}_1^{M-1}\right)+\mathcal{K}_{M-2}\otimes\left(\hat{O}_1^{M-1}-\hat{O}_0^{M-1}\right)\right)\otimes\left(\hat{O}_0^M-\hat{O}_1^M\right) \qquad (3.52)\\ =&\frac{1}{4}\mathcal{K}_{M-2}\otimes\left(\left(\hat{O}_0^{M-1}+\hat{O}_1^{M-1}\right)\otimes\left(\hat{O}_0^M+\hat{O}_1^M\right)+\left(\hat{O}_1^{M-1}-\hat{O}_0^{M-1}\right)\otimes\left(\hat{O}_0^M-\hat{O}_1^M\right)\right)\\ &+\frac{1}{4}\overline{\mathcal{K}}_{M-2}\otimes\left(\left(\hat{O}_0^{M-1}+\hat{O}_1^{M-1}\right)\otimes\left(\hat{O}_0^M-\hat{O}_1^M\right)+\left(\hat{O}_1^{M-1}-\hat{O}_0^{M-1}\right)\otimes\left(\hat{O}_0^M+\hat{O}_1^M\right)\right) \qquad (3.53)\\ =&\frac{1}{2}\mathcal{K}_{M-2}\otimes\left(\hat{O}_0^{M-1}\otimes\hat{O}_1^M+\hat{O}_1^{M-1}\otimes\hat{O}_0^M\right)+\frac{1}{2}\overline{\mathcal{K}}_{M-2}\otimes\left(\hat{O}_1^{M-1}\otimes\hat{O}_0^M-\hat{O}_0^{M-1}\otimes\hat{O}_1^M\right). \qquad (3.54)\end{aligned}$$

Relabelling $\hat{O}_1^{M-1}\otimes\hat{O}_0^M$ as $\hat{O}_0^{[M-1]}$, and $\hat{O}_0^{M-1}\otimes\hat{O}_1^M$ as $\hat{O}_1^{[M-1]}$, we get

$$V_M = \frac{1}{2}\left|\mathrm{Tr}\left[\mathcal{F}\left(\mathcal{K}_{M-2}, \overline{\mathcal{K}}_{M-2}, \hat{O}_0^{[M-1]}, \hat{O}_0^{[M-1]}\right)\rho_{\hat{A}_{[M]}}\right]\right|. \tag{3.55}$$

Now, we have shown that the proposition is true for $M' = 1$ and $M' = 2$. We can now use induction to show that our proposition holds for all $1 \leq M' \leq M-1$. Let assume that for some $M' = m$, the following hold:

$$\mathcal{K}_M = \frac{1}{2}\mathcal{K}_{M-m}\otimes\left(\hat{O}_0^{[M-m+1]}+\hat{O}_1^{[M-m+1]}\right)+\frac{1}{2}\overline{\mathcal{K}}_{M-m}\otimes\left(\hat{O}_0^{[M-m+1]}-\hat{O}_1^{[M-m+1]}\right) \tag{3.56}$$

and

$$V_M = \frac{1}{2}\left|\mathrm{Tr}\left[\mathcal{F}\left(\mathcal{K}_{M-m}, \overline{\mathcal{K}}_{M-m}, \hat{O}_0^{[M-m+1]}, \hat{O}_1^{[M-m+1]}\right)\rho_{\hat{A}_{[M]}}\right]\right|. \tag{3.57}$$

where, $\mathcal{K}_{M-m}$ is defined in (3.9), and $\hat{O}_0^{[M-m+1]}$ and $\hat{O}_1^{[M-m+1]}$ are observables similar to those in (3.55) involving parties $M-m+1,\ldots,M$. We know that

$$\mathcal{K}_{M-m} = \frac{1}{2}\mathcal{K}_{M-m-1} \otimes \left(\hat{O}_0^{M-m} + \hat{O}_1^{M-m}\right) + \frac{1}{2}\overline{\mathcal{K}}_{M-m} \otimes \left(\hat{O}_0^{M-m} - \hat{O}_1^{M-m}\right). \tag{3.58}$$

By substituting (3.58) in (3.56), we get

$$\begin{aligned}\mathcal{K}_M = \frac{1}{4}\mathcal{K}_{M-(m+1)} \otimes \left(\left(\hat{O}_0^{M-m} + \hat{O}_1^{M-m}\right) \otimes \left(\hat{O}_0^{[M-m+1]} + \hat{O}_1^{[M-m+1]}\right)\right) \\ + \frac{1}{4}\mathcal{K}_{M-(m+1)} \otimes \left(\left(\hat{O}_0^{M-m} - \hat{O}_1^{M-m}\right) \otimes \left(\hat{O}_0^{[M-m+1]} - \hat{O}_1^{[M-m+1]}\right)\right) \\ + \frac{1}{4}\overline{\mathcal{K}}_{M-(m+1)} \otimes \left(\left(\hat{O}_0^{M-m} + \hat{O}_1^{M-m}\right) \otimes \left(\hat{O}_0^{[M-m+1]} - \hat{O}_1^{[M-m+1]}\right)\right) \\ + \frac{1}{4}\overline{\mathcal{K}}_{M-(m+1)} \otimes \left(\left(\hat{O}_0^{M-m} - \hat{O}_1^{M-m}\right) \otimes \left(\hat{O}_0^{[M-m+1]} + \hat{O}_1^{[M-m+1]}\right)\right)\end{aligned} \tag{3.59}$$

$$\begin{aligned}= \frac{1}{2}\mathcal{K}_{M-(m+1)} \otimes \left(\hat{O}_0^{M-m} \otimes \hat{O}_1^{[M-m+1]} + \hat{O}_1^{M-m} \otimes \hat{O}_0^{[M-m+1]}\right) \\ + \frac{1}{2}\overline{\mathcal{K}}_{M-(m+1)} \otimes \left(\hat{O}_1^{M-m} \otimes \hat{O}_0^{[M-m+1]} - \hat{O}_0^{M-m} \otimes \hat{O}_1^{[M-m+1]}\right).\end{aligned} \tag{3.60}$$

Therefore,

$$V_M = \frac{1}{2}\left|\mathrm{Tr}\left[\mathcal{F}\left(\mathcal{K}_{M-(m+1)}, \overline{\mathcal{K}}_{M-(m+1)}, \hat{O}_1^{M-m} \otimes \hat{O}_0^{[M-m+1]}, \hat{O}_0^{M-m} \otimes \hat{O}_1^{[M-m+1]}\right)\rho_{\hat{A}_{[M]}}\right]\right|. \tag{3.61}$$

Hence, by strong induction, we have proven our proposition. ■

Given the above operations and Lemma 2, we can use a prior result from [144, Lemma 14] to obtain our max-tradeoff function. We can replace the CHSH violation β_2 in (3.14) with the multipartite MABK violation β_M in (3.13) for our case. We restate [144, Lemma 14] for convenience.

Lemma 3 (Lemma 14 of [144]) *For every Bell-diagonal state $\sigma_{\hat{A}\hat{B}}$ that can be used to violate the CHSH inequality with violation $\beta_2 \in [2, 2\sqrt{2}]$, the following inequality holds:*

$$H(\hat{A}|\hat{B}) \leq 2h_2\left(\frac{1}{2} - \frac{\beta_2}{4\sqrt{2}}\right) - 1, \tag{3.62}$$

where $h_2(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function and β_2 is defined in (3.14).

These lemmas can be applied to Protocol 2 in the following manner. Using Lemma 2 and Lemma 3, we find that

$$\sup_{\sigma\in\Sigma_p} H\left(\hat{A}_{[M'],j}\middle|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\,T_j\right)_{\mathcal{N}_j(\sigma)} \leq (1-\gamma)\left(2h_2\left(\frac{1}{2} - \frac{\beta_M}{4\sqrt{2}}\right) - 1\right), \tag{3.63}$$

where β_M is defined in (3.13). Using (3.63), we can state the following theorems.

Theorem 15 *For all $M' \in [M]$ with M even and $\omega \in [p^e_{\min}, p^e_{\max}]$ as defined in (3.19), respectively, let Σ_p (defined in (3.37)) be such that the winning probability is strictly greater than ω (i.e., $p(1)/\gamma > \omega$). Then,*

$$\sup_{\sigma\in\Sigma_p} H\left(\hat{A}_{[M'],j}\middle|\hat{A}_{[M'+1,M],j}\,(ADX)_{[M],j}\,T_j\right)_{\mathcal{N}_j(\sigma)} \leq (1-\gamma)\cdot g_e(\omega), \tag{3.64}$$

where γ is defined in Protocol 1,

$$g_e(\omega) := 2h_2\left(\frac{1}{2} - \frac{2\omega - 1}{\sqrt{2}}\right) - 1, \tag{3.65}$$

and $h_2(p)$ is the binary entropy function.

Proof. When M is even, the MABK game winning probability and the MABK violation in (3.12) are related as follows [45]: $\beta_M = 8\omega - 4$. Substituting $\beta_M = 8\omega - 4$ in (3.63), we get the required result. ■

Theorem 16 *For all $M' \in [M]$ with M odd and $\omega \in [p^o_{\min}, p^o_{\max}]$ as defined in (3.20), respectively, let Σ_p (defined in (3.37)) be such that the winning probability is strictly greater than ω (i.e., $p(1)/\gamma > \omega$). Then,*

$$\sup_{\sigma \in \Sigma_p} H\Big(\hat{A}_{[M'],j} \Big| \hat{A}_{[M'+1,M],j} \, (ADX)_{[M],j} \, T_j\Big)_{\mathcal{N}_j(\sigma)} \leq (1-\gamma) \cdot g_o(\omega), \tag{3.66}$$

where γ is defined in Protocol 1,

$$g_o(\omega) := 2h_2\left(\frac{1}{2} - \frac{4\omega - 1}{2}\right) - 1, \tag{3.67}$$

and $h_2(p)$ is the binary entropy function.

Proof. When M is odd, the MABK game winning probability and the MABK violation in (3.12) are related as follows [45]: $\beta_M = 8\sqrt{2}\omega - 2\sqrt{2}$. Substituting $\beta_M = 8\sqrt{2}\omega - 2\sqrt{2}$ in (3.63), we get the required result. ■

These theorems serve as the basis for our max-tradeoff function. Using Theorems 15 and 16 to define a max-tradeoff function for all p with $p(1)/\gamma \in [\, p_{\min}, p_{\max}]$. Define a function f in the following fashion: when M is even

$$f(p, M) := \begin{cases} (1-\gamma) \cdot g_e\left(\frac{p(1)}{\gamma}\right) & \frac{p(1)}{\gamma} \in [0, p^e_{\max}] \\ \gamma - 1 & \frac{p(1)}{\gamma} \in [p^e_{\max}, 1] \end{cases}, \tag{3.68}$$

and when M is odd,

$$f(p, M) := \begin{cases} (1-\gamma) \cdot g_o\left(\frac{p(1)}{\gamma}\right) & \frac{p(1)}{\gamma} \in [0, p^o_{\max}] \\ \gamma - 1 & \frac{p(1)}{\gamma} \in [p^o_{\max}, 1] \end{cases}, \tag{3.69}$$

From Theorems 15 and 16, we know that any choice of $f_{\max}(p, M)$ that is differentiable and satisfies $f_{\max}(p, M) \geq f(p, M)$ for all p will be a valid max-tradeoff function for our EAT channels. Since the derivatives of f in (3.68) and (3.69) at $p(1)/\gamma = p^e_{\max}$ and $p(1)/\gamma = p^o_{\max}$, respectively, are infinite, we now choose a function $f_{\max}(p, M)$ such that $\|\nabla f_{\max}(p, M)\|_\infty$ is finite. Let

$$f_{\max}(p, p_t, M) := \begin{cases} f(p, M) & p(1) \leq p_t(1) \\ a(p_t) \cdot p(1) + b(p_t) & p(1) > p_t(1) \end{cases}, \tag{3.70}$$

where p_t is a probability distribution over $\{0, 1, \perp\}$,

$$a(p_t) := \frac{\partial}{\partial p(1)} f(p, M)\Big|_{p(1)=p_t(1)}, \text{ and} \tag{3.71}$$

$$b(p_t) := f(p_t) - a(p_t) \cdot p_t(1). \tag{3.72}$$

It follows from the definition of $f_{\max}(p, M)$ that $f_{\max}(p, M)$ is differentiable and, for all p_t, $\|\nabla f_{\max}(\cdot, p_t, M)\|_\infty \leq a(p_t)$. Furthermore, as f is a concave function, $f_{\max}(p, p_t, M) \geq f(p, M)$ for all p. Thus, $f_{\max}(p, p_t, M)$ is a max-tradeoff function.

3.5.4 Applying the EAT

We can finally apply the EAT, stated in Theorem 13, to derive an upper bound on the conditional smooth max-entropy. By obtaining the exact form of $f_{\max}$, we have the calculated t on the right-hand side of (3.29). We need to calculate (3.30). We know that the dimension of all quantum registers involved is two, which means

that $d_{O_i} = 2M'$. From (3.70), we get $\|\nabla f_{\max}\|_\infty \leq a(p_t)$. According to Condition 2 in Definition 8, for soundness, we require that, for every source ϕ and measurement device, Protocol 1 either certifies a minimum amount of GHZ entanglement or aborts with probability greater than $1-\varepsilon_{\text{snd}}$ when applied on σ. So, the probability of Protocol 1 not aborting is negligible i.e., $\Pr[\Omega]_\tau \leq \varepsilon_{\text{snd}}$. Also, note that ε_{smo} is chosen such that the fidelity constraint in (3.2) is satisfied. When Protocol 2 does not abort, we can define the following quantity, which corresponds to the right-hand side of (3.29):

$$\begin{aligned}\eta(\omega_{\text{exp}}\gamma - \delta_{\text{est}}, p_t, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M) \coloneqq \\ n \cdot f_{\max}\Big(\omega_{\text{exp}}\gamma - \delta_{\text{est}}, p_t, M\Big) + 2\sqrt{n}\left(\log_2(1+2M') + \lceil a(p_t)\rceil\right) \\ \times \sqrt{1 - 2\log_2\left(\varepsilon_{\text{smo}} \cdot \varepsilon_{\text{snd}}\right)}, \quad (3.73)\end{aligned}$$

where $\omega_{\text{exp}}\gamma - \delta_{\text{est}}$ is the minimum acceptable $p(1)$ as outlined in Step 12 of Protocol 2. We still have one free variable p_t. We can optimize over p_t to get the following equation.

$$\begin{aligned}\eta_{\text{opt}}\left(\omega_{\text{exp}}\gamma - \delta_{\text{est}}, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M\right) \coloneqq \\ \min_{p_t : p_{\min} < \frac{p_t(1)}{\gamma} < p_{\max}} \eta\left(\omega_{\text{exp}}\gamma - \delta_{\text{est}}, p_t, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M\right). \quad (3.74)\end{aligned}$$

Finally, we can state the following:

Theorem 17 *For every source and all measurement devices in the setting detailed earlier, let ρ be the state generated using Protocol 2, Ω the event that Protocol 2 does not abort, and $\rho_{|\Omega}$ the state conditioned on Ω. Then, for all $8 \cdot 3^{M/2}\sqrt{\varepsilon_{\text{smo}}}, \varepsilon_{\text{snd}} \in (0,1)$, either Protocol 2*

aborts with probability greater than $1 - \varepsilon_{\text{snd}}$ *or*

$$H_{\max}^{\varepsilon_{\text{smo}}}\left(\hat{A}_{[M'],[n]}\middle|\hat{A}_{[M'+1,M],[n]}\,(ADX)_{[M],[n]}\,T\right)_{\rho_{|\Omega}} < \eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M\right), \tag{3.75}$$

where η_{opt} *is defined in* (3.74).

Proof. In Subsection 3.5.2, we showed that Protocol 2 consists of EAT channels (defined in Definition 13). In Subsection 3.5.3, we derived the appropriate max-tradeoff function (as defined in Definition 14). Hence, using Theorem 13, the claim follows. ■

Now, we have all the ingredients to show that Protocol 1 is sound.

3.5.5 Soundness

In this subsection, we show that Protocol 1 is sound. To do this, we need to bound the quantity in (3.27) in a device-independent manner. We use the preceding theorems to obtain this bound and certify the multipartite entanglement distillation rate from a source. This brings us to our final theorem, which is as follows.

Theorem 18 *Fix* $\varepsilon_{\text{smo}} > 0$ *such that* $\varepsilon := 8 \cdot 3^{M/2}\sqrt{\varepsilon_{\text{smo}}} \in (0,1)$. *For all* $\varepsilon_{\text{snd}}, \varepsilon_{\text{cmp}}, \varepsilon \in (0,1)$, *Protocol 1 is a DIMEC protocol with*

1. *Noise tolerance (completeness): The probability that Protocol 1 aborts when applied on* $\phi^{\text{honest}} \in \mathcal{S}^{\text{honest}}$ *using a measurement device from* $\mathcal{D}^{\text{honest}}$ *is at most*

$\varepsilon_{\text{cmp}} \leq \exp\left(-2n\delta_{\text{est}}^2\right)$, *as shown in Theorem 10.*

2. *Entanglement certification (soundness): For every source σ and measurement device, either Protocol 1 aborts with probability greater than $1 - \varepsilon_{\text{snd}}$ when applied on σ or*

$$E_D^{\varepsilon}(\rho_{|\Omega}) \geq \frac{-\eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{snd}}, \varepsilon_{\text{smo}}, M-1, M\right)}{M-1} + \frac{2\log \varepsilon_{\text{smo}}}{M-1}, \tag{3.76}$$

where η_{opt} is defined in (3.74).

Proof. Using Theorem 17, we get

$$-H_{\max}^{\varepsilon_{\text{smo}}}\left(\hat{A}_{[M'],[n]} \middle| \hat{A}_{[M'+1,M],[n]} \, (ADX)_{[M],[n]} \, T\right)_{\rho_{|\Omega}} \geq -\eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M\right), \tag{3.77}$$

Notice that all our prior analysis is agnostic to what $i \in [M]$ is assigned to which specific party involved. Also recall that $M' \in [M-1]$. Hence,

$$-H_{\max}^{\varepsilon_{\text{smo}}}\left(\hat{A}_{K,[n]} \middle| \hat{A}_{[M]\setminus K,[n]} \, (ADX)_{[M],[n]} \, T\right)_{\rho_{|\Omega}} \geq -\eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{smo}}, \varepsilon_{\text{snd}}, M', M\right), \tag{3.78}$$

where $K \subseteq [M]\backslash k$ for some $k \in [M]$.

This bound holds regardless of the individual elements that constitute K. We can then use the above inequality to obtain a lower bound on the quantity in (3.27). Hence, we get

$$\begin{aligned}\max_{k\in[M]} \left\{ \min_{K\subseteq[M]\setminus k} \frac{-H_{\max}^{\varepsilon_{\text{smo}}}\left(\hat{A}_{K,[n]} \middle| \hat{A}_{[M]\setminus K,[n]} \, (ADX)_{[M],[n]} \, T\right)_{\rho_{|\Omega}}}{|K|} \right\} + \frac{2\log \varepsilon_{\text{smo}}}{M-1} \\ \geq \max_{k\in[M]} \left\{ \min_{K\subseteq[M]\setminus k} \frac{-\eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{snd}}, \varepsilon_{\text{smo}}, |K|, M\right)}{|K|} \right\} + \frac{2\log \varepsilon_{\text{smo}}}{M-1}. \end{aligned} \tag{3.79}$$

The optimizations involved can be solved since $\eta_{\text{opt}}(\varepsilon_{\text{snd}}, \varepsilon_{\text{smo}}, |K|, M)$ depends only on $|K|$, leading to

$$E_D^{\varepsilon}(\rho_{|\Omega}) \geq \frac{-\eta_{\text{opt}}\left(\omega_{\text{exp}}, \varepsilon_{\text{snd}}, \varepsilon_{\text{smo}}, M-1, M\right)}{M-1} + \frac{2\log \varepsilon_{\text{smo}}}{M-1}, \tag{3.80}$$

which concludes the proof. ■

We plot also $-\eta_{\text{opt}}(\omega_{\text{exp}})/n(M-1)$ for $M = 4$ and $\gamma = 0.5$ up to leading order in Figure 3.1.

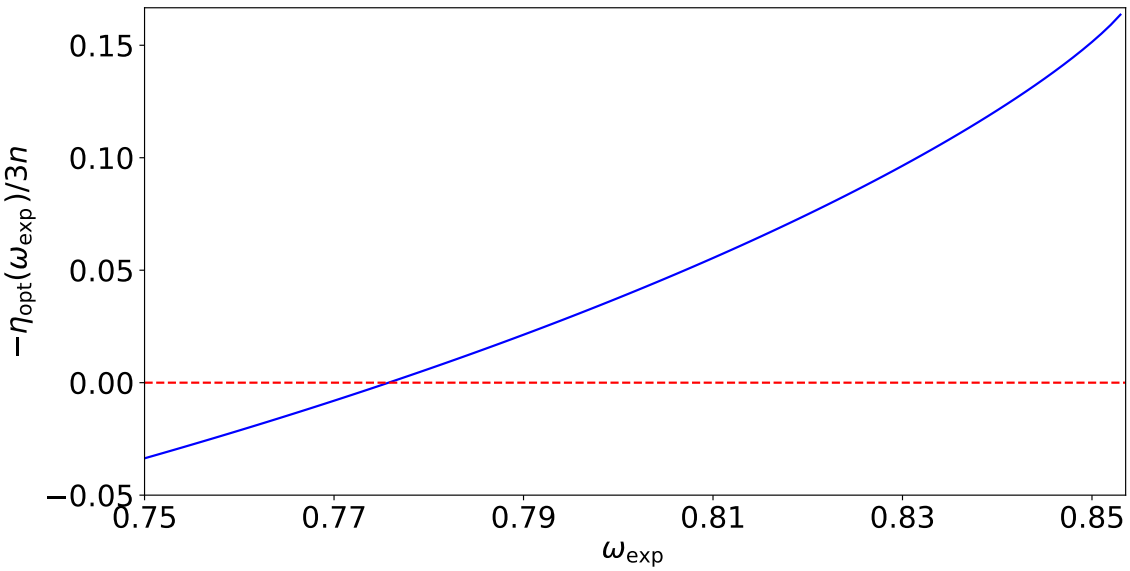


Figure 3.1: Plot of $-\eta_{\text{opt}}(\omega_{\text{exp}})/n(M-1)$, defined in (3.74), for $M = 4$ and $\gamma = 0.5$ up to leading order in n for $\omega_{\text{exp}} \in [p^e_{\text{min}}, p^e_{\text{max}}]$ defined in (3.19). The solid line corresponds to $-\eta_{\text{opt}}(\omega_{\text{exp}})/n(M-1)$. The dashed line corresponds to $-\eta_{\text{opt}}/n(M-1) = 0$. The quantity $-\eta_{\text{opt}}(\omega_{\text{exp}})/n(M-1)$ represents the amount of multipartite distillable entanglement that can be certified per round by Protocol 1 as function of ω_{exp}.

3.6 Conclusion

In this chapter, we defined a DI, M-partite entanglement distillation certification protocol consisting of completeness and soundness conditions. We then proposed a protocol and showed that it is indeed a DI multipartite entanglement distillation certification protocol. Specifically, we proved that Protocol 1 is indeed a DI multipartite entanglement distillation certification protocol. Our proposed protocol is centered around the MABK inequality [41, 42, 43], which is critical to proving the completeness and soundness conditions. To prove the soundness condition, we used the entropy accumulation theorem [145], the structure of the MABK inequality [41, 42, 43], and the multipartite entanglement distillation protocols and rates described in [148, 149].

CHAPTER 4

MULTIPARTITE INTRINSIC NON-LOCALITY AND DEVICE-INDEPENDENT CONFERENCE KEY AGREEMENT

4.1 Introduction

In principle, quantum key distribution (QKD) can produce a secret key secured by the laws of physics [155, 33, 156]. In the device-dependent setting of QKD, it is assumed that the devices possessed by Alice and Bob are perfectly characterized and trusted; i.e., the measurements applied, and the states used are assumed to be known and certified. However, after several experiments implementing QKD protocols, researchers have found this assumption to be too restrictive.

To combat our reliance on some of these strong assumptions underpinning QKD, several scenarios have been developed with varying degrees of trust in the measurements and states used. In QKD, if the measurements, states, or devices possessed by one of the parties are not trusted, the scenario is called one-sided device-independent QKD [157, 158]. If all devices involved are deemed to be untrustworthy, the scenario is called device-independent QKD [159, 160, 161, 34].

Researchers have established upper bounds on the secret key agreement capacity for all the scenarios described above [162, 163] (see also [164]). The basic idea behind these upper bounds comes from a classical information measure called intrinsic information [165]. Intrinsic information inspired the squashed-

entanglement upper bound for device-dependent QKD [166, 162], and squashed entanglement in turn inspired the development of quantum intrinsic non-locality [163] and quantum intrinsic steerability [167]. These latter quantities serve as upper bounds for device-independent QKD and one-sided device-independent QKD, respectively, as shown in [163]. Along with being upper bounds on the performance of certain cryptographic tasks, these quantities are also resource quantifiers for Bell non-locality and steerability, respectively.

Here, we go beyond device-independent QKD and Bell non-locality for two parties and address device-independent (DI) conference key agreement [3, 50] and multipartite non-locality. Conference key agreement is the task of distributing secret key among more than two users, as encountered in the context of quantum networks. Part of the interest in this task comes from the fact that a protocol based on genuinely multipartite entangled states can achieve higher rates of conference key agreement than a protocol based on a combination of bipartite entangled states [46]. Just as Bell non-locality is the key resource for DIQKD, one would expect multipartite non-locality to be the key resource in DI conference key agreement.

Here, we propose a resource quantifier for multipartite non-locality called multipartite intrinsic non-locality. We base instances of this resource quantifier on total correlation and dual total correlation [168] (see also [169, 170]), which generalize mutual information to the multipartite case. Total correlation and dual total correlation have previously been used to establish upper bounds on entan-

glement distillation and secret key agreement capacities of quantum broadcast channels [171]; see [169] for its use in establishing an upper bound on distillable secret key and distillable entanglement of a multipartite state. We use multiparite intrinsic non-locality to derive upper bounds on the ultimate rate at which device-independent (DI) conference key agreement is possible.

To show that our quantity is indeed a useful upper bound, it is necessary to prove that it is additive. In order to prove additivity (and other useful properties) of multipartite intrinsic non-localities, we establish a chain rule for total correlation and dual total correlation of two rounds of the conference key agreement protocol in Section 4.7. The chain rule for total correlation expresses the total correlation of two rounds of the conference key agreement protocol as the sum of total correlation terms related to the individual rounds of the conference key agreement protocol and other information theoretic quantities. These additional information-theoretic quantities are expressed in terms of conditional mutual information. For these, we derive a chain rule for total correlation and dual total correlation that meets the aforementioned criteria and holds for all finite M. Such a broadly applicable chain rule is not obtained in [163].

In what follows, we first discuss no-signaling and quantum correlation and then proceed to no-signaling and quantum extensions. After that, we define a quantum tripartite intrinsic non-locality, which is based on tripartite total correlation, and prove that it is indeed additive, convex, and monotone under local operations and common randomness. We then define the multipartite intrinsic non-

localities using total correlation and dual total correlation, starting by defining and discussing multipartite intrinsic non-locality based on total correlation and then moving on to the one defined in terms of dual total correlation. We establish important identities (our chain rule) for total correlation and dual total correlation that allow us to use arguments similar to those presented for the tripartite scenario to prove that the multipartite intrinsic non-localities, presented in this chapter, are additive, convex upper bounds on the device-independent conference key agreement capacity in the general M-partite case. Then, we give a general overview of device-independent conference key agreement for the tripartite case and define the DI conference key agreement capacity. Finally, we show that tripartite intrinsic no-locality is an upper bound on DI conference key agreement capacity for the tripartite situation and provide arguments to show that multipartite intrinsic non-locality upper bounds the M-partite DI conference key agreement capacity, for all finite M.

As other contributions, we calculate upper bounds on both quantum tripartite intrinsic non-localities using eavesdropper attacks similar to those from [163] and [2], which were used to calculate upper bounds on quantum intrinsic non-locality. We plot quantum tripartite intrinsic non-locality versus parity-CHSH violation under these attacks, and we compare these to previously calculated lower bounds from [3]. We also consider a noise model in which each share of the tripartite state passes through a qubit depolarizing channel. We plot quantum tripartite intrinsic non-localities versus the depolarizing parameter p_{dep} for this noise model and compare them to the lower bound from [3].

The rest of this chapter is structured as follows. Section 4.2 discusses no-signaling constraints, no-signaling extensions, and quantum extensions, focusing especially on the tripartite case. Section 4.3 contains the definition of tripartite intrinsic non-locality and proves that it is additive using a chain rule, which we derive here. Sections 4.7 and 4.8 generalize tripartite intrinsic non-locality and all of its properties to the multipartite case using total correlation and dual total correlation, respectively, and generalizations of the aforementioned chain rule. Section 4.9 introduces a general form of a DI conference key agreement protocol and its associated capacity. Then, we show that tripartite intrinsic non-locality is an upper bound on the tripartite device-independent conference key agreement capacity. Section 4.10 contains some examples of our upper bound calculated under various attacks by an eavesdropper. Section 4.11 contains our conclusions and possible directions for future work.

4.2 Correlations, No-Signaling Conditions, and Quantum Extensions

First, let us define the types of correlations that we are concerned with in this chapter: no-signaling correlations and quantum correlations. Let us begin by discussing no-signaling correlations.

No-signaling conditions impose constraints on correlations, which imply that

parties sharing the correlation cannot use it alone to communicate; i.e., no party can infer the input choices of another party based solely on their own outputs [172]. On a technical level, no-signaling conditions imply that tracing over subsets of outputs of a correlation results in tracing over the corresponding inputs [173]. These conditions are relevant in our scenario as it is necessary to verify that the correlations observed are from the state and measurement choices shared by the participants and not from classical communication when the input choices are made. Compliance with no-signaling conditions can be enforced by imposing space-like separation between measuring parties or constructing other barriers to prevent communication.

No-signaling conditions for the tripartite scenario are as follows:

$$\begin{aligned}
\sum_a p(a,b,c\,|\,x,y,z) &= \sum_a p(a,b,c\;|\;\bar{x},y,z) = p(b,c\,|\,y,z) \quad \forall x,\bar{x},\\
\sum_b p(a,b,c\,|\,x,y,z) &= \sum_b p(a,b,c\,|\,x,\bar{y},z) = p(a,c\,|\,x,z) \quad \forall y,\bar{y},\\
\sum_c p(a,b,c\,|\,x,y,z) &= \sum_c p(a,b,c\,|\,x,y,\bar{z}) = p(a,b\,|\,x,y) \quad \forall z,\bar{z}.
\end{aligned} \tag{4.1}$$

The set of all correlations that satisfy the above three conditions in (4.1) are called no-signaling correlations. The no-signaling conditions above can also equivalently be expressed in terms of conditional mutual information as follows:

$$I(X;BC\,|\,YZ)_\rho = I(Y;AC\,|\,XZ)_\rho = I(Z;AB\,|\,XY)_\rho = 0, \tag{4.2}$$

where

$$\rho_{ABCXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z)\, p(a,b,c\,|\,x,y,z)\; |abcxyz\rangle\langle abcxyz|_{ABCXYZ}\,, \tag{4.3}$$

$p(a, b, c \mid x, y, z)$ is a no-signaling correlation, and the conditional mutual information of random variables K, L, and M is defined as

$$I(K; L \mid M) := H(KM) + H(LM) - H(M) - H(KLM), \tag{4.4}$$

where H denotes the entropy. It suffices to take the input distribution q to be uniform. Note that the conditions in (4.1) imply the following ones, by tracing over two of the outputs, rather than just one:

$$I(YZ; A \mid X)_\rho = I(XZ; B \mid Y)_\rho = I(XY; C \mid Z)_\rho = 0. \tag{4.5}$$

Now we move on to quantum correlations. Consider the following scenario: Alice, Bob and Charlie are given a share of a tripartite quantum state $\rho_{\hat{A}\hat{B}\hat{C}}$ that is distributed to them by a possibly unknown entity, and each party has access to a black box with which they can interact classically. For each classical input, the corresponding black box applies a positive operator-valued measure (POVM) on its respective share of the tripartite state. After the application of the POVM, the box outputs a classical value that is recorded by the corresponding participant. The correlation that is obtained using the aforementioned process is of the following form:

$$p(a, b, c \mid x, y, z) = \mathrm{Tr}\Big([\Pi_a^{(x)} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)}]\, \rho_{\hat{A}\hat{B}\hat{C}}\Big), \tag{4.6}$$

where $\{\Pi_a^{(x)}\}_a$, $\{\Pi_b^{(y)}\}_b$, and $\{\Pi_c^{(z)}\}_c$ are POVMs. Correlations of the form described in (4.6) are called quantum correlations. Quantum correlations are a subset of no-signaling correlations. This fact can easily be seen in the example analysis below:

$$\sum_a p(a, b, c \mid x, y, z) = \sum_a \mathrm{Tr}\Big([\Pi_a^{(x)} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)}]\, \rho_{\hat{A}\hat{B}\hat{C}}\Big) \tag{4.7}$$

$$= \mathrm{Tr}\Big([\mathbb{I} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)}]\,\rho_{\hat{A}\hat{B}\hat{C}}\Big) \tag{4.8}$$

$$= \mathrm{Tr}\Big([\Pi_b^{(y)} \otimes \Pi_c^{(z)}]\,\rho_{\hat{B}\hat{C}}\Big) \tag{4.9}$$

$$= p(b, c \,|\, y, z). \tag{4.10}$$

Since we are looking at non-locality for the sake of a cryptographic task, it is necessary that we delineate the power that the eavesdropper possesses. We do so by allowing the eavesdropper to possess either a no-signaling extension or a quantum extension. No-signaling extensions are extensions of a correlation that obey the above no-signaling constraints and can be expressed as follows:

$$\begin{aligned}
\sum_a p(a,b,c \,|\, x,y,z)\,\rho_E^{abcxyz} &= \sum_a p(a,b,c \,|\, \bar{x},y,z)\,\rho_E^{a,b,c,\bar{x},y,z} \quad \forall x,\bar{x},\\
\sum_b p(a,b,c \,|\, x,y,z)\,\rho_E^{abcxyz} &= \sum_b p(a,b,c \,|\, \bar{y},x,z)\,\rho_E^{a,b,c,\bar{y},x,z} \quad \forall y,\bar{y},\\
\sum_c p(a,b,c \,|\, x,y,z)\,\rho_E^{abcxyz} &= \sum_c p(a,b,c \,|\, \bar{z},y,x)\,\rho_E^{a,b,c,\bar{z},y,x} \quad \forall z,\bar{z}.
\end{aligned} \tag{4.11}$$

A type of no-signaling extension, in which we are interested, are quantum extensions. Here, the eavesdropper is in possession of a system E that extends the state $\rho_{\hat{A}\hat{B}\hat{C}}$ shared by Alice, Bob, and Charlie in the sense that the extension state $\rho_{\hat{A}\hat{B}\hat{C}E}$ satisfies $\rho_{\hat{A}\hat{B}\hat{C}} = \mathrm{Tr}_E[\rho_{\hat{A}\hat{B}\hat{C}E}]$. A quantum extension of a correlation is defined as follows:

$$\begin{aligned}
&\rho_{ABCEXYZ}\\
&= \sum_{a,b,c,x,y,z} q(x,y,z)\,|abcxyz\rangle\langle abcxyz|_{ABCXYZ} \otimes \mathrm{Tr}_{ABC}\Big[\Big(\Pi_a^{(x)} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)} \otimes \mathbb{I}_E\Big)\rho_{\hat{A}\hat{B}\hat{C}E}\Big]\\
&= \sum_{a,b,c,x,y,z} q(x,y,z)\,|abcxyz\rangle\langle abcxyz|_{ABCXYZ} \otimes p(a,b,c \,|\, x,y,z)\rho_E^{abcxyz}.
\end{aligned} \tag{4.12}$$

Notation 1 *Henceforth, we employ the shorthand*

$$[abcxyz]_{ABCXYZ} \equiv |abcxyz\rangle\langle abcxyz|_{ABCXYZ}\,, \tag{4.13}$$

for the sake of brevity.

The above no-signaling constraints and extensions, as well as quantum extensions, can be generalized to any multipartite scenario using the basic principle behind the no-signaling constraints. Appropriate no-signaling constraints apply when considering correlations involving multiple parties. Only after we have considered the no-signaling constraints can we begin to speak about what non-locality is and quantifying non-locality. To proceed, we need to define a quantity that can serve as a quantifier for multipartite non-locality.

4.3 Tripartite Intrinsic Non-Locality and its Properties

4.3.1 Conditional Total Correlation

In this subsection, we review the conditional total correlation and its properties [168] (see also [170, 169]), before defining our non-locality quantifier. We will discuss dual total correlation and its related non-locality quantifier in Section 4.8.

Total correlation is an M-partite generalization of mutual information. Conditional total correlation is the conditional version of total correlation, and it has

previously been used in various multipartite scenarios in quantum information [170, 169, 171, 174]. Conditional total correlation of a multipartite state $\rho_{A_1\cdots A_M E}$ is defined as

$$I(A_1;\cdots;A_M\,|\,E) \coloneqq \sum_{i=1}^{M} H(A_i\,|\,E) - H(A_1\cdots A_M\,|\,E), \tag{4.14}$$

where $H(A\,|\,E) \coloneqq H(AE) - H(E)$, and $H(A) \coloneqq -\mathrm{Tr}[\rho_A \log_2 \rho_A]$. The chain rule for the bipartite conditional mutual information is as follows:

$$I(A;BC\,|\,E) = I(A;B\,|\,CE) + I(A;C\,|\,E). \tag{4.15}$$

There exist chain rules for conditional total correlation [168, 169, 174], which are as follows:

$$I(BA_1;A_2;\cdots;A_M\,|\,E) = I(A_1;A_2;\cdots;A_M\,|\,BE) + \sum_{i=2}^{M} I(B;A_i\,|\,E), \tag{4.16}$$

$$I(A_1;\cdots;A_M\,|\,E) = \sum_{j=1}^{M-1} I(A_j;A_{j+1}\cdots A_M\,|\,E). \tag{4.17}$$

Let $\rho_{A_1\cdots A_M E}$ and $\sigma_{A_1\cdots A_M E}$ be multipartite states, for which each of the subsystems $A_1, \ldots, A_M$ are finite-dimensional. Suppose that $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$, where $\varepsilon \in [0,1]$. Then the following uniform continuity bound holds [175, Eq. (60)]:

$$|\, I(A_1;\cdots;A_M\,|\,E)_\rho - I(A_1;\cdots;A_M\,|\,E)_\sigma \,| \leq 2\varepsilon \log_2 \dim \mathcal{H}_{A_1\cdots A_{M-1}} + M g(\varepsilon), \tag{4.18}$$

where

$$g(\varepsilon) \coloneqq (\varepsilon+1)\log_2(\varepsilon+1) - \varepsilon \log_2 \varepsilon. \tag{4.19}$$

Conditional total correlation obeys data processing under local channels [169]:

$$I(A_1;\cdots;A_M\,|\,E)_\rho \geq I(\hat{A}_1;\cdots;\hat{A}_M\,|\,E)_\omega, \tag{4.20}$$

where

$$\omega_{\hat{A}_1\cdots\hat{A}_M E} \coloneqq \left(\mathcal{N}^{(1)}_{A_1\to\hat{A}_1}\otimes\cdots\otimes\mathcal{N}^{(M)}_{A_M\to\hat{A}_M}\right)\left(\rho_{\hat{A}_1\cdots\hat{A}_M E}\right), \tag{4.21}$$

and $\mathcal{N}^{(i)}_{A_i\to\hat{A}_i}$ is a channel, for $i\in\{1,\ldots,M\}$. We now define a first version of tripartite intrinsic non-locality.

Definition 15 *Let $p(a,b,c\,|\,x,y,z)$ be a no-signaling correlation. Tripartite intrinsic non-locality (TINL) of p is defined as*

$$N(A;B;C)_p \coloneqq \frac{1}{2}\sup_{q(x,y,z)}\inf_{\rho_{ABCXYZE}} I(A;B;C\,|\,EXYZ)_\rho, \tag{4.22}$$

where $q(x,y,z)$ is a probability distribution for the inputs of Alice, Bob, and Charlie and $\rho_{ABCXYZE}$ is a no-signaling extension of the state shared by Alice, Bob, and Charlie, given by

$$\rho_{ABCXYZE} = \sum_{a,b,c,x,y,z} q(x,y,z)\,p(a,b,c\,|\,x,y,z)\,[abcxyz]_{ABCXYZ}\otimes\rho_E^{abcxyz}. \tag{4.23}$$

Definition 16 *Quantum tripartite intrinsic non-locality (QTINL) of a quantum correlation $p(a,b,c\,|\,x,y,z)$ is defined as*

$$N_Q(A;B;C)_p \coloneqq \frac{1}{2}\sup_{q(x,y,z)}\inf_{\rho_{ABCXYZE}} I(A;B;C\,|\,EXYZ)_\rho, \tag{4.24}$$

where $q(x,y,z)$ is a probability distribution for the inputs of Alice, Bob, and Charlie and $\rho_{ABCXYZE}$ is a quantum extension, as in (4.12), of the state shared by Alice, Bob, and Charlie, given by

$$\rho_{ABCXYZE} = \sum_{a,b,c,x,y,z} q(x,y,z)\,p(a,b,c\,|\,x,y,z)\,[abcxyz]_{ABCXYZ}\otimes\rho_E^{abcxyz}. \tag{4.25}$$

The rest of this section is structured as follows. In Section 4.3.2, we derive the chain rule that will help us prove further theorems about tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality. In Section 4.3.3, we prove that tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality are additive. Additionally, we prove important properties of tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality, such as convexity and monotonicity under local operations and common randomness in Sections 4.4 and 4.5, respectively. We also prove in Section 4.6 that tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality vanish for local tripartite correlations. These results are important from a resource-theoretic perspective.

4.3.2 Chain Rule for Tripartite Conditional Total Correlation

Before we can prove additivity and other important properties of tripartite intrinsic non-locality, we need to establish a chain rule for the conditional total correlation of two rounds of the conference key agreement protocol:

$$I(A_1A_2; B_1B_2; C_1C_2 \,|\, E). \tag{4.26}$$

We will resolve this quantity into a sum of conditional total correlation terms related to the individual rounds of the protocol and other information theoretic quantities that depend on both rounds. These extra information-theoretic quantities are expressed as conditional mutual information quantities. Later in Theorem 27, we establish a general multipartite version of this chain rule.

Theorem 19 *For every state $\rho_{A_1B_1C_1A_2B_2C_2E}$, the following equality holds:*

$$I(A_1A_2;B_1B_2;C_1C_2\,|\,E)_\rho = I(A_1;B_1;C_1\,|\,EA_2B_2C_2)_\rho + I(A_2;B_2;C_2\,|\,E)_\rho + I(C_1;A_2B_2\,|\,EC_2)_\rho + I(A_1;B_2C_2\,|\,EA_2)_\rho + I(B_1;A_2C_2\,|\,EB_2)_\rho. \tag{4.27}$$

Proof. Consider that, by applying definitions and the chain rule for conditional entropy,

$$I(A_1A_2;B_1B_2;C_1C_2\,|\,E)$$

$$= H(A_1A_2\,|\,E) + H(B_1B_2\,|\,E) + H(C_1C_2\,|\,E) - H(A_1A_2B_1B_2C_1C_2\,|\,E) \tag{4.28}$$

$$= H(A_2\,|\,E) + H(A_1\,|\,EA_2) + H(B_2\,|\,E) + H(B_1\,|\,EB_2) + H(C_2\,|\,E) + H(C_1\,|\,EC_2) - H(A_2B_2C_2\,|\,E) - H(A_1B_1C_1\,|\,EA_2B_2C_2) \tag{4.29}$$

$$= I(A_2;B_2;C_2\,|\,E) + H(A_1\,|\,EA_2) + H(B_1\,|\,EB_2) + H(C_1\,|\,EC_2) - H(A_1B_1C_1\,|\,EA_2B_2C_2). \tag{4.30}$$

Then consider that

$$H(A_1\,|\,EA_2) + H(B_1\,|\,EB_2) + H(C_1\,|\,EC_2) - H(A_1B_1C_1\,|\,EA_2B_2C_2)$$

$$= H(A_1\,|\,EA_2) + H(B_1\,|\,EB_2) + H(C_1\,|\,EC_2) - H(A_1B_1C_1\,|\,EA_2B_2C_2) + H(A_1\,|\,EA_2B_2C_2) - H(A_1\,|\,EA_2B_2C_2) + H(B_1\,|\,EA_2B_2C_2) - H(B_1\,|\,EA_2B_2C_2) + H(C_1\,|\,EA_2B_2C_2) - H(C_1\,|\,EA_2B_2C_2) \tag{4.31}$$

$$= I(A_1;B_1;C_1\,|\,EA_2B_2C_2) + H(A_1\,|\,EA_2) - H(A_1\,|\,EA_2B_2C_2) + H(B_1\,|\,EB_2) - H(B_1\,|\,EA_2B_2C_2) + H(C_1\,|\,EC_2) - H(C_1\,|\,EA_2B_2C_2) \tag{4.32}$$

$$= I(A_1;B_1;C_1\,|\,EA_2B_2C_2) + I(A_1;B_2C_2\,|\,EA_2) + I(B_1;A_2C_2\,|\,EB_2) + I(C_1;A_2B_2\,|\,EC_2). \tag{4.33}$$

This concludes the proof. ■

4.3.3 Additivity

In this section, we prove that tripartite intrinsic non-locality is additive. This is indeed essential for the tripartite intrinsic non-locality to be a useful upper bound on DI conference key agreement capacity.

Theorem 20 (Additivity of TINL) *Let* $p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2)$ *be a no-signaling correlation for which no-signaling constraints hold for all parties. For example, the no-signaling constraints for Alice are as follows:*

$$\sum_{a_1} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = \sum_{a_1} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, \bar{x}_1, x_2, y_1, y_2, z_1, z_2) \quad \forall x_1, \bar{x}_1, \tag{4.34}$$

$$\sum_{a_2} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = \sum_{a_2} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, \bar{x}_2, y_1, y_2, z_1, z_2) \quad \forall x_2, \bar{x}_2. \tag{4.35}$$

Suppose that similar constraints hold for Bob and Charlie as well. Let $t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1)$ *and* $r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2)$ *be no-signaling correlations corresponding to the marginals of* p*. Then the intrinsic non-locality is superadditive, in the sense that*

$$N(A_1A_2; B_1B_2; C_1C_2)_p \geq N(A_1; B_1; C_1)_t + N(A_2; B_2; C_2)_r. \tag{4.36}$$

If

$$p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1) r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2), \tag{4.37}$$

then the intrinsic non-locality is additive in the following sense:

$$N(A_1A_2;B_1B_2;C_1C_2)_p = N(A_1;B_1;C_1)_t + N(A_2;B_2;C_2)_r. \tag{4.38}$$

No-signaling constraints like (4.34)–(4.35) can in principle be enforced by a party performing parallel measurements shielded from each other, such as Alice recording a_1 and a_2 at separate locations between which communication is not possible. The stronger product assumption in (4.37) cannot be enforced in this way, but the condition will hold in the natural setting of sequential experimental trials in which an i.i.d. assumption is made.

Proof of Theorem 20. We first prove that tripartite intrinsic non-locality is superadditive in the sense of (4.36), and then we prove it is subadditive when (4.37) holds. Additivity when (4.37) holds then follows as a consequence.

First, let us prove superadditivity. To begin, let us consider states that arise from embedding an arbitrary no-signaling extension of $p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2)$ into the following quantum state:

$$\begin{aligned}\zeta_{A_1B_1C_1A_2B_2C_2EX_1X_2Y_1Y_2Z_1Z_2} = \\ \sum_{\substack{a_1,b_1,c_1,a_2,b_2,c_2,\\ x_1,y_1,z_1,x_2,y_2,z_2}} q(x_1,y_1,z_1,x_2,y_2,z_2)\, p(a_1,b_1,c_1,a_2,b_2,c_2 \,|\, x_1,y_1,z_1,x_2,y_2,z_2) \\ [a_1b_1c_1a_2b_2c_2x_1y_1z_1x_2y_2z_2]_{A_1B_1C_1A_2B_2C_2X_1X_2Y_1Y_2Z_1Z_2} \otimes \rho_E^{a_1b_1c_1a_2b_2c_2x_1y_1z_1x_2y_2z_2}.\end{aligned} \tag{4.39}$$

We define the states τ and γ to be the following arbitrary no-signaling extensions of t and r, respectively:

$$\tau_{A_1B_1C_1EX_1Y_1Z_1} = \sum_{a_1,b_1,c_1,x_1,y_1,z_1} q(x_1,y_1,z_1)\, t(a_1,b_1,c_1 \,|\, x_1,y_1,z_1)$$
$$[a_1b_1c_1x_1y_1z_1]_{A_1B_1C_1X_1Y_1Z_1} \otimes \rho_E^{a_1b_1c_1x_1y_1z_1}, \quad (4.40)$$

and

$$\gamma_{A_2B_2C_2EX_2Y_2Z_2} = \sum_{a_2,b_2,c_2,x_2,y_2,z_2} q(x_2,y_2,z_2)\, r(a_2,b_2,c_2 \,|\, x_2,y_2,z_2)$$
$$[a_2b_2c_2x_2y_2z_2]_{A_2B_2C_2X_2Y_2Z_2} \otimes \rho_E^{a_2b_2c_2x_2y_2z_2}. \quad (4.41)$$

Now, we use the chain rule from Theorem 19 to conclude that

$$\begin{aligned}
&I(A_1A_2;B_1B_2;C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&= I(A_1;B_1;C_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2A_2B_2C_2)_\zeta + I(A_2;B_2;C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&\quad + I(A_2B_2;C_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2C_2)_\zeta + I(B_2C_2;A_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2A_2)_\zeta \\
&\quad + I(A_2C_2;B_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2B_2)_\zeta \quad (4.42)
\end{aligned}$$

Since conditional mutual information is always non-negative, we conclude that

$$\begin{aligned}
&I(A_1A_2;B_1B_2;C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&\geq I(A_1;B_1;C_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2A_2B_2C_2)_\zeta + I(A_2;B_2;C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta. \quad (4.43)
\end{aligned}$$

The state $\zeta_{A_1B_1C_1A_2B_2C_2EX_1X_2Y_1Y_2Z_1Z_2}$ is a valid no-signaling extension of t with extension systems $EX_2Y_2Z_2A_2B_2C_2$, and the state $\zeta_{A_2B_2C_2EX_1X_2Y_1Y_2Z_1Z_2}$ is a valid no-signaling extension of r with extension systems $EX_1Y_1Z_1$. So we conclude that

$$\begin{aligned}
&I(A_1A_2;B_1B_2;C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&\geq I(A_1;B_1;C_1 \,|\, EX_1X_2Y_1Y_2Z_1Z_2A_2B_2C_2)_\zeta + I(A_2;B_2;C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \quad (4.44)
\end{aligned}$$

$$\geq \inf_{\text{ext. in (4.40)}} I(A_1; B_1; C_1 \,|\, EX_1Y_1Z_1)_\tau + \inf_{\text{ext. in (4.41)}} I(A_2; B_2; C_2 \,|\, EX_2Y_2Z_2)_\gamma. \tag{4.45}$$

Since the state $\zeta_{A_1B_1C_1A_2B_2C_2EX_1X_2Y_1Y_2Z_1Z_2}$ is an arbitrary no-signaling extension of p, we conclude that

$$\begin{aligned}
&\inf_{\text{ext. in (4.39)}} I(A_1A_2; B_1B_2; C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&\qquad \geq \inf_{\text{ext. in (4.40)}} I(A_1; B_1; C_1 \,|\, EX_1Y_1Z_1)_\tau + \inf_{\text{ext. in (4.41)}} I(A_2; B_2; C_2 \,|\, EX_2Y_2Z_2)_\gamma.
\end{aligned} \tag{4.46}$$

By optimizing over product input probability distributions, we have that

$$\begin{aligned}
&\sup_{q(x_1,y_1,z_1)q(x_2,y_2,z_2)} \inf_{\text{ext. in (4.39)}} I(A_1A_2; B_1B_2; C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta \\
&\qquad \geq \sup_{q(x_1,y_1,z_1)} \inf_{\text{ext. in (4.40)}} I(A_1; B_1; C_1 \,|\, EX_1Y_1Z_1)_\tau + \\
&\qquad\qquad \sup_{q(x_2,y_2,z_2)} \inf_{\text{ext. in (4.41)}} I(A_2; B_2; C_2 \,|\, EX_2Y_2Z_2)_\gamma.
\end{aligned} \tag{4.47}$$

Hence, by optimizing the left-hand side over all input probability distributions, we conclude that

$$N(A_1A_2; B_1B_2; C_1C_2)_p \geq N(A_1; B_1; C_1)_t + N(A_2; B_2; C_2)_r. \tag{4.48}$$

This concludes the proof of superadditivity (i.e., the proof of (4.36)).

Let us prove subadditivity when (4.37) holds; i.e., let us prove that

$$N(A_1A_2; B_1B_2; C_1C_2)_p \leq N(A_1; B_1; C_1)_t + N(A_2; B_2; C_2)_r. \tag{4.49}$$

Consider the following quantum embeddings:

$$\zeta_{A_1B_1C_1A_2B_2C_2EX_1X_2Y_1Y_2Z_1Z_2} =$$

$$\sum_{\substack{a_1,b_1,c_1,a_2,b_2,c_2,\\ x_1,y_1,z_1,x_2,y_2,z_2}} q(x_1,y_1,z_1,x_2,y_2,z_2)t(a_1,b_1,c_1\,|\,x_1,y_1,z_1)r(a_2,b_2,c_2\,|\,x_2,y_2,z_2)$$

$$[a_1b_1c_1a_2b_2c_2x_1y_1z_1x_2y_2z_2]_{A_1B_1C_1A_2B_2C_2X_1X_2Y_1Y_2Z_1Z_2} \otimes \zeta_E^{a_1b_1c_1x_1y_1z_1a_2b_2c_2x_2y_2z_2} \tag{4.50}$$

$$\rho_{A_1B_1C_1A_2B_2C_2X_1X_2Y_1Y_2Z_1Z_2E_1E_2} =$$

$$\sum_{\substack{a_1,b_1,c_1,a_2,b_2,c_2,\\ x_1,y_1,z_1,x_2,y_2,z_2}} q(x_1,y_1,z_1,x_2,y_2,z_2)t(a_1,b_1,c_1\,|\,x_1,y_1,z_1)r(a_2,b_2,c_2\,|\,x_2,y_2,z_2)$$

$$[a_1b_1c_1a_2b_2c_2x_1y_1z_1x_2y_2z_2]_{A_1B_1C_1A_2B_2C_2X_1X_2Y_1Y_2Z_1Z_2} \otimes \rho_{E_1}^{a_1b_1c_1x_1y_1z_1} \otimes \rho_{E_2}^{a_2b_2c_2x_2y_2z_2}, \tag{4.51}$$

$$\tau_{A_1B_1C_1EX_1Y_1Z_1} =$$

$$\sum_{a_1,b_1,c_1,x_1,y_1,z_1} q(x_1,y_1,z_1)\, t(a_1,b_1,c_1\,|\,x_1,y_1,z_1)\, [a_1b_1c_1x_1y_1z_1]_{A_1B_1C_1X_1Y_1Z_1} \otimes \rho_{E_1}^{a_1b_1c_1x_1y_1z_1}, \tag{4.52}$$

and

$$\gamma_{A_2B_2C_2EX_2Y_2Z_2} =$$

$$\sum_{a_2,b_2,c_2,x_2,y_2,z_2} q(x_2,y_2,z_2)\, r(a_2,b_2,c_2\,|\,x_2,y_2,z_2)\, [a_2b_2c_2x_2y_2z_2]_{A_2B_2C_2X_2Y_2Z_2} \otimes \rho_{E_2}^{a_2b_2c_2x_2y_2z_2}. \tag{4.53}$$

All the extensions above are no-signaling extensions. Consider that

$$\inf_{\text{ext. in (4.50)}} I(A_1A_2;B_1B_2;C_1C_2\,|\,EX_1X_2Y_1Y_2Z_1Z_2)_\zeta$$

$$\leq I(A_1A_2;B_1B_2;C_1C_2\,|\,E_1E_2X_1X_2Y_1Y_2Z_1Z_2)_\rho. \tag{4.54}$$

Using the chain rule from Theorem 19, we find that

$$I(A_1A_2;B_1B_2;C_1C_2\,|\,E_1E_2X_1X_2Y_1Y_2Z_1Z_2)_\rho$$

$$= I(A_1; B_1; C_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2A_2B_2C_2)_\rho + I(A_2; B_2; C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2)_\rho$$
$$+ I(A_2B_2; C_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2C_2)_\rho + I(B_2C_2; A_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2A_2)_\rho$$
$$+ I(A_2C_2; B_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho. \tag{4.55}$$

We can write $I(A_2C_2; B_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho$ as follows:

$$I(A_2C_2; B_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho$$
$$= H(A_2C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho - H(A_2C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2B_1)_\rho \tag{4.56}$$
$$= \sum_{x_1,y_1,z_1,x_2,y_2,z_2} p(x_1, y_1, z_1, x_2, y_2, z_2) \,[\, H(A_2C_2 \,|\, E_1E_2B_2)_{\eta^{x_1y_1z_1x_2y_2z_2}}$$
$$- H(A_2C_2 \,|\, E_1E_2B_2B_1)_{\eta^{x_1y_1z_1x_2y_2z_2}} \,], \tag{4.57}$$

where, due to the no-signaling constraints on p, t, and r, we can write

$$\eta^{x_1y_1z_1x_2y_2z_2}_{B_1A_2B_2C_2E_1E_2} = \sum_{b_1} t(b_1 \,|\, y_1) \,[b_1] \otimes \rho^{b_1y_1}_{E_1} \otimes \sum_{a_2,b_2,c_2} r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2) \,[a_2b_2c_2] \otimes \rho^{a_2b_2c_2x_2y_2z_2}_{E_2}, \tag{4.58}$$

and

$$\eta^{x_1y_1z_1x_2y_2z_2}_{A_2B_2C_2E_1E_2} = \sum_{a_2,b_2,c_2} r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2) \,[a_2b_2c_2] \otimes \rho^{a_2b_2c_2x_2y_2z_2}_{E_2} \otimes \rho_{E_1}, \tag{4.59}$$

where

$$\rho^{b_1y_1}_{E_1} = \sum_{a_1,c_1} t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1) \,\rho^{a_1b_1c_1x_1y_1z_1}_{E_1}, \tag{4.60}$$
$$\rho_{E_1} = \sum_{a_1,b_1,c_1} t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1) \,\rho^{a_1b_1c_1x_1y_1z_1}_{E_1}. \tag{4.61}$$

From the above definitions, we can conclude that

$$H(A_2C_2 \,|\, E_1E_2B_2B_1)_{\eta^{x_1y_1z_1x_2y_2z_2}} = H(A_2C_2 \,|\, E_1E_2B_2)_{\eta^{x_1y_1z_1x_2y_2z_2}}. \tag{4.62}$$

Hence,

$$I(A_2C_2; B_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho$$
$$= H(A_2C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho - H(A_2C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho = 0. \quad (4.63)$$

The quantities $I(B_2C_2; A_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2A_2)_\rho$ and $I(A_2C_2; B_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2B_2)_\rho$ are equal to zero using similar arguments. This leads to the following conclusion:

$$\inf_{\text{ext. in (4.50)}} I(A_1A_2; B_1B_2; C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta$$
$$\leq I(A_1A_2; B_1B_2; C_1C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2)_\rho$$
$$= I(A_1; B_1; C_1 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2A_2B_2C_2)_\rho + I(A_2; B_2; C_2 \,|\, E_1E_2X_1X_2Y_1Y_2Z_1Z_2)_\rho$$
$$= I(A_1; B_1; C_1 \,|\, E_1X_1Y_1Z_1)_\tau + I(A_2; B_2; C_2 \,|\, E_2X_2Y_2Z_2)_\gamma, \quad (4.64)$$

where the last line follows from the structure of the state in (4.51) and the fact that the extension is a no-signaling extension. Since the no-signaling extensions τ and γ are arbitrary, we conclude that

$$\inf_{\text{ext. in (4.50)}} I(A_1A_2; B_1B_2; C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta$$
$$\leq \inf_{\text{ext. in (4.52)}} I(A_1; B_1; C_1 \,|\, EX_1Y_1Z_1)_\tau + \inf_{\text{ext. in (4.53)}} I(A_2; B_2; C_2 \,|\, EX_2Y_2Z_2)_\gamma. \quad (4.65)$$

Now optimizing over arbitrary input probability distributions, we find that

$$\sup_q \inf_{\text{ext. in (4.50)}} I(A_1A_2; B_1B_2; C_1C_2 \,|\, EX_1X_2Y_1Y_2Z_1Z_2)_\zeta$$
$$\leq \sup_q \inf_{\text{ext. in (4.52)}} I(A_1; B_1; C_1 \,|\, EX_1Y_1Z_1)_\tau + \sup_q \inf_{\text{ext. in (4.53)}} I(A_2; B_2; C_2 \,|\, EX_2Y_2Z_2)_\gamma. \quad (4.66)$$

Hence,

$$N(A_1A_2; B_1B_2; C_1C_2)_p \leq N(A_1; B_1; C_1)_t + N(A_2; B_2; C_2)_r. \quad (4.67)$$

Putting together (4.48) and (4.67), we have established additivity (i.e., we have proven (4.38)). ■

Theorem 21 (Additivity of QTINL) *Let* $p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2)$ *be a quantum correlation for which no-signaling constraints hold for all parties. For example, the no-signaling constraints for Alice are as follows:*

$$\sum_{a_1} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = \sum_{a_1} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, \bar{x}_1, x_2, y_1, y_2, z_1, z_2) \quad \forall x_1, \bar{x}_1, \tag{4.68}$$

$$\sum_{a_2} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = \sum_{a_2} p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, \bar{x}_2, y_1, y_2, z_1, z_2) \quad \forall x_2, \bar{x}_2. \tag{4.69}$$

Suppose that similar constraints hold for Bob and Charlie as well. Let $t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1)$ *and* $r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2)$ *be quantum correlations corresponding to the marginals of* p*. Then the quantum intrinsic non-locality is superadditive, in the sense that*

$$N_Q(A_1A_2; B_1B_2; C_1C_2)_p \geq N_Q(A_1; B_1; C_1)_t + N_Q(A_2; B_2; C_2)_r. \tag{4.70}$$

If

$$p(a_1, a_2, b_1, b_2, c_1, c_2 \,|\, x_1, x_2, y_1, y_2, z_1, z_2) = t(a_1, b_1, c_1 \,|\, x_1, y_1, z_1) r(a_2, b_2, c_2 \,|\, x_2, y_2, z_2), \tag{4.71}$$

then the quantum intrinsic non-locality is additive in the following sense:

$$N_Q(A_1A_2; B_1B_2; C_1C_2)_p = N_Q(A_1; B_1; C_1)_t + N_Q(A_2; B_2; C_2)_r. \tag{4.72}$$

Proof. The proof follows by using similar techniques as Theorem 20 and by taking appropriate quantum extensions. ■

4.4 Convexity

Convexity of tripartite intrinsic non-locality is another important property because convex combinations of no-signaling correlations are also valid no-signaling correlations. This is also the case for quantum correlations [176].

Theorem 22 (Convexity of TINL) *Let $t(a,b,c\,|\,x,y,z)$ and $r(a,b,c\,|\,x,y,z)$ be two no-signaling correlations, and let $\lambda \in [0,1]$. Let $p(a,b,c\,|\,x,y,c)$ be a mixture of the two correlations, defined as*

$$p(a,b,c\,|\,x,y,c) = \lambda\, t(a,b,c\,|\,x,y,z) + (1-\lambda) r(a,b,c\,|\,x,y,z). \tag{4.73}$$

Then,

$$N(A;B;C)_p \leq \lambda N(A;B;C)_t + (1-\lambda) N(A;B;C)_r. \tag{4.74}$$

Proof. Consider the quantum embeddings of arbitrary no-signaling extensions of t, r, and p:

$$\tau_{ABCEXYZ} = \sum_{a,b,c,x,y,z} p(x,y,z) t(a,b,c\,|\,x,y,z) [abcxyz]_{ABCXYZ} \otimes \tau_E^{abcxyz}, \tag{4.75}$$

$$\gamma_{ABCEXYZ} = \sum_{a,b,c,x,y,z} p(x,y,z) r(a,b,c\,|\,x,y,z) [abcxyz]_{ABCXYZ} \otimes \gamma_E^{abcxyz}, \tag{4.76}$$

and

$$\begin{aligned}\zeta_{ABCEXYZ} &= \sum_{a,b,c,x,y,z} p(x,y,z)p(a,b,c\,|\,x,y,z)[abcxyz]_{ABCXYZ} \otimes \rho_E^{abcxyz} \\ &= \sum_{a,b,c,x,y,z} p(x,y,z)\{(\lambda)t(a,b,c\,|\,x,y,z) + (1-\lambda)r(a,b,c\,|\,x,y,z)\} \\ &\qquad \times [abcxyz]_{ABCXYZ} \otimes \rho_E^{abcxyz}. \end{aligned} \tag{4.77}$$

A particular no-signaling extension of (4.77) is as follows:

$$\begin{aligned}\rho_{ABCEXYZ\Lambda} = \sum_{a,b,c,x,y,z,\lambda} & p(x,y,z)\{(\lambda)t(a,b,c\,|\,x,y,z)[a,b,c,x,y,z]_{ABCXYZ} \otimes \tau_E^{abcxyz} \otimes [0]_\Lambda \\ & + (1-\lambda)r(a,b,c\,|\,x,y,z)[abcxyz]_{ABCXYZ} \otimes \gamma_E^{abcxyz} \otimes [1]_\Lambda\}. \end{aligned} \tag{4.78}$$

Consider then

$$\begin{aligned} & \inf_{\text{ext. in (4.77)}} I(A;B;C\,|\,EXYZ)_\zeta \\ & \leq I(A;B;C\,|\,EXYZ\Lambda)_\rho & (4.79) \\ & = (\lambda)I(A;B;C\,|\,EXYZ)_\tau + (1-\lambda)I(A;B;C\,|\,EXYZ)_\gamma & (4.80) \\ & \leq (\lambda) \inf_{\text{ext. in (4.75)}} I(A;B;C\,|\,EXYZ)_\tau + (1-\lambda) \inf_{\text{ext. in (4.76)}} I(A;B;C\,|\,EXYZ)_\gamma. & (4.81) \end{aligned}$$

The first inequality holds because we picked a particular no-signaling extension. The second inequality holds due to the convexity of the individual terms in the definition of conditional total correlation. Since τ and γ are arbitrary no-signaling extensions of t and r, and optimizing over arbitrary input probability distributions, we find that

$$\sup_q \inf_{\text{ext. in (4.77)}} I(A;B;C\,|\,EXYZ)_p$$

$$\leq (\lambda) \sup_{q} \inf_{\text{ext. in (4.75)}} I(A;B;C\,|\,EXYZ)_t + (1-\lambda) \sup_{q} \inf_{\text{ext. in (4.76)}} I(A;B;C\,|\,EXYZ)_r. \quad (4.82)$$

This concludes the proof. ■

Theorem 23 (Convexity of QTINL) *Let $t(a,b,c\,|\,x,y,z)$ and $r(a,b,c\,|\,x,y,z)$ be two quantum correlations, and let $\lambda \in [0,1]$. Let $p(a,b,c\,|\,x,y,c)$ be a mixture of the two correlations, defined as*

$$p(a,b,c\,|\,x,y,c) = \lambda t(a,b,c\,|\,x,y,z) + (1-\lambda) r(a,b,c\,|\,x,y,z). \quad (4.83)$$

Then,

$$N_Q(A;B;C)_p \leq \lambda N_Q(A;B;C)_t + (1-\lambda) N_Q(A;B;C)_r. \quad (4.84)$$

Proof. Consider the following quantum extensions of t, r, and p:

$$\tau_{ABCEXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z) t(a,b,c\,|\,x,y,z) [abcxyz]_{ABCXYZ} \otimes \tau_E^{abcxyz}, \quad (4.85)$$

$$\gamma_{ABCEXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z) r(a,b,c\,|\,x,y,z) [abcxyz]_{ABCXYZ} \otimes \gamma_E^{abcxyz}, \quad (4.86)$$

$$\zeta_{ABCEXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z) p(a,b,c\,|\,x,y,z) [abcxyz]_{ABCXYZ} \otimes \rho_E^{abcxyz}. \quad (4.87)$$

Let $\tau_{\hat{A}\hat{B}\hat{C}}$ be a quantum state that, along with the POVMs characterized by $\{\Pi_a^{(x)}\}_a$, $\{\Pi_b^{(y)}\}_b$, and $\{\Pi_c^{(z)}\}_c$, yield the correlation $t(a,b,c\,|\,x,y,c)$. Let $\tau_{\hat{A}\hat{B}\hat{C}E}$ be a quantum extension of $\tau_{\hat{A}\hat{B}\hat{C}}$. Similarly, let $\gamma_{\hat{A}\hat{B}\hat{C}}$ be a quantum state that, along with the POVMs characterized by $\{\Lambda_a^{(x)}\}_a$, $\{\Lambda_b^{(y)}\}_b$, and $\{\Lambda_c^{(z)}\}_c$, yield the correlation $r(a,b,c\,|\,x,y,z)$. Let $\gamma_{\hat{A}\hat{B}\hat{C}E}$ be a quantum extension of $\gamma_{\hat{A}\hat{B}\hat{C}}$. Then, a particular quantum state that realizes the correlation $p(a,b,c\,|\,x,y,z)$ is the following:

$$\rho_{\hat{A}\hat{B}\hat{C}A'B'C'} = \lambda \tau_{\hat{A}\hat{B}\hat{C}} \otimes |000\rangle\langle 000|_{A'B'C'} + (1-\lambda) \gamma_{\hat{A}\hat{B}\hat{C}} \otimes |111\rangle\langle 111|_{A'B'C'}. \quad (4.88)$$

Then,

$$p(a,b,c\,|\,x,y,z) = \text{Tr}\Big[\Pi_a^{(x)} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)} \otimes |000\rangle\langle 000|_{A'B'C'} (\rho_{\hat{A}\hat{B}\hat{C}A'B'C'})\Big] + \\ \text{Tr}\Big[\Lambda_a^{(x)} \otimes \Lambda_b^{(y)} \otimes \Lambda_c^{(z)} \otimes |111\rangle\langle 111|_{A'B'C'} (\rho_{\hat{A}\hat{B}\hat{C}A'B'C'})\Big], \quad (4.89)$$

where it is understood that Alice is measuring σ_Z on her system A', Bob is measuring σ_Z on B', and Charlie is measuring σ_Z on C', in addition to the other measurements on their systems A, B, and C. Now, consider the following quantum extension of $\rho_{ABCA'B'C'}$,

$$\rho_{\hat{A}\hat{B}\hat{C}A'B'C'} = \lambda \tau_{\hat{A}\hat{B}\hat{C}E} \otimes |0000\rangle\langle 0000|_{A'B'C'E'} + (1-\lambda)\gamma_{\hat{A}\hat{B}\hat{C}E} \otimes |1111\rangle\langle 1111|_{A'B'C'E'}. \quad (4.90)$$

Furthermore, consider the following particular quantum extension of $\zeta_{ABCEXYZ}$:

$$\rho_{ABCXYZEE'} = \sum_{a,b,c,x,y,z} p(x,y,z)\{(\lambda)t(a,b,c\,|\,x,y,z)[a,b,c,x,y,z] \otimes \tau_E^{abcxyz} \otimes [0]_{E'} \\ + (1-\lambda)r(a,b,c\,|\,x,y,z)[a,b,c,x,y,z] \otimes \gamma_E^{abcxyz} \otimes [1]_{E'}\}.$$

Then following similar arguments given in the proof of Theorem 22, we obtain

$$N_Q(A;B;C)_p \leq \lambda N_Q(A;B;C)_t + (1-\lambda) N_Q(A;B;C)_r. \quad (4.91)$$

This concludes the proof. ■

4.5 Monotonicity under Local Operations and Common Randomness

Local Operations and Common Randomness (LOCR) is the set of free operations within the setup of conference key agreement. These free operations are chosen so that they are consistent with the prerequisites of the parity-CHSH game [3], which are similar to those of the CHSH game [177, 178]. By common randomness, we mean that all parties have access to a common random variable and an instance that is made available to all parties before each round of the protocol. Using this common randomness, all parties can perform local operations and pre- and post-processing on their inputs and outputs. LOCR can be applied to an input distribution $p_i(a,b,c\,|\,x,y,z)$ to arrive at an output distribution $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ as follows:

$$p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f) = \sum_{a,b,c,x,y,z} O^{(L)}(a_f,b_f,c_f\,|\,x_f,y_f,z_f,a,b,c,x,y,z) \\ p_i(a,b,c\,|\,x,y,z) I^{(L)}(x,y,z\,|\,x_f,y_f,z_f), \quad (4.92)$$

where

$$O^{(L)}(a_f,b_f,c_f\,|\,x_f,y_f,z_f,a,b,c,x,y,z) = \sum_{\lambda_2} p(\lambda_2) O_A(a_f\,|\,a,x,x_f,\lambda_2) \\ \times O_B(b_f\,|\,b,y,y_f,\lambda_2) O_C(c_f\,|\,c,z,z_f,\lambda_2), \quad (4.93)$$

and

$$I^{(L)}(x,y,z\,|\,x_f,y_f,z_f) = \sum_{\lambda_1} p(\lambda_1) I_A(x\,|\,x_f,\lambda_1) I_B(y\,|\,y_f,\lambda_1) I_C(z\,|\,z_f,\lambda_1). \quad (4.94)$$

The bipartite case has been considered previously in [179]. In the above equations, O_A, O_B, O_C, I_A, I_B, and I_C are the pre-agreed local operations, and λ_1 and λ_2 represent the common randomness shared between the parties before and after obtaining the outputs from the initial correlation, respectively.

Theorem 24 (Monotonicity under LOCR) *Let $p_i(a,b,c\,|\,x,y,z)$ be a no-signaling correlation, and let $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ result from the action of local operations and common randomness on $p_i(a,b,c\,|\,x,y,z)$, as described in (4.92). Then,*

$$N(A_i;B_i;C_i)_{p_i} \geq N(A_i;B_f;C_f)_{p_f}. \tag{4.95}$$

Proof. Consider the following respective no-signaling extensions of $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ and $p_i(a,b,c\,|\,x,y,z)$:

$$\zeta_{A_fB_fC_fEX_fY_fZ_f} = \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f)p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f) \\ [a_fb_fc_fx_fy_fz_f]_{A_fB_fC_fEX_fY_fZ_f} \otimes \zeta_E^{a_f,b_f,c_fx_f,y_f,z_f}, \tag{4.96}$$

and

$$\tau_{ABCEXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z)p_i(a,b,c\,|\,x,y,z)[abcxyz]_{ABCEXYZ} \otimes \rho_E^{abcxyz}. \tag{4.97}$$

Let us embed $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ in the following quantum state:

$$\rho_{A_fB_fC_fX_fY_fZ_f} = \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f) \sum_{a,b,c,x,y,z} \sum_{\lambda_2} p(\lambda_2)O_A(a_f\,|\,a,x,x_f,\lambda_2) \\ O_B(b_f\,|\,b,y,y_f,\lambda_2)O_C(c_f\,|\,c,z,z_f,\lambda_2)p_i(a,b,c\,|\,x,y,z) \sum_{\lambda_1} p(\lambda_1)I_A(x\,|\,x_f,\lambda_1)I_B(y\,|\,y_f,\lambda_1)$$

$$I_B(y\,|\,y_f,\lambda_1)I_C(z\,|\,z_f,\lambda_1)[a_f b_f c_f x_f y_f z_f]_{A_f B_f C_f X_f Y_f Z_f}. \quad (4.98)$$

A particular no-signaling extension of this state is as follows:

$$\begin{aligned}
&\rho_{ABCA_fB_fC_fEXYZX_fY_fZ_f\Lambda_1\Lambda_2} \\
&= \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f) \sum_{a,b,c,x,y,z} \sum_{\lambda_2} p(\lambda_2) O_A(a_f\,|\,a,x,x_f,\lambda_2) O_B(b_f\,|\,b,y,y_f,\lambda_2)\times \\
&\qquad O_C(c_f\,|\,c,z,z_f,\lambda_2) p_i(a,b,c\,|\,x,y,z) \sum_{\lambda_1} p(\lambda_1) I_A(x\,|\,x_f,\lambda_1) I_B(y\,|\,y_f,\lambda_1) I_B(y\,|\,y_f,\lambda_1)\times \\
&\qquad I_C(z\,|\,z_f,\lambda_1)[abcxyza_f b_f c_f x_f y_f z_f]_{ABCA_fB_fC_fXYZX_fY_fZ_f} \otimes \rho_E^{abcxyz} \otimes [\lambda_1\lambda_2]_{\Lambda_1\Lambda_2}.
\end{aligned} \quad (4.99)$$

Now let us begin with the following inequality:

$$\inf_{\text{ext. in (4.96)}} I(A_f;B_f;C_f\,|\,EX_fY_fZ_f)_\zeta \leq I(A_f;B_f;C_f\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho. \quad (4.100)$$

The above inequality holds for a specific choice $\rho_{ABCA_fB_fC_fEXYZX_fY_fZ_f\Lambda_1\Lambda_2}$ of a no-signaling extension of $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$. Using data processing of conditional total correlation under local channels, we find that

$$I(A_f;B_f;C_f\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho \leq I(AXX_f\Lambda_2;BYY_f\Lambda_2;CZZ_f\Lambda_2\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho. \quad (4.101)$$

Since X_f, Y_f, Z_f, and Λ_2 are classical copies of themselves, it follows that

$$\begin{aligned}
&I(AXX_f\Lambda_2;BYY_f\Lambda_2;CZZ_f\Lambda_2\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho \\
&\qquad = I(AX;BY;CZ\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho.
\end{aligned} \quad (4.102)$$

Since none of A, X, B, Y, C, and Z depend on Λ_2, we conclude that

$$I(AX;BY;CZ\,|\,EX_fY_fZ_f\Lambda_1\Lambda_2)_\rho = I(AX;BY;CZ\,|\,EX_fY_fZ_f\Lambda_1)_\rho. \quad (4.103)$$

Hence,

$$\inf_{\text{ext. in (4.96)}} I(A_f; B_f; C_f \,|\, EX_fY_fZ_f)_\zeta \leq I(AX; BY; CZ \,|\, EX_fY_fZ_f\Lambda_1)_\rho. \tag{4.104}$$

Using (4.27), we find that

$$\begin{aligned} I(AX; BY; CZ \,|\, EX_fY_fZ_f\Lambda_1)_\rho &= I(A; B; C \,|\, EX_fY_fZ_f\Lambda_1XYZ)_\rho \\ &\quad + I(X; Y; Z \,|\, YEX_fY_fZ_f\Lambda_1)_\rho + I(YZ; A \,|\, XEX_fY_fZ_f\Lambda_1)_\rho \\ &\quad + I(XZ; B \,|\, YEX_fY_fZ_f\Lambda_1)_\rho + I(XY; C \,|\, ZEX_fY_fZ_f\Lambda_1)_\rho. \end{aligned} \tag{4.105}$$

The information-theoretic quantities $I(YZ; A \,|\, XEX_fY_fZ_f\Lambda_1)_\rho$, $I(XZ; B \,|\, YEX_fY_fZ_f\Lambda_1)_\rho$, and $I(XY; C \,|\, ZEX_fY_fZ_f\Lambda_1)_\rho$ are equal to zero due to the no-signaling constraints elucidated in (4.5) and the structure in (4.94) of the local box I_L. The information-theoretic quantity $I(X; Y; Z \,|\, YEX_fY_fZ_f\Lambda_1)_\rho$ is equal to zero due to (4.94). The structure of ρ implies that all the terms are equal to zero, except for the first term. So,

$$\begin{aligned} \inf_{\text{ext. in (4.96)}} I(A_i; B_f; C_f \,|\, EX_fY_fZ_f)_\zeta &\leq I(A; B; C \,|\, XYZEX_fY_fZ_f\Lambda_1)_\rho & (4.106) \\ &= I(A; B; C \,|\, XYZE)_\tau, & (4.107) \end{aligned}$$

where the equality is a consequence of the structure of $\rho_{ABCEXYZX_fY_fZ_f\Lambda_1}$. Since τ is an arbitrary no-signaling extension of p_i, we conclude that

$$\inf_{\text{ext. in (4.96)}} I(A_i; B_f; C_f \,|\, EX_fY_fZ_f)_\zeta \leq \inf_{\text{ext. in (4.97)}} I(A; B; C \,|\, XYZE)_\tau. \tag{4.108}$$

By optimizing over arbitrary input probability distributions, we conclude that

$$\sup_q \inf_{\text{ext. in (4.96)}} I(A_f; B_f; C_f \,|\, EX_fY_fZ_f)_{p_f} \leq \sup_q \inf_{\text{ext. in (4.97)}} I(A; B; C \,|\, XYZE)_{p_i}, \tag{4.109}$$

which is the desired inequality in (4.95). ■

Theorem 25 (Monotonicity of QTINL under LOCR) *Let $p_i(a,b,c\,|\,x,y,z)$ be a quantum correlation, and let $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ result from the action of local operations and common randomness on $p_i(a,b,c\,|\,x,y,z)$, as described in (4.92). Then*

$$N_Q(A_i;B_i;C_i)_{p_i} \geq N_Q(A_i;B_f;C_f)_{p_f}. \tag{4.110}$$

Proof. First, let us embed $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ in a quantum state:

$$\zeta_{A_fB_fC_fX_fY_fZ_f} = \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f)p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)[a_fb_fc_fx_fy_fz_f]_{A_fB_fC_fX_fY_fZ_f}, \tag{4.111}$$

where $q(x_f,y_f,z_f)$ is an arbitrary probability distribution for x_f, y_f, and z_f. The set Q of quantum correlations is closed under the action of local operations and common randomness, implying that $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f) \in Q$. Since $p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)$ is also a quantum correlation, we know that there exists an underlying state $\zeta_{\hat{A}_f\hat{B}_f\hat{C}_f}$and POVMs $\{\Pi^{(x_f)}_{a_f}\}_{a_f}$, $\{\Pi^{(y_f)}_{b_f}\}_{b_f}$, and $\{\Pi^{(z_f)}_{c_f}\}_{c_f}$ such that

$$p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f) = \mathrm{Tr}\Big[\Big(\Pi^{(x_f)}_{a_f}\otimes\Pi^{(y_f)}_{b_f}\otimes\Pi^{(z_f)}_{c_f}\Big)\zeta_{\hat{A}_f\hat{B}_f\hat{C}_f}\Big]. \tag{4.112}$$

An arbitrary quantum extension of the state $\zeta_{A_fB_fC_fX_fY_fZ_f}$ is given by

$$\zeta_{A_fB_fC_fEX_fY_fZ_f} = \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f)p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f) [a_fb_fc_fx_fy_fz_f]_{A_fB_fC_fEX_fY_fZ_f}\otimes\zeta_E^{a_f,b_f,c_fx_f,y_f,z_f}, \tag{4.113}$$

where

$$\zeta_E^{a_f,b_f,c_fx_f,y_f,z_f} = \frac{1}{p_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)}\mathrm{Tr}\Big[\Big(\Pi^{(x_f)}_{a_f}\otimes\Pi^{(y_f)}_{b_f}\otimes\Pi^{(z_f)}_{c_f}\otimes\mathbb{I}\Big)\zeta_{\hat{A}_f\hat{B}_f\hat{C}_fE}\Big], \tag{4.114}$$

and $\zeta_{A_f B_f C_f E}$ is an quantum extension of $\zeta_{A_f B_f C_f}$. Now, we know that

$$p_f(a_f, b_f, c_f \,|\, x_f, y_f, z_f) = \sum_{a,b,c,x,y,z} O^{(L)}(a_f, b_f, c_f \,|\, x_f, y_f, z_f, a, b, c, x, y, z) \\ p_i(a, b, c \,|\, x, y, z) I^{(L)}(x, y, z \,|\, x_f, y_f, z_f), \quad (4.115)$$

as well as the facts that $I^{(L)}(x, y, z \,|\, x_f, y_f, z_f)$ and $O^{(L)}(a_f, b_f, c_f \,|\, x_f, y_f, z_f, a, b, c, x, y, z)$ are local correlations. Therefore, there exist separable states ζ_{XYZ} and $\rho_{\hat{A}_f \hat{B}_f \hat{C}_f}$, along with POVMs that result in the correlations $I^{(L)}$ and $O^{(L)}$. That is,

$$I^{(L)}(x, y, z \,|\, x_f, y_f, z_f) = \mathrm{Tr}\Big[\Big(\Pi_x^{(x_f)} \otimes \Pi_y^{(y_f)} \otimes \Pi_z^{(z_f)}\Big) \zeta_{XYZ}\Big], \quad (4.116)$$

and

$$O^{(L)}(a_f, b_f, c_f \,|\, x_f, y_f, z_f, a, b, c, x, y, z) = \mathrm{Tr}\Big[\Big(\Pi_{a_f}^{(x_f, a, x)} \otimes \Pi_{b_f}^{(y_f, b, y)} \otimes \Pi_{c_f}^{(z_f, c, z)}\Big) \rho_{\hat{A}_f \hat{B}_f \hat{C}_f}\Big]. \quad (4.117)$$

Furthermore, we know that the correlation $p_i(a, b, c \,|\, x, y, z)$ is a quantum correlation. Thus, there exists an underlying state $\zeta_{\hat{A}\hat{B}\hat{C}}$ and POVMs $\{\Pi_a^{(x)}\}_a$, $\{\Pi_b^{(y)}\}_b$, and $\{\Pi_c^{(z)}\}_b$ such that

$$p(a_f, b_f, c_f \,|\, x_f, y_f, z_f) = \\ \sum_{a,b,c,x,y,z} \mathrm{Tr}\Big[\Big(\Pi_{a_f}^{(x_f, a, x)} \otimes \Pi_{b_f}^{(y_f, b, y)} \otimes \Pi_{c_f}^{(z_f, c, z)} \otimes \Pi_x^{(x_f)} \otimes \Pi_y^{(y_f)} \otimes \Pi_z^{(z_f)} \otimes \Pi_a^{(x)} \otimes \Pi_b^{(y)} \otimes \Pi_c^{(z)}\Big) \\ \Big(\rho_{\hat{A}_f \hat{B}_f \hat{C}_f} \otimes \zeta_{XYZ} \otimes \zeta_{\hat{A}\hat{B}\hat{C}}\Big)\Big]. \quad (4.118)$$

Since ζ_{XYZ} is a separable state, we can write it as $\zeta_{XYZ} = \sum_{\lambda_1} p(\lambda_1) \zeta_X^{\lambda_1} \otimes \zeta_Y^{\lambda_1} \otimes \zeta_Z^{\lambda_1}$. Let $\zeta_{XYZ\Lambda_1} = \sum_{\lambda_1} p(\lambda_1) \zeta_X^{\lambda_1} \otimes \zeta_Y^{\lambda_1} \otimes \zeta_Z^{\lambda_1} \otimes [\lambda_1]_{\Lambda_1}$ be a particular quantum extension of ζ_{XYZ}.

Similarly, let $\rho_{\hat{A}_f\hat{B}_f\hat{C}_f\Lambda_2}$ be a quantum extension of $\rho_{\hat{A}_f\hat{B}_f\hat{C}_f}$ and $\zeta_{\hat{A}\hat{B}\hat{C}E}$ an extension of $\zeta_{\hat{A}\hat{B}\hat{C}}$. A particular quantum extension of the state in (4.113) is given by

$$\rho_{A_fB_fC_fEX_fY_fZ_f\Lambda_1\Lambda_2} = \sum_{a_f,b_f,c_f,x_f,y_f,z_f} p(x_f,y_f,z_f)q_f(a_f,b_f,c_f\,|\,x_f,y_f,z_f)\times$$
$$[a_fb_fc_fx_fy_fz_f]_{A_fB_fC_fX_fY_fZ_f}\otimes\rho_E^{abcxyz}\otimes[\lambda_1\lambda_2]_{\Lambda_1\Lambda_2}, \quad (4.119)$$

where

$$\rho_E^{a,b,c,x,y,z} = \frac{1}{p(a,b,c,\,|\,x,y,z)}\,\mathrm{Tr}\Big[\Big(\Pi_a^{(x)}\otimes\Pi_b^{(y)}\otimes\Pi_c^{(z)}\otimes\mathbb{I}\Big)\zeta_{\hat{A}\hat{B}\hat{C}E}\Big], \quad (4.120)$$

which then gives

$$\rho_{ABCA_fB_fC_fEXYZX_fY_fZ_f\Lambda_1\Lambda_2}$$
$$= \sum_{a_f,b_f,c_f,x_f,y_f,z_f} q(x_f,y_f,z_f)\sum_{a,b,c,x,y,z}\sum_{\lambda_2} p(\lambda_2)O_A(a_f\,|\,a,x,x_f,\lambda_2)O_B(b_f\,|\,b,y,y_f,\lambda_2)\times$$
$$O_C(c_f\,|\,c,z,z_f,\lambda_2)p_i(a,b,c\,|\,x,y,z)\sum_{\lambda_1} p(\lambda_1)I_A(x\,|\,x_f,\lambda_1)I_B(y\,|\,y_f,\lambda_1)I_B(y\,|\,y_f,\lambda_1)\times$$
$$I_C(z\,|\,z_f,\lambda_1)[abcxyza_fb_fc_fx_fy_fz_f]_{ABCA_fB_fC_fXYZX_fY_fZ_f}\otimes\rho_E^{abcxyz}\otimes[\lambda_1\lambda_2]_{\Lambda_1\Lambda_2}. \quad (4.121)$$

Then, following arguments similar to that given in Theorem 24, we obtain the desired inequality in (4.110). ■

4.6 Local Hidden-Variable Models

In this section, we show that tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality vanish for tripartite correlations that admit a local

hidden-variable model. A tripatite correlation admits a local hidden-variable model if it is of the following form [173]:

$$p(a,b,c\,|\,x,y,z) = \sum_{\Lambda} p_{\Lambda}(\lambda)p(a\,|\,x,\lambda)p(b\,|\,y,\lambda)p(c\,|\,z,\lambda), \tag{4.122}$$

where λ is a local hidden variable. If a distribution admits such a model, then the model can be reformulated so that all the factor distributions $p(a|x,\lambda)$, $p(b|y,\lambda)$, and $p(c|z,\lambda)$ are deterministic with probabilities equal to either zero or one. In this case, using the classical information λ and the input settings of x, y, and z, an eavesdropper can deduce the outcomes a, b, and c with certainty. Hence, tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality should vanish for local tripartite correlations.

Theorem 26 (TINL & QTINL for local correlations) *Tripartite intrinsic non-locality and quantum tripartite intrinsic non-locality vanish for every distribution $p(a,b,c\,|\,x,y,z)$ having a local hidden-variable model, i.e., $N(A;B;C)_p = 0$ and $N_Q(A;B;C)_p = 0$.*

Proof. Consider the following no-signaling extension of $p(a,b,c\,|\,x,y,z)$:

$$\zeta_{ABCEXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z)p(a,b,c\,|\,x,y,z)[abcxyz]_{ABCXYZ} \otimes \rho_E^{abcxyz}. \tag{4.123}$$

A particular no-signaling extension of $p(a,b,c\,|\,x,y,z)$ is

$$\begin{aligned}\rho_{ABCEXYZ} &= \sum_{a,b,c,x,y,z,\Lambda} p_{\Lambda}(\lambda)q(x,y,z)p(a\,|\,x,\lambda)p(b\,|\,y,\lambda)p(c\,|\,z,\lambda)[abcxyz]_{ABCXYZ} \otimes [\lambda]_E \\ &= \sum_{\Lambda} p_{\Lambda}(\lambda)\rho^{\lambda}_{ABCXYZ} \otimes [\lambda]_E \end{aligned} \tag{4.124}$$

where,

$$\rho^{\lambda}_{ABCXYZ} = \sum_{a,b,c,x,y,z} q(x,y,z)p(a\,|\,x,\lambda)p(b\,|\,y,\lambda)p(c\,|\,z,\lambda)[abcxyz]_{ABCXYZ}. \tag{4.125}$$

Then, it follows that

$$\inf_{\text{ext. in (4.123)}} I(A;B;C\,|\,EXYZ)_{\zeta} \leq I(A;B;C\,|\,EXYZ)_{\rho} = \sum_{\Lambda} p_{\Lambda}(\lambda) I(A;B;C\,|\,XYZ)_{\rho_{\lambda}} \tag{4.126}$$

From inspection of (4.125), we conclude that $I(A;B;C\,|\,XYZ)_{\rho_{\lambda}} = 0$. Therefore, we obtain the first desired claim: $N(A;B;C)_p = 0$. One can see that $N_Q(A;B;C)_p = 0$ by considering the appropriate quantum extensions. ■

4.7 Multipartite Intrinsic Non-Locality

We now generalize the tripartite case to the multipartite case. Henceforth, we denote the ith input to the measurement device by x_i, and we denote the outcome of a measurement by a_i, where $i \in \{1,\ldots,M\}$ and M is the number of parties involved. Now, we can define multipartite intrinsic non-locality, using conditional total correlation, for a no-signaling correlation as follows:

Definition 17 *Let $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ be a no-signaling correlation. Multipartite intrinsic non-locality of p is defined as*

$$N(A_1;\cdots;A_M)_p \coloneqq \frac{1}{M-1} \sup_{q(x_1,\ldots,x_M)} \inf_{\rho_{A_1\cdots A_M X_1\cdots X_M E}} I(A_1;\cdots;A_M\,|\,EX_1\cdots X_M)_{\rho}, \tag{4.127}$$

where $q(x_1, \ldots, x_M)$ is a probability distribution for the inputs of the Alices, and the state $\rho_{A_1 \cdots A_M X_1 \cdots X_M E}$ is a no-signaling extension of the state shared by the Alices, given by

$$\rho_{A_1 \cdots A_M X_1 \cdots X_M E} = \sum_{a_1,\ldots,a_M,x_1,\ldots,x_M} q(x_1, \ldots, x_M) p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M) \\ [a_1, \ldots, a_M, x_1, \ldots, x_M]_{A_1 \cdots A_M X_1 \cdots X_M} \otimes \rho_E^{a_1,\ldots,a_M,x_1,\ldots,x_M}. \quad (4.128)$$

We define quantum multipartite quantum intrinsic non-locality, based on conditional total correlation, for a quantum correlation as follows:

Definition 18 *Multipartite quantum intrinsic non-locality of $p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M)$, a quantum correlation, is defined as*

$$N_Q(A_1; \cdots; A_M)_p := \frac{1}{M-1} \sup_{q(x_1,\ldots,x_M)} \inf_{\rho_{A_1 \cdots A_M X_1 \cdots X_M E}} I(A_1; \cdots; A_M \,|\, E X_1 \cdots X_M)_\rho, \quad (4.129)$$

where $q(x_1, \ldots, x_M)$ is a probability distribution for generating the inputs used by the Alices and $\rho_{A_1 \cdots A_M X_1 \cdots X_M E}$ is a quantum extension of the state shared by the Alices, given by

$$\rho_{A_1 \cdots A_M X_1 \cdots X_M E} = \sum_{a_1,\ldots,a_M,x_1,\ldots,x_M} q(x_1, \ldots, x_M) p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M) \\ [a_1, \ldots, a_M, x_1, \ldots, x_M]_{A_1 \cdots A_M X_1 \cdots X_M} \otimes \rho_E^{a_1,\ldots,a_M,x_1,\ldots,x_M}. \quad (4.130)$$

We now derive a chain rule for the quantity $I(A_{1,1}A_{1,2}; \cdots; A_{i,1}A_{i,2}; \cdots; A_{M,1}A_{M,2} \,|\, E)$ similar to that in Theorem 19. In doing so, we generalize (4.27) to every finite M such that we can prove additivity and other relevant properties of multipartite (quantum) intrinsic non-locality. Let us define $[M] := \{1, 2, \ldots, m\}$ and $A_{\{i,\ldots,M\},j} \equiv A_{i,j} \cdots A_{M,j}$.

Theorem 27 *For every multipartite state $\rho_{A_{1,1}A_{1,2}\cdots A_{i,1}A_{i,2}\cdots A_{M,1}A_{M,2}E}$, the following equality holds:*

$$I(A_{1,1}A_{1,2};\cdots;A_{i,1}A_{i,2};\cdots;A_{M,1}A_{M,2}\,|\,E) =$$
$$I(A_{1,2};\cdots;A_{M,2}\,|\,E) + I(A_{1,1};\cdots;A_{M,1}\,|\,EA_{[M],2}) + \sum_{i=1}^{M} I(A_{i,1};A_{[M]\setminus\{i\},2}\,|\,EA_{i,2}). \quad (4.131)$$

Proof. By applying definitions and the chain rule for conditional entropy, we find that

$$\begin{aligned}
&I(A_{1,1}A_{1,2};A_{2,1}A_{2,2};\cdots;A_{M,1}A_{M,2}\,|\,E)\\
&= \sum_{i=1}^{M} H(A_{i,1}A_{i,2}\,|\,E) - H(A_{1,1}A_{1,2}A_{2,1}A_{2,2}\cdots A_{M,1}A_{M,2}\,|\,E) && (4.132)\\
&= \sum_{i=1}^{M} \left[H(A_{i,2}\,|\,E) + H(A_{i,1}\,|\,EA_{i,2})\right]\\
&\qquad - \left[H(A_{1,2}A_{2,2}\cdots A_{M,2}\,|\,E) - H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{1,2}A_{2,2}\cdots A_{M,2})\right] && (4.133)\\
&= I(A_{1,2};A_{2,2};\cdots;A_{M,2}\,|\,E) + \sum_{i=1}^{M} H(A_{i,1}\,|\,EA_{i,2}) - H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2}). && (4.134)
\end{aligned}$$

Continuing, we find that

$$\begin{aligned}
&\sum_{i=1}^{M} H(A_{i,1}\,|\,EA_{i,2}) - H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2})\\
&= \sum_{i=1}^{M} \left[H(A_{i,1}\,|\,EA_{i,2}) - H(A_{i,1}\,|\,EA_{[M],2}) + H(A_{i,1}\,|\,EA_{[M],2})\right]\\
&\qquad - H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2}) && (4.135)\\
&= \sum_{i=1}^{M} I(A_{i,1};A_{[M]\setminus\{i\},2}\,|\,EA_{i,2}) + I(A_{1,1};A_{2,1};\cdots;A_{M,1}\,|\,EA_{[M],2}). && (4.136)
\end{aligned}$$

This concludes the proof. ■

Now, let us note that if we consider the particular case when $M = 3$, we recover the exact form obtained earlier in (4.27). Then, we can extend the arguments presented for the tripartite case to obtain additivity, convexity, and monotonicity under LOCR for multipartite intrinsic non-locality and multipartite quantum intrinsic non-locality, primarily due to the structure of (4.131) producing similar terms for every finite M.

4.8 Dual Multipartite Intrinsic Non-Locality

Until now, we have defined multipartite intrinsic non-locality based on conditional total correlation. As noted earlier, total correlation is just one possible generalization of mutual information that has found uses in quantum information. Dual total correlation is another M-partite generalization of mutual information, first introduced in [180, 181]. Both total correlation and dual total correlation reduce to mutual information in the bipartite scenario. Since a distinction between total correlation and dual total correlation would only arise in the multipartite scenario, it is worthwhile to discuss the multipartite intrinsic non-locality based on conditional dual total correlation to note the differences in quantities that arise and compare the two quantities.

In this section, we discuss multipartite intrinsic non-locality based on dual to-

tal correlation. Conditional dual total correlation is the conditional version of dual total correlation, and it has been previously used in various multipartite scenarios in quantum information [169, 182]. Conditional dual total correlation of a state $\rho_{A_1\cdots A_M E}$ is defined as

$$\widetilde{I}(A_1;\cdots;A_M\,|\,E) \coloneqq \sum_{i=1}^{m} H(A_{[M]\setminus\{i\}}\,|\,E) - (m-1)H(A_1\cdots A_M\,|\,E). \tag{4.137}$$

The chain rule for conditional dual total correlation is as follows:

$$\widetilde{I}(BA_1;A_2;\cdots;A_M\,|\,E) = \widetilde{I}(A_1;A_2;\cdots;A_M\,|\,BE) + I(B;A_2\cdots A_M\,|\,E). \tag{4.138}$$

We now define the multipartite intrinsic non-locality based on conditional dual total correlation, and we refer to it as dual multipartite intrinsic non-locality:

Definition 19 *Dual multipartite intrinsic non-locality of a no-signaling correlation $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ is defined as*

$$\widetilde{N}(A_1;\cdots;A_M)_p \coloneqq \sup_{q(x_1,\ldots,x_M)} \inf_{\rho_{A_1\cdots A_M X_1\cdots X_M E}} \widetilde{I}(A_1;\cdots;A_M\,|\,EX_1\cdots X_M)_\rho, \tag{4.139}$$

where $q(x_1,\ldots,x_M)$ is a probability distribution for the inputs of the Alices, and the state $\rho_{A_1\cdots A_M X_1\cdots X_M E}$ is a no-signaling extension of the state shared by the Alices, given by

$$\rho_{A_1\cdots A_M X_1\cdots X_M} = \sum_{a_1,\ldots,a_M,x_1,\ldots,x_M} q(x_1,\ldots,x_M)p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M) \\ [a_1,\ldots,a_M,x_1,\ldots,x_M]_{A_1\cdots A_M X_1\cdots X_M} \otimes \rho_E^{a_1,\ldots,a_M,x_1,\ldots,x_M}. \tag{4.140}$$

We define dual multipartite quantum intrinsic non-locality for a quantum correlation as follows:

Definition 20 *Dual multipartite quantum intrinsic non-locality of $p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M)$, a quantum correlation, is defined as*

$$\widetilde{N}_Q(A_1; \cdots; A_M)_p \coloneqq \sup_{q(x_1,\ldots,x_M)} \inf_{\rho_{A_1 \cdots A_M X_1 \cdots X_M E}} \widetilde{I}(A_1; \cdots; A_M \,|\, E X_1 \cdots X_M)_\rho, \tag{4.141}$$

where $q(x_1, \ldots, x_M)$ is a probability distribution that generates the inputs used by the Alices and $\rho_{A_1 \cdots A_M X_1 \cdots X_M E}$ is a quantum extension of the state shared by the Alices, given by

$$\rho_{A_1 \cdots A_M X_1 \cdots X_M} = \sum_{a_1,\ldots,a_M,x_1,\ldots,x_M} q(x_1, \ldots, x_M) p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M) \\ [a_1, \ldots, a_M, x_1, \ldots, x_M]_{A_1 \cdots A_M X_1 \cdots X_M} \otimes \rho_E^{a_1,\ldots,a_M,x_1,\ldots,x_M}. \tag{4.142}$$

We now derive a chain rule for the quantity $\widetilde{I}(A_{1,1}A_{1,2}; \cdots; A_{i,1}A_{i,2}; \cdots; A_{M,1}A_{M,2} \,|\, E)$ similar to that in Theorem 19. In doing so, we generalize (4.131) to conditional dual total correlation and every finite M, such that we can prove additivity and other relevant properties of dual multipartite (quantum) intrinsic non-locality.

Theorem 28 *For every multipartite state $\rho_{A_{1,1}A_{1,2} \cdots A_{i,1}A_{i,2} \cdots A_{M,1}A_{M,2}E}$, the following equality holds:*

$$\widetilde{I}(A_{1,1}A_{1,2}; \cdots; A_{i,1}A_{i,2}; \cdots; A_{M,1}A_{M,2} \,|\, E) = \widetilde{I}(A_{1,2}; \cdots; A_{M,2} \,|\, E) \\ + \widetilde{I}(A_{1,1}; \cdots; A_{M,1} \,|\, E A_{[M],2}) + \sum_{i=1}^{M} I(A_{[M]\setminus\{i\},1}; A_{i,2} \,|\, E A_{[M]\setminus\{i\},2}). \tag{4.143}$$

Proof. By applying definitions and the chain rule for conditional entropy, we find that

$$\widetilde{I}(A_{1,1}A_{1,2}; A_{2,1}A_{2,2}; \cdots; A_{M,1}A_{M,2} \,|\, E)$$

$$= \sum_{i=1}^{M} H(A_{[M]\setminus\{i\},1}A_{[M]\setminus\{i\},2}\,|\,E) - (m-1)H(A_{1,1}A_{1,2}A_{2,1}A_{2,2}\cdots A_{M,1}A_{M,2}\,|\,E) \tag{4.144}$$

$$= \sum_{i=1}^{M} \left[H(A_{[M]\setminus\{i\},2}\,|\,E) + H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M]\setminus\{i\},2})\right]$$

$$- (m-1)\left[H(A_{1,2}A_{2,2}\cdots A_{M,2}\,|\,E) - H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{1,2}A_{2,2}\cdots A_{M,2})\right] \tag{4.145}$$

$$= \widetilde{I}(A_{1,2};A_{2,2};\cdots;A_{M,2}\,|\,E)$$

$$+ \sum_{i=1}^{M} H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M]\setminus\{i\},2}) - (m-1)H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2}). \tag{4.146}$$

Continuing, we find that

$$\sum_{i=1}^{M} H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M]\setminus\{i\},2}) - (m-1)H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2})$$

$$= \sum_{i=1}^{M} \left[H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M]\setminus\{i\},2}) - H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M],2}) + H(A_{[M]\setminus\{i\},1}\,|\,EA_{[M],2})\right]$$

$$- (m-1)H(A_{1,1}A_{2,1}\cdots A_{M,1}\,|\,EA_{[M],2}) \tag{4.147}$$

$$= \sum_{i=1}^{M} I(A_{[M]\setminus\{i\},1};A_{i,2}\,|\,EA_{[M]\setminus\{i\},2}) + \widetilde{I}(A_{1,1};A_{2,1};\cdots;A_{M,1}\,|\,EA_{[M],2}). \tag{4.148}$$

This concludes the proof. ■

For the particular case of $M = 3$, the expression in (4.143) reduces to

$$\widetilde{I}(A_1A_2;B_1B_2;C_1C_2\,|\,E) = \widetilde{I}(A_2;B_2;C_2\,|\,E) + \widetilde{I}(A_1;B_1;C_1\,|\,EA_2B_2C_2)$$

$$+ I(B_1C_1;A_2\,|\,EB_2C_2) + I(A_1C_1;B_2\,|\,EA_2C_2) + I(B_1A_1;C_2\,|\,EB_2A_2). \tag{4.149}$$

One can use the above equation to establish additivity of dual multipartite intrinsic non-locality for the tripartite case. Then, we can extend the arguments presented for the multipartite intrinsic non-locality to obtain additivity, convexity, and monotonicity under LOCR for dual multipartite intrinsic non-locality and

dual multipartite quantum intrinsic non-locality, primarily due to the structure of (4.143) producing similar terms for every finite M.

4.9 Device-Independent Conference Key Agreement Capacity

In this section, we define a general form of a tripartite device-independent conference key agreement protocol and its associated capacity. We shall then upper bound this capacity using tripartite intrinsic non-locality. Here, we show details of the definition for the case in which the eavesdropper possesses a no-signaling extension of the underlying correlation, and then we remark how the definition can be modified to the case in which the eavesdropper is restricted by quantum mechanics.

Let $n \in \mathbb{Z}^+$, $R \geq 0$, and $\varepsilon \in [0,1]$. Let $p(a,b,c\,|\,x,y,z)$ be the correlation of the device shared by Alice, Bob, and Charlie. We define an (n,R,ε) device-independent conference-key-agreement protocol as follows:

- Alice, Bob, and Charlie generate the input sequences x^n, y^n, and z^n to their devices according to the probability distribution $q_{X^nY^nZ^n}(x^n,y^n,z^n)$. The device is used n times, and the distribution $q_{X^nY^nZ^n}(x^n,y^n,z^n)$ is independent of the eavesdropper. For round $j \in \{1,\ldots,n\}$, Alice inputs x_j and obtains the output a_j; Bob inputs y_j and obtains the output b_j; Charlie inputs z_j and obtains the output c_j. The distribution for the inputs and outputs can be embedded in

the state $\sigma_{A^nB^nC^nX^nY^nZ^n}$, defined as

$$\sigma_{A^nB^nC^nX^nY^nZ^n} = \sum_{a^n,b^n,c^n,x^n,y^n,z^n} q_{X^nY^nZ^n}(x^n,y^n,z^n) p^n(a^n,b^n,c^n \mid x^n,y^n,z^n) \times |a^nb^nc^nx^ny^nz^n\rangle\langle a^nb^nc^nx^ny^nz^n|_{A^nB^nC^nX^nY^nZ^n}, \quad (4.150)$$

where $p^n(a^n,b^n,c^n \mid x^n,y^n,z^n)$ is the n-fold independent and identically distributed extension of $p(a,b,c \mid x,y,z)$. The joint state held by Alice, Bob, Charlie, and Eve is an arbitrary no-signaling extension $\sigma_{A^nB^nC^nX^nY^nZ^nE}$ of $\sigma_{A^nB^nC^nX^nY^nZ^n}$, as defined in (4.11).

- Alice performs a local channel $\mathcal{L}^A_{A^n\to M_AC_A}$, with C_A denoting a classical register that is publicly communicated from Alice to Bob and Charlie, and M_A denotes a classical local memory register that is not used for public communication. The register $\bar{C}_A$ is a classical register held by Eve, which is a copy of C_A. Similarly, Bob performs a local channel $\mathcal{L}^B_{B^n\to M_BC_B}$, with C_B denoting the classical register that is publicly communicated from Bob to Alice and Charlie, and M_B denotes a classical local memory register that is not used for public communication. The register $\bar{C}_B$ is a classical register held by Eve, which is a copy of C_B. Charlie performs a local channel $\mathcal{L}^C_{C^n\to M_CC_C}$, with C_C denoting the classical register that is publicly communicated from Charlie to Bob and Alice, and M_C denotes a classical local memory register, which is not used for public communication. The register $\bar{C}_C$ is a classical register held by Eve, which is a copy of C_C. The registers C_A, C_B, and C_C (public communication) are used for parameter estimation. If the parameters are found to be outside of a predetermined range, the protocol is aborted and no secret

key is agreed upon.

- Alice then performs the decoding channel $\mathcal{D}^A_{M_A C_A C_B C_C \to L_A}$ to obtain her final key system L_A. Bob performs the decoding channel $\mathcal{D}^B_{M_B C_A C_B C_C \to L_B}$ to obtain his final key system L_B. Charlie performs the decoding channel $\mathcal{D}^C_{M_C C_A C_B C_C \to L_C}$ to obtain his final key system L_C. This protocol yields a state $\omega_{L_A L_B L_C E X^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C}$ that satisfies

$$\frac{1}{2} \left\| \Phi_{L_A L_B L_C E X^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C} - \omega_{L_A L_B L_C E X^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C} \right\|_1 \leq \varepsilon, \tag{4.151}$$

where

$$\Phi_{L_A L_B L_C E X^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C} = 2^{-nR} \sum_{l=1}^{2^{nR}} |l\rangle\langle l|_{L_A} \otimes |l\rangle\langle l|_{L_B} \otimes |l\rangle\langle l|_{L_C} \otimes \omega_{E X^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C}. \tag{4.152}$$

A general protocol of the above form is depicted in Figure 4.1. A rate R is achievable for a device characterized by a correlation p if there exists an $(n, R-\delta, \varepsilon)$ device-independent conference key agreement protocol for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n. The maximum achievable rate is denoted by $\mathrm{DI}(p)$ and is called the DI conference key agreement capacity.

These definitions can easily be modified to the case in which the eavesdropper is restricted by quantum mechanics. The main modification is that the underlying correlation is a quantum correlation, and the eavesdropper is allowed to possess a quantum extension of it. We denote the resulting capacity by $\mathrm{DI}_Q(p)$.

It is straightforward to generalize everything stated above to the case of a multipartite correlation $p(a_1, \ldots, a_M \,|\, x_1, \ldots, x_M)$.

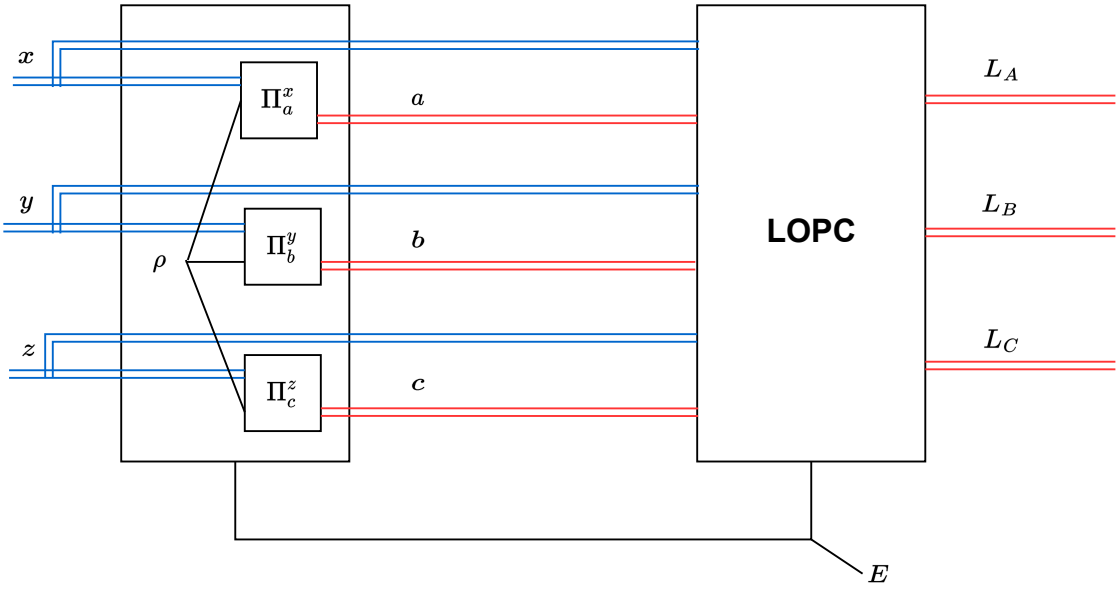


Figure 4.1: General schematic for device-independent conference key agreement. The POVMs $\{\Pi_a^{(x)}\}_a$, $\{\Pi_b^{(y)}\}_b$, and $\{\Pi_c^{(z)}\}_c$ are available to Alice, Bob, and Charlie, respectively. The eavesdropper is in possession of the quantum and classical information in system E. LOPC stands for local operations and public communication and is used by Alice, Bob, and Charlie to distill the final conference key.

In [3], a lower bound on conference key agreement rate was established for a particular protocol. In this chapter, we are trying to address a different question that can be answered regardless of any particular choice of protocol. We are concerned with the no-signaling or quantum correlations that characterize the devices used for device-independent conference key agreement. The question we want to answer is as follows: *given a correlation $p(a,b,c\,|\,x,y,z)$, produced by a device, what is a non-trivial upper bound on the conference key agreement rate that can be extracted from*

this device with any possible protocol?

We answer this question for independent and identically distributed (i.i.d.) devices, which means, in each round of the protocol, the device is characterized by the correlation $p(a, b, c \mid x, y, z)$. The inputs within each round of the protocol can be correlated, but not across rounds. This i.i.d. assumption is not a drawback as we are interested in calculating *upper* bounds on conference key agreement rates: if we show that a correlation can certify no more than a certain limit of key rate against an eavesdropper restricted to i.i.d. attacks, then the correlation certainly cannot certify more than this limit against an eavesdropper without such a restriction.

4.9.1 Upper Bound on DI Conference Key Agreement Capacity

Now, we prove that tripartite intrinsic non-locality is indeed an upper bound on the DI conference key agreement capacity.

Theorem 29 *The tripartite intrinsic non-locality $N(A; B; C)_p$ is an upper bound on the device-independent conference key agreement capacity of a device characterized by the no-signaling correlation $p(a, b, c \mid x, y, z)$ and sharing no-signaling correlations with an eavesdropper:*

$$\mathrm{DI}(p) \leq N(A; B; C)_p. \tag{4.153}$$

Proof. The states Φ, ω, and σ are given in the definition of device-independent conference key agreement in Section 4.9. Using (4.151) and (4.18), we find that

$$2nR = I(L_A; L_B; L_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\Phi \tag{4.154}$$

$$\leq I(L_A; L_B; L_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon}. \tag{4.155}$$

where $\tilde{\varepsilon} = 4\varepsilon nR + 3g(\varepsilon)$ and $g(\varepsilon)$ is defined in (4.19). Using data processing of conditional total correlation for L_A, L_B, and L_C under the local channels $\mathcal{D}^A_{M_A C_A C_B C_C \to L_A}$, $\mathcal{D}^B_{M_B C_A C_B C_C \to L_A}$, and $\mathcal{D}^C_{M_C C_A C_B C_C \to L_A}$, we conclude that

$$2nR \leq I(L_A; L_B; L_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon} \tag{4.156}$$

$$\leq I(M_A C_A C_B C_C; M_B C_A C_B C_C; M_C C_A C_B C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon}. \tag{4.157}$$

Now, since $\bar{C}_B$ is a copy of C_B and $\bar{C}_C$ is a copy of C_C, we conclude that

$$H(M_A C_A C_B C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C) = H(M_A C_A \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C). \tag{4.158}$$

A similar manipulation can be applied to $H(M_B C_A C_B C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)$ and $H(M_C C_A C_B C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)$, giving us

$$\begin{aligned} 2nR &\leq I(M_A C_A C_B C_C; M_B C_A C_B C_C; M_C C_A C_B C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon} \\ &\leq I(M_A C_A; M_B C_B; M_C C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon}. \end{aligned} \tag{4.159}$$

Using (4.16) and ignoring the negative terms that arise, we find that

$$\begin{aligned} 2nR &\leq I(M_A C_A; M_B C_B; M_C C_C \,|\, EX^n Y^n Z^n \bar{C}_A \bar{C}_B \bar{C}_C)_\omega + \tilde{\varepsilon} \\ &\leq I(M_A C_A \bar{C}_A; M_B C_B \bar{C}_B; M_C C_C \bar{C}_C \,|\, EX^n Y^n Z^n)_\omega + \tilde{\varepsilon} \\ &= I(M_A C_A; M_B C_B; M_C C_C \,|\, EX^n Y^n Z^n)_\omega + \tilde{\varepsilon}. \end{aligned} \tag{4.160}$$

Using data processing of conditional total correlation on $M_A C_A$, $M_B C_B$, and $M_C C_C$,

$$\begin{aligned} 2nR &\leq I(M_A C_A; M_B C_B; M_C C_C \,|\, EX^n Y^n Z^n)_\omega + \tilde{\varepsilon} \\ &\leq I(A^n; B^n; C^n \,|\, EX^n Y^n Z^n)_\sigma + \tilde{\varepsilon}. \end{aligned} \tag{4.161}$$

Using the fact that the no-signaling extension applied in the protocol in Section 4.9 is arbitrary,

$$2nR \leq \inf_{\text{ext.}} I(A^n; B^n; C^n \,|\, EX^n Y^n Z^n)_\sigma + \tilde{\varepsilon} \tag{4.162}$$

Using $\tilde{\varepsilon} = 4\varepsilon nR + 3g(\varepsilon)$,

$$2(1 - 2\varepsilon)nR \leq \inf_{\text{ext.}} I(A^n; B^n; C^n \,|\, EX^n Y^n Z^n)_\sigma + 3g(\varepsilon). \tag{4.163}$$

Taking the supremum over all input distributions,

$$2(1 - 2\varepsilon)nR \leq \sup_q \inf_{\text{ext.}} I(A^n; B^n; C^n \,|\, EX^n Y^n Z^n)_\sigma + 3g(\varepsilon). \tag{4.164}$$

Using additivity (see Theorem 20),

$$2(1 - 2\varepsilon)nR \leq \sup_q \inf_{\text{ext.}} I(A^n; B^n; C^n \,|\, EX^n Y^n Z^n)_\rho + 3g(\varepsilon) \tag{4.165}$$

$$= n \cdot \sup_q \inf_{\text{ext.}} I(A; B; C \,|\, EXYZ)_\rho + 3g(\varepsilon) \tag{4.166}$$

$$\implies 2(1 - 2\varepsilon)R \leq \sup_q \inf_{\text{ext.}} I(A; B; C \,|\, EXYZ)_\rho + \frac{3}{n} g(\varepsilon). \tag{4.167}$$

Taking the limit $n \to \infty$ and then $\varepsilon \to 0$, we conclude that

$$\text{DI}(p) \leq N(A; B; C). \tag{4.168}$$

This concludes the proof. ■

Using similar techniques and taking appropriate quantum extensions establishes the following:

Theorem 30 *The quantum tripartite intrinsic non-locality $N_Q(A;B;C)_p$ is an upper bound on the device-independent conference key agreement capacity of a device characterized by the quantum correlation $p(a,b,c\,|\,x,y,z)$ and sharing quantum correlations with an eavesdropper:*

$$\mathrm{DI}_Q(p) \leq N_Q(A;B;C)_p. \tag{4.169}$$

All the steps (i.e., data processing and additivity) in the proof of Theorem 29 can be easily extended to apply to multipartite intrinsic non-locality, dual multipartite intrinsic non-locality, and their respective quantum counterparts. This leads to the following theorems:

Theorem 31 *The multipartite intrinsic non-locality $N(A_1;\cdots;A_M)_p$ is an upper bound on the device-independent conference key agreement capacity of a device characterized by a no-signaling correlation $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ and sharing no-signaling correlations with an eavesdropper:*

$$\mathrm{DI}(p) \leq N(A_1;\cdots;A_M)_p. \tag{4.170}$$

Theorem 32 *The multipartite quantum intrinsic non-locality $N_Q(A_1;\cdots;A_M)_p$ is an upper bound on the device-independent conference key agreement capacity of a device characterized by a quantum correlation $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ and sharing quantum correlations with an eavesdropper:*

$$\mathrm{DI}_Q(p) \leq N_Q(A_1;\cdots;A_M)_p. \tag{4.171}$$

Theorem 33 *Dual multipartite intrinsic non-locality* $\widetilde{N}(A_1;\cdots;A_M)_p$ *is an upper bound on the device-independent conference key agreement capacity of a device characterized by a no-signaling correlation* $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ *and sharing no-signaling correlations with an eavesdropper:*

$$\mathrm{DI}(p) \leq \widetilde{N}(A_1;\cdots;A_M)_p. \tag{4.172}$$

Theorem 34 *Dual multipartite quantum intrinsic non-locality* $\widetilde{N}_Q(A_1;\cdots;A_M)_p$ *is an upper bound on the device-independent conference key agreement capacity of a device characterized by a quantum correlation* $p(a_1,\ldots,a_M\,|\,x_1,\ldots,x_M)$ *and sharing quantum correlations with an eavesdropper:*

$$\mathrm{DI}_Q(p) \leq \widetilde{N}_Q(A_1;\cdots;A_M)_p. \tag{4.173}$$

4.10 Evaluating Quantum Tripartite Intrinsic Non-Locality

In this section, we evaluate quantum tripartite intrinsic non-locality for various examples. While evaluating the quantum tripartite intrinsic non-locality, we should consider the actions of an eavesdropper, who is in possession of an extension of the underlying quantum state shared by Alice, Bob, and Charlie. We note here that all source files needed to generate the plots in this section are available with the arXiv posting of [142].

An eavesdropper, Eve, of a DIQKD protocol is allowed access to a quantum extension system of the state shared between Alice and Bob prior to public com-

munication of measurement settings. Eve is also assumed to be in possession of copies of all classical communication exchanged by Alice and Bob, as well as all local hidden variables that can be attributed to the correlations that Alice and Bob share. We also assume that the state and black boxes received by Alice and Bob are in fact supplied by Eve herself.

For DI conference key agreement protocols, we assume that Eve has access to all the same quantum and classical information as in DIQKD but sourced from all the participants of the DI conference key agreement protocol. Eve can then use this collected information to reduce the key agreement rate. Any procedure employed by Eve to reduce the key agreement rate is known as an attack.

The first attack that we consider is a modification of the attack for DIQKD used in [163], which was helpful for calculating an upper bound on quantum intrinsic non-locality. We use the RMW18 Protocol [3] for all further calculations. First, suppose that the underlying state is as follows:

$$\rho_{\hat{A}\hat{B}\hat{C}} = (1-p)\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_{\hat{A}\hat{B}\hat{C}} + p\frac{\mathbb{I}_{\hat{A}\hat{B}\hat{C}}}{8}, \tag{4.174}$$

where $|\mathrm{GHZ}\rangle := (|000\rangle + |111\rangle)/\sqrt{2}$. Alice's measurement choice $x = 0$ corresponds to σ_Z, and $x = 1$ corresponds to σ_X. Bob's measurement choice $y = 0$ corresponds to $(\sigma_Z - \sigma_X)/\sqrt{2}$, the choice $y = 1$ corresponds to $(\sigma_Z + \sigma_X)/\sqrt{2}$, and the choice $y = 2$ corresponds to σ_Z. Charlie's measurement choices are σ_Z when $z = 0$ and σ_X when $z = 1$. This leads to a quantum correlation $q(a, b, c|x, y, z)$.

Using the Bell inequality corresponding to the parity-CHSH game [3, 50], the

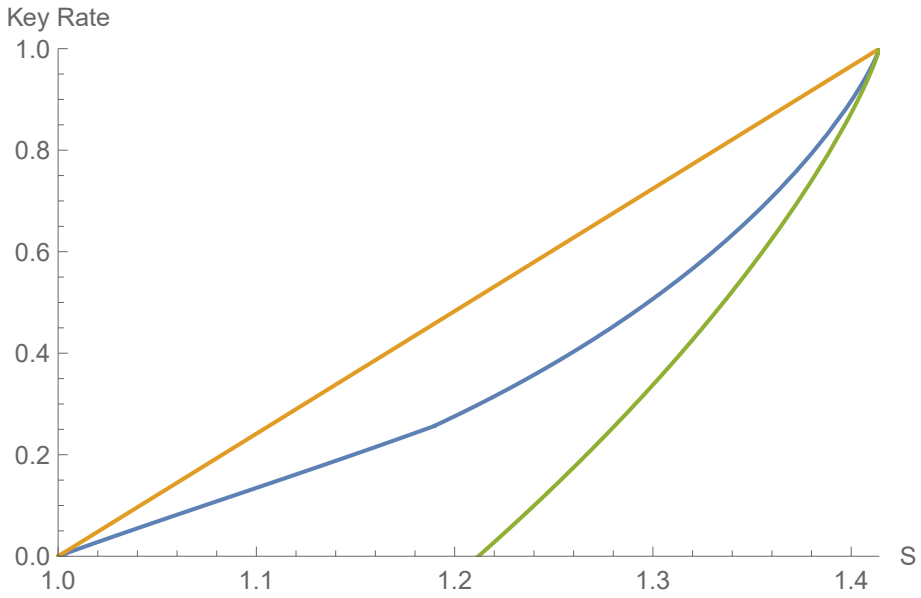


Figure 4.2: Key rate versus parity-CHSH violation S. The orange line is an upper bound on quantum tripartite intrinsic non-locality computed for the attack described in (4.179), the blue line is an upper bound on quantum tripartite intrinsic non-locality for the correlation parameterized by S using a multipartite generalization of the attack in [1, 2], and the green solid line is the lower bound for the state in (4.174) calculated from [3].

parity-CHSH violation S is as follows:[1]

$$S = \sqrt{2}(1-p). \tag{4.175}$$

We see that $\rho_{\hat{A}\hat{B}\hat{C}}$ produces a local correlation when the parity-CHSH violation is less than or equal to one or, equivalently, when $p \geq 1 - 1/\sqrt{2}$. Let $q_{S^p}(a,b,c\,|\,x,y,z)$ denote a quantum correlation with parity-CHSH violation S^p. For $\varepsilon \leq p \leq 1 - \frac{1}{\sqrt{2}}$, we can think of the correlation $q_{S^p}(a,b,c\,|\,x,y,z)$ as a convex combination of

[1]The calculations for all S, p_{win}, and plots are in the Mathematica files included with the arXiv posting of [142].

$q_{S^\varepsilon}(a,b,c\,|\,x,y,z)$, which is non-local, and $q_{S^{1-\frac{1}{\sqrt{2}}}}(a,b,c\,|\,x,y,z)$, which is local, in the following fashion:

$$q_{S^p}(a,b,c\,|\,x,y,z) = (1-\alpha(\varepsilon))q_{S^\varepsilon}(a,b,c\,|\,x,y,z) + \alpha(\varepsilon)q_{S^{1-\frac{1}{\sqrt{2}}}}(a,b,c\,|\,x,y,z), \tag{4.176}$$

where

$$\alpha(\varepsilon) = \frac{p-\varepsilon}{1-\frac{1}{\sqrt{2}}-\varepsilon}. \tag{4.177}$$

For local correlations, quantum tripartite intrinsic non-locality is equal to zero. Hence, using Theorem 23, we conclude that

$$N_Q(A;B;C)_{q_{S^p}} \leq (1-\alpha(\varepsilon))N_Q(A;B;C)_{q_{S^\varepsilon}}. \tag{4.178}$$

By considering the trivial extension for $q_{S^p}(a,b,c\,|\,x,y,z)$, we obtain

$$N_Q(A;B;C)_{q_{S^p}} \leq \min_{0\leq\varepsilon\leq p} \sup_{q(x,y,z)} (1-\alpha(\varepsilon))I(A;B;C)_{q_{S^\varepsilon}}. \tag{4.179}$$

The lower bound is calculated using the probability of winning the parity-CHSH game, given by

$$p_{\text{win}} = \frac{1}{2} + \frac{(1-p)}{2\sqrt{2}}. \tag{4.180}$$

We then plot this quantity against the parity-CHSH violation S in Figure 4.2.

The second attack on the RMW18 Protocol [3] that we consider is a multipartite generalization of the attack on DIQKD first proposed in [1], in the context of a lower bound. It has also been used in [2] for evaluating an upper bound on

DIQKD. It can be thought of as a particular way of achieving a desired parity-CHSH violation S and quantum bit error rate (QBER) Q. In the multipartite generalization, we consider the following state:

$$\frac{1-C}{2}(Z_{\hat{A}}\otimes Z_{\hat{B}}\otimes Z_{\hat{C}})(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_{\hat{A}\hat{B}\hat{C}})(Z_{\hat{A}}\otimes Z_{\hat{B}}\otimes Z_{\hat{C}})+\frac{1+C}{2}|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_{\hat{A}\hat{B}\hat{C}}, \quad (4.181)$$

which results from the action of collective dephasing on the GHZ state, and which is purified by the following state vector:

$$\sqrt{\frac{1-C}{2}}\left(\frac{|000\rangle-|111\rangle}{\sqrt{2}}\right)_{\hat{A}\hat{B}\hat{C}}\otimes|0\rangle_E+\sqrt{\frac{1+C}{2}}\left(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\right)_{\hat{A}\hat{B}\hat{C}}\otimes|1\rangle_E\,. \quad (4.182)$$

Alice's measurement choice $x=0$ corresponds to σ_Z, and $x=1$ corresponds to σ_X. Bob's measurement choice $y=0$ corresponds to $(\sigma_Z+C\sigma_X)/\sqrt{1+C^2}$, the choice $y=1$ corresponds to $(\sigma_Z-C\sigma_X)/\sqrt{1+C^2}$, and $y=2$ corresponds to σ_Z. Charlie's measurement choices are σ_Z when $z=0$ and σ_Z when $z=1$. The parity-CHSH violation S is given by $S=\sqrt{1+C^2}$. To generate key, Alice and Charlie measure σ_Z and Bob, with probability $1-2Q$, measures σ_Z and, with probability $2Q$, assigns a random bit. This gives us a QBER of Q. The post-measurement state is as follows:

$$\frac{1-Q}{2}\left(|000\rangle\langle 000|\otimes\rho_E^{+}+|111\rangle\langle 111|\otimes\rho_E^{-}\right)+\frac{Q}{2}\left(|001\rangle\langle 001|\otimes\rho_E^{+}+|110\rangle\langle 110|\otimes\rho_E^{-}\right), \quad (4.183)$$

where

$$\rho_E^{\pm}=\frac{1}{2}\begin{pmatrix}1+C & \pm\sqrt{1-C^2}\\ \pm\sqrt{1-C^2} & 1-C\end{pmatrix}. \quad (4.184)$$

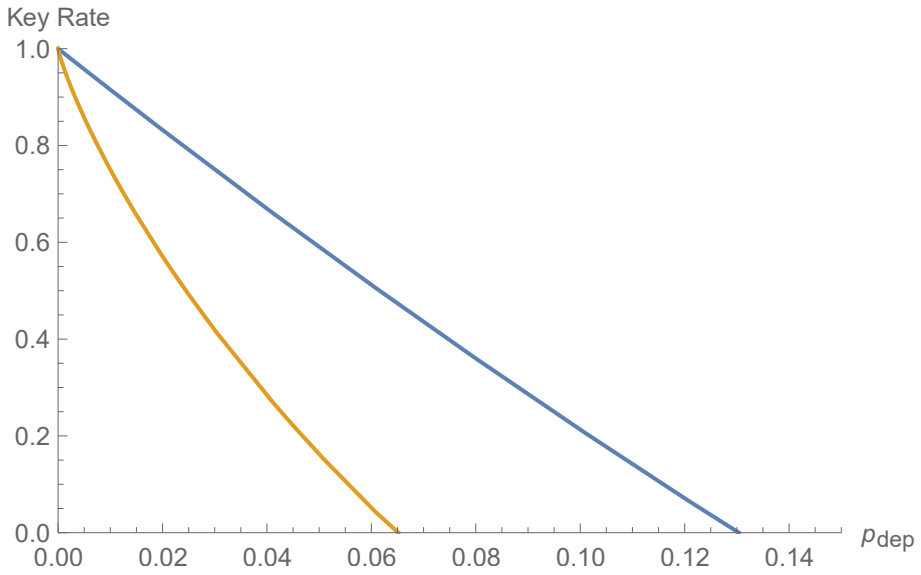


Figure 4.3: The blue line is the plot of tripartite intrinsic non-locality as function of p_{dep} for the state $\mathcal{D}^{\otimes 3}(|\text{GHZ}\rangle\langle\text{GHZ}|)$ using the attack leading to (4.179). The gold line indicates the lower bound calculated from [3].

Note that for the state in (4.174), the parity-CHSH violation S and QBER Q are related as follows: $Q = \frac{1}{2}(1 - \frac{S}{\sqrt{2}})$. After we apply this relation between S and Q, we get a correlation that is parameterized by S. We then calculate an upper bound on quantum tripartite intrinsic non-locality as a function of S and plot it versus S in Figure 4.2. It is important to note that this parameterized correlation is not convex in the parameter S, as required by (4.73); so if such a curve is not convex to begin with, Theorem 23 cannot be invoked to produce a lower, convex curve that is also an upper bound on the quantum tripartite non-locality for the parameterized correlations.

A common qubit noise model is the depolarizing channel, described as

$$\mathcal{D}(\rho) := (1 - p_{\text{dep}})\rho + p_{\text{dep}}\frac{\mathbb{I}}{2}. \tag{4.185}$$

We can then consider a more realistic noise model given by $\rho_{\hat{A}\hat{B}\hat{C}} = \mathcal{D}^{\otimes 3}(|\text{GHZ}\rangle\langle\text{GHZ}|)$. For this state, we can consider the attack leading to (4.179) using the parity-CHSH violation S, given by

$$S = \frac{(1 - p_{\text{dep}})^3}{\sqrt{2}} + \frac{(1 - p_{\text{dep}})^2}{\sqrt{2}}. \tag{4.186}$$

The lower bound from [3] is calculated using the probability of winning the parity-CHSH game, given by

$$p_{\text{win}} = \frac{1}{2} + \frac{(1 - p_{\text{dep}})^3}{2\sqrt{2}} + \frac{p(1 - p_{\text{dep}})^2}{4\sqrt{2}}. \tag{4.187}$$

We plot quantum tripartite intrinsic non-locality against p_{dep} in Figure 4.3.

Here we note that tripartite intrinsic non-locality based on dual total correlation provides the exact same upper bounds when calculated using the attack in (4.179). For the other examples we have studied, tripartite intrinsic non-locality based on conditional dual total correlation gives worse upper bounds than multipartite intrinsic non-locality based on conditional total correlation.

4.11 Conclusion

In this chapter, we defined multipartite intrinsic non-localities using conditonal total correlation and conditional dual total correlation, and we proved that these

quantities are indeed additive and convex upper bounds on the DI conference key agreement capacity. These multipartite intrinsic non-localities are also monotone under local operations and common randomness. A key technical contribution is our derivation of the chain rule for conditional total correlation and conditional dual total correlation, which are applicable to all correlations and may be of independent interest beyond their applications to conference key agreement.

We can also see from Figure 4.2 that there is a significant gap between the upper and lower bounds on tripartite DI conference key agreement, so that there is room for improvement. We also want to find new attacks specific to DI conference key agreement to improve the upper bound further and bring it closer to the lower bound. One can also look at convex combinations of various attacks on DI conference key agreement, as shown for DI quantum key distribution in [183]. Deriving a different multipartite intrinsic non-locality using another information quantity may also be of interest to improve the upper bound.

For future work, we are interested in pursuing more novel DI conference key agreement protocols beyond the one presented in [3]. Specifically, one can look for protocols that have more than one measurement setting in the key generation phase because such protocols require lower detector efficiency for DI quantum key distribution, as shown in [184]. We could also investigate other Bell inequalities presented in [50] in order to find better protocols.

CHAPTER 5

CONCLUSION AND OPEN QUESTIONS

In this thesis, we have explored a few important aspects of multipartite entanglement. The main themes we dealt are as follows: testing multipartite entanglement, certification of multipartite distillable entanglement, and upper bounds on conference key agreement. In analyzing these tasks, we drew inspiration from their bipartite counterparts and gained a better understanding of multipartite entanglement as a whole.

In Chapter 2, we explored how we can test whether a given state is entangled or not. We began by developing a test for bipartite pure states. We then use this test as the basis for a separability test for bipartite mixed states that uses a computationally limited verifier and a computationally unbounded prover. The prover in our analysis is restricted to performing only entanglement-breaking channels. To adapt our separability test to state-of-the-art quantum computers, we replace the prover with parameterized unitary circuits and classical optimization techniques giving us, Variational Quantum Steering Algorithms (VQSAs). VQSAs are charaterized by the inclusion of mid-circuit measurement, allowing for optimizations over pure state decompositions of mixed states. We also simulate our VQSA on noisy quantum simulators. We also develop semi-definite programs to benchmark the performance of our VQSA. We then extend our separability test to the multipartite scenario by modifying the test in accordance with the definitions of multipartite entanglement. We also discuss the computational complexity

of performing our separability test. To do this, we introduced a new complexity class, $\mathrm{QIP}_{\mathrm{EB}}(2)$, and discussed its relationship with other known complexity classes. With this work, we showed a link between entanglement, steering, quantum algorithms, and quantum complexity classes.

From here, we consider it an important open question in quantum computational complexity theory to place a non-trivial upper bound on the class $\mathrm{QIP}_{\mathrm{EB}}(2)$. As indicated in Remark 4, an approach using the known quantum de Finetti theorem from [91, Theorem II.7′] does not appear to be helpful for this task.

In Chapter 4, we develop a technique to quantify resources for device independent conference key agreement, a multipartite generalization of quantum key distribution. Our method, multipartite intrinsic non-locality, is additive, convex, and a monotone under the class of free operations, we call, local operations and common randomness. We show that multipartite intrinsic non-locality is an upper bound on the conference key agreement rate in the device independent scenario. To prove these important properties, we derive a chain rule for two variants of multipartite mutual information. The two variants of multipartite mutual information we use are multipartite generalizations of conditional mutual information. We then dsicuss DI conference key agreement protocols and calculate the tripartite intrinsic non-locality for these protocols and compare them against known lower bounds.

It is still an open question whether either multipartite intrinsic non-locality is indeed a monotone of genuine multipartite Bell non-locality. It is also easy to see

that multipartite intrinsic non-locality is equal to zero for correlations that can be described by a local hidden variable common to all parties involved. However, multipartite intrinsic non-locality is not known to be equal to zero for correlations that fail to be genuinely multipartite nonlocal as defined in [185], such as (for instance) tripartite correlations that can be decomposed into a convex mixture of correlations that are each only bipartite nonlocal.

Finally, we can also look at securing device-independent conference key agreement using just computational assumptions. There have already been attempts at securing DI quantum key distribution and self testing under computational assumptions based on the learning with errors problem [186, 187]. It may be interesting to extend this analysis to the multipartite scenario of DI conference key agreement.

Finally, we discussed how to certify multipartite distillable entanglement in a quantum network. Since the constituent components of a quantum network may vary widely in their underlying technologies, we propose that this certification must be device independent. In Chapter 3, we define multipartite distillable entanglement and device-independent multipartite distillable entanglement certification protocol. A device-independent multipartite distillable entanglement certification protocol must consist of a completeness condition and a soundness condition. Our proposed certification protocol is based on the MABK inequality [41, 42, 43]. We showed that this protocol is complete and sound. To show soundness, we used the entropy accumulation theorem [145], the structure of the

MABK inequality [41, 42, 43], and the multipartite entanglement distillation protocols and rates described in [148, 149].

For future works, we are interested in using other Bell-type inequalities that involve more than two binary measurements or measurements that have more than two outcomes. In this work, we have focused entirely on GHZ states while leaving out the W state. The W and GHZ states are not interconvertible using LOCC alone [188]. Hence, our analysis here for GHZ states does not immediately apply to W states, but it is an interesting extension. It is also worth noting that there are infinitely many classes of genuinely multipartite entangled states that involve four or more parties [189]. It will be interesting to see what a unified certification protocol for such classes of states might look like.

We also note that our results are centered around a protocol based on state merging [148, 149]. One could always consider another protocol that does not involve state merging. An approach that does not rely on the equivalence between Bell inequality and MABK inequality may be necessary for this scenario.

BIBLIOGRAPHY

[1] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 11(4):045021, April 2009. arXiv:0903.4460.

[2] Rotem Arnon-Friedman and Felix Leditzky. Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture. IEEE Transactions on Information Theory, 67(10):6606–6618, June 2021. arXiv:2005.12325.

[3] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. Reply to "Comment on 'Fully device-independent conference key agreement' ". Physical Review A, 100:026302, Aug 2019.

[4] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? Physical Review, 47(10):777–780, May 1935.

[5] John S. Bell. On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, 1:195–200, November 1964.

[6] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. Physical Review Letters, 23:880–884, October 1969.

[7] Ellie D'Hondt and Prakash Panangaden. The computational power of the W and GHZ states, 2006. arXiv:quant-ph/0412177.

[8] Robert Raussendorf and Hans J. Briegel. A One-Way Quantum Computer. Physical Review Letters, 86:5188–5191, May 2001.

[9] Changliang Ren and Holger F. Hofmann. Clock synchronization using maximal multipartite entanglement. Physical Review A, 86:014301, July 2012.

[10] Zachary Eldredge, Michael Foss-Feig, Jonathan A. Gross, S. L. Rolston, and Alexey V. Gorshkov. Optimal and secure measurement protocols for quantum sensor networks. Physical Review A, 97:042337, April 2018.

[11] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin. Quantum-assisted telescope arrays. Physical Review A, 100:022316, August 2019.

[12] Timothy Qian, Jacob Bringewatt, Igor Boettcher, Przemyslaw Bienias, and Alexey V. Gorshkov. Optimal measurement of field properties with quantum sensor networks. Physical Review A, 103:L030601, March 2021.

[13] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. Physical Review A, 59:1829–1834, March 1999.

[14] Changhua Zhu, Feihu Xu, and Changxing Pei. W-state analyzer and multi-party measurement-device-independent quantum key distribution. Scientific Reports, 5(1):17449, December 2015.

[15] Hayata Yamasaki, Alexander Pirker, Mio Murao, Wolfgang Dür, and Barbara Kraus. Multipartite entanglement outperforming bipartite entanglement under limited quantum system sizes. Physical Review A, 98:052313, November 2018.

[16] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Physical Review A, 40(8):4277–4281, October 1989.

[17] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). Communications in Mathematical Physics, 328(1):303–326, March 2014.

[18] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. Quantum entanglement. Reviews of Modern Physics, 81(2):865–942, June 2009. arXiv:quant-ph/0702225.

[19] Leonid Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing, pages 10–19, San Diego, California, USA, June 2003. arXiv:quant-ph/0303055.

[20] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. Quantum Information and Computation, 10(3):343–360, March 2010. arXiv:0810.4507.

[21] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. In Proceedings of the 18th Annual IEEE Conference on Computational Complexity, pages 156–167, Palo Alto, California, USA, June 2013.

[22] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. Quantum Information and Computation, 14(5 & 6):384–416, April 2014. arXiv:1211.6120.

[23] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. Quantum interactive proofs and the complexity of separability testing. Theory of Computing, 11(3):59–103, 2015. arXiv:1308.5788.

[24] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. Entanglement in many-body systems. Reviews of Modern Physics, 80(2):517–576, May 2008. arXiv:quant-ph/0703044.

[25] Marcus Cramer, Martin B. Plenio, and Harald Wunderlich. Measuring entanglement in condensed matter systems. Physical Review Letters, 106(2):020401, January 2011. arXiv:1009.2956.

[26] Nicolas Laflorencie. Quantum entanglement in condensed matter systems. Physics Reports, 646:1–59, August 2016. arXiv:1512.03388.

[27] Tadashi Takayanagi. Entanglement entropy from a holographic viewpoint. Classical and Quantum Gravity, 29(15):153001, June 2012.

[28] Sougato Bose, Anupam Mazumdar, Gavin W. Morley, Hendrik Ulbricht, Marko Toroš, Mauro Paternostro, Andrew A. Geraci, Peter F. Barker, M. S. Kim, and Gerard Milburn. Spin entanglement witness for quantum gravity. Physical Review Letters, 119(24):240401, December 2017. arXiv:1707.06050.

[29] Chiara Marletto and Vlatko Vedral. Gravitationally induced entanglement between two massive particles is sufficient evidence of quantum effects in gravity. Physical Review Letters, 119(24):240402, December 2017. arXiv:1707.06036.

[30] Xiao-Liang Qi. Does gravity come from quantum information? Nature Physics, 14(10):984–987, 2018.

[31] Brian Swingle. Spacetime from entanglement. Annual Review of Condensed Matter Physics, 9(1):345–358, 2018.

[32] Claude Fabre and Nicolas Treps. Modes and states in quantum optics. Reviews of Modern Physics, 92(3):035005, September 2020. arXiv:1912.09321.

[33] Artur K. Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6):661–663, August 1991.

[34] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. Physical Review Letters, 113:140501, September 2014. arXiv:1210.1810.

[35] Charles H. Bennett and Stephen J. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 69(20):2881, November 1992.

[36] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 70(13):1895, March 1993.

[37] Vlatko Vedral, Martin B. Plenio, M. A. Rippin, and Peter L. Knight. Quantifying entanglement. Physical Review Letters, 78(12):2275–2279, March 1997. arXiv:quant-ph/9702027.

[38] Vlatko Vedral and Martin B. Plenio. Entanglement measures and purification procedures. Physical Review A, 57(3):1619–1633, March 1998. arXiv:quant-ph/9707035.

[39] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. Quantum Information and Computation, 4(4):273–286, July 2004.

[40] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. Journal of Physics A: Mathematical and Theoretical, 45(45):455304, October 2012.

[41] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. Physical Review A, 46:5375–5378, November 1992.

[42] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. Physical Review Letters, 65:1838–1840, October 1990.

[43] A. V. Belinskiĭ and D. N. Klyshko. Interference of light and Bell's theorem. Physics-Uspekhi, 36(8):653, August 1993.

[44] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In Proceedings. 19th IEEE Annual Conference on Computational Complexity, pages 236–249, 2004.

[45] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. Fully device-independent conference key agreement. Physical Review A, 97:022307, February 2018.

[46] Michael Epping, Hermann Kampermann, and Dagmar Bruß. Large-scale quantum networks based on graphs. New Journal of Physics, 18(5):053036, May 2016. arXiv:1504.06599.

[47] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. Quantum conference key agreement: A review. Advanced Quantum Technologies, 3(11):2000025, November 2020.

[48] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 81:3018–3021, October 1998.

[49] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. Finite-key

effects in multipartite quantum key distribution protocols. New Journal of Physics, 20(11):113014, November 2018.

[50] Timo Holz, Hermann Kampermann, and Dagmar Bruß. A genuine multipartite Bell inequality for device-independent conference key agreement. Physical Review Research, 2:023251, May 2020. arXiv:1910.11360.

[51] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. Variational quantum algorithms. Nature Reviews Physics, 3(9):625–644, August 2021. arXiv:2012.09265.

[52] Bryan T. Gard, Linghua Zhu, George S. Barron, Nicholas J. Mayhall, Sophia E. Economou, and Edwin Barnes. Efficient symmetry-preserving state preparation circuits for the variational quantum eigensolver algorithm. npj Quantum Information, 6(1):10, January 2020.

[53] Matthew Otten, Cristian L. Cortes, and Stephen K. Gray. Noise-resilient quantum dynamics using symmetry-preserving ansatzes, 2019. arXv:1910.06284.

[54] Zoë Holmes, Kunal Sharma, M. Cerezo, and Patrick J. Coles. Connecting ansatz expressibility to gradient magnitudes and barren plateaus. PRX Quantum, 3:010313, January 2022.

[55] Jirawat Tangpanitanon, Supanut Thanasilp, Ninnat Dangniam, Marc-Antoine Lemonde, and Dimitris G. Angelakis. Expressibility and trainabil-

ity of parametrized analog quantum systems for machine learning applications. Physical Review Research, 2:043364, December 2020.

[56] Jarrod R. McClean, Sergio Boixo, Vadim N. Smelyanskiy, Ryan Babbush, and Hartmut Neven. Barren plateaus in quantum neural network training landscapes. Nature Communications, 9(1):4812, 2018. arXiv:1803.11173.

[57] Marco Cerezo, Akira Sone, Tyler Volkoff, Lukasz Cincio, and Patrick J. Coles. Cost function dependent barren plateaus in shallow parametrized quantum circuits. Nature Communications, 12(1):1791, March 2021. arXiv:2001.00550.

[58] J. P. Home, M. J. McDonnell, D. M. Lucas, G. Imreh, B. C. Keitch, D. J. Szwer, N. R. Thomas, S. C. Webster, D. N. Stacey, and A. M. Steane. Deterministic entanglement and tomography of ion–spin qubits. New Journal of Physics, 8(9):188–188, September 2006. arXiv:quant-ph/0603273.

[59] Matthias Steffen, M. Ansmann, Radoslaw C. Bialczak, N. Katz, Erik Lucero, R. McDermott, Matthew Neeley, E. M. Weig, A. N. Cleland, and John M. Martinis. Measurement of the entanglement of two superconducting qubits via state tomography. Science, 313(5792):1423–1425, September 2006.

[60] Asher Peres. Separability criterion for density matrices. Physical Review Letters, 77(8):1413–1415, August 1996. arXiv:quant-ph/9604005.

[61] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separabil-

ity of mixed states: necessary and sufficient conditions. Physics Letters A, 223(1-2):1–8, November 1996. arXiv:quant-ph/9605038.

[62] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. Letters in Mathematical Physics, 17(4):359–363, May 1989.

[63] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. Physical Review A, 69(2):022308, February 2004. arXiv:quant-ph/0308032.

[64] Margarite L. LaBorde, Soorya Rethinasamy, and Mark M. Wilde. Testing symmetry on quantum computers. Quantum, 7:1120, September 2023. arXiv:2105.12758.

[65] Erwin Schrödinger. Die gegenwärtige situation in der quantenmechanik. Die Naturwissenschaften, 23(50):844–849, December 1935.

[66] Erwin Schrödinger. Discussion of probability relations between separated systems. Mathematical Proceedings of the Cambridge Philosophical Society, 31(4):555–563, October 1935.

[67] Daniel Cavalcanti and Paul Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. Reports on Progress in Physics, 80(2):024001, December 2016. arXiv:1604.00501.

[68] Roope Uola, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne. Quan-

tum steering. Reviews of Modern Physics, 92(1):015001, March 2020. arXiv:1903.06663.

[69] Shuheng Liu, Dongmei Han, Na Wang, Yu Xiang, Fengxiao Sun, Meihong Wang, Zhongzhong Qin, Qihuang Gong, Xiaolong Su, and Qiongyi He. Experimental demonstration of remotely creating Wigner negativity via quantum steering. Physical Review Letters, 128(20):200401, May 2022. arXiv:2204.11552.

[70] Marie Ioannou, Bradley Longstaff, Mikkel V. Larsen, Jonas S. Neergaard-Nielsen, Ulrik L. Andersen, Daniel Cavalcanti, Nicolas Brunner, and Jonatan Bohr Brask. Steering-based randomness certification with squeezed states and homodyne measurements. Physical Review A, 106(4):042414, October 2022. arXiv:2111.06186.

[71] Bernhard Wittmann, Sven Ramelow, Fabian Steinlechner, Nathan K. Langford, Nicolas Brunner, Howard M. Wiseman, Rupert Ursin, and Anton Zeilinger. Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering. New Journal of Physics, 14(5):053030, May 2012. arXiv:1111.0760.

[72] Meng Wang, Yu Xiang, Qiongyi He, and Qihuang Gong. Detection of quantum steering in multipartite continuous-variable Greenberger-Horne-Zeilinger–like states. Physical Review A, 91(1):012112, January 2015.

[73] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[74] John Watrous. Quantum computational complexity. Encyclopedia of Complexity and System Science, 2009. arXiv:0804.3401.

[75] Thomas Vidick and John Watrous. Quantum proofs. Foundations and Trends in Theoretical Computer Science, 11(1–2):1–215, March 2016. arXiv:1610.01664.

[76] Mirko Consiglio, Tony John George Apollaro, and Marcin Wieśniak. Variational approach to the quantum separability problem. Physical Review A, 106(6):062413, December 2022. arXiv:2209.01430.

[77] Xu-Fei Yin, Yuxuan Du, Yue-Yang Fei, Rui Zhang, Li-Zheng Liu, Yingqiu Mao, Tongliang Liu, Min-Hsiu Hsieh, Li Li, Nai-Le Liu, Dacheng Tao, Yu-Ao Chen, and Jian-Wei Pan. Efficient bipartite entanglement detection scheme with a quantum adversarial solver. Physical Review Letters, 128(11):110501, March 2022. arXiv:2203.07749.

[78] Kun Wang, Zhixin Song, Xuanqiang Zhao, Zihe Wang, and Xin Wang. Detecting and quantifying entanglement on near-term quantum devices. npj Quantum Information, 8(1):52, 2022.

[79] A. D. Muñoz Moller, L. Pereira, L. Zambrano, J. Cortés-Vega, and A. Delgado. Variational determination of multiqubit geometrical entanglement in noisy intermediate-scale quantum computers. Physical Review Applied, 18(2):024048, August 2022.

[80] George Androulakis and Ryan McGaha. Variational quantum algorithm

for approximating convex roofs. Quantum Information and Computation, 22(13&14):1081–1109, October 2022. arXiv:2203.02099.

[81] Gavin K. Brennen. An observable measure of entanglement for pure states of multi-qubit systems. Quantum Information and Computation, 3(6):619–626, 2003. arXiv:quant-ph/9604024.

[82] Aram Harrow and Ashley Montanaro. An efficient test for product states with applications to quantum Merlin–Arthur games. In Proceedings of the 51st Annual IEEE Symposium on the Foundations of Computer Science (FOCS), pages 633–642, Las Vegas, Nevada, USA, October 2010. arXiv:1001.0017.

[83] Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. SIAM Journal on Computing, 26(5):1541–1557, 1997. arXiv:quant-ph/9604028.

[84] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. Physical Review Letters, 87(16):167902, September 2001. arXiv:quant-ph/0102001.

[85] John Watrous. The Theory of Quantum Information. Cambridge University Press, 2018.

[86] Michal Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement

breaking channels. Reviews in Mathematical Physics, 15(6):629–641, August 2003. arXiv:quant-ph/0302031.

[87] A. Uhlmann. The "transition probability" in the state space of a $*$-algebra. Reports on Mathematical Physics, 9(2):273–279, April 1976.

[88] Alexander Streltsov, Hermann Kampermann, and Dagmar Bruß. Linking a distance measure of entanglement to its convex roof. New Journal of Physics, 12(12):123004, December 2010. arXiv:1006.3077.

[89] John Watrous. Simpler semidefinite programs for completely bounded norms. Chicago Journal of Theoretical Computer Science, July 2013. arXiv:1207.5726.

[90] Hamza Fawzi. The set of separable states has no finite semidefinite representation except in dimension 3×2. Communications in Mathematical Physics, 386(3):1319–1335, September 2021. arXiv:1905.02575.

[91] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. Communications in Mathematical Physics, 273(2):473–498, July 2007. arXiv:quant-ph/0602130.

[92] Alexey E. Rastegin. Sine distance for quantum states, February 2006. arXiv:quant-ph/0602112.

[93] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. IEEE Transactions on Information Theory, 45(4):1216, May 1999. arXiv:quant-ph/9712042.

[94] Lukasz Pankowski, Fernando G. S. L. Brandao, Michal Horodecki, and Graeme Smith. Entanglement distillation by extendible maps. Quantum Information and Computation, 13(9–10):751–770, September 2013. arXiv:1109.1779.

[95] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. Physical Review Letters, 123(7):070502, 2019. arXiv:2108.03137.

[96] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource theory of unextendibility and nonasymptotic quantum capacity. Physical Review A, 104(2):022401, August 2021. arXiv:1803.10710.

[97] Mario Berta, Francesco Borderi, Omar Fawzi, and Volkher Scholz. Semidefinite programming hierarchies for constrained bilinear optimization. Mathematical Programming, 194:781–829, July 2022. arXiv:1810.12197.

[98] Joel J. Wallman and Steven T. Flammia. Randomized benchmarking with confidence. New Journal of Physics, 16(10):103032, October 2014. arXiv:1404.6025.

[99] Sumeet Khatri, Ryan LaRose, Alexander Poremba, Lukasz Cincio, Andrew T. Sornborger, and Patrick J. Coles. Quantum-assisted quantum compiling. Quantum, 3:140, May 2019. arXiv:1807.00800.

[100] L. Zambrano, A. D. Muñoz-Moller, M. Muñoz, L. Pereira, and A. Delgado.

Avoiding barren plateaus in the variational determination of geometric entanglement. Quantum Science and Technology, 9(2):025016, February 2024.

[101] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M. Chow, and Jay M. Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. Nature, 549(7671):242–246, 2017. arXiv:1704.05018.

[102] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 2009.

[103] Benjamin Schumacher. Quantum coding. Physical Review A, 51(4):2738–2747, April 1995.

[104] Nilanjana Datta, Min-Hsiu Hsieh, and Mark M. Wilde. Quantum rate distortion, reverse Shannon theorems, and source-channel separation. IEEE Transactions on Information Theory, 59(1):615–630, January 2013. arXiv:1108.4940.

[105] Koenraad M. R. Audenaert, Christopher A. Fuchs, Christopher King, and Andreas Winter. Multiplicativity of accessible fidelity and quantumness for sets of quantum states. Quantum Information and Computation, 4(1):1–11, January 2004. arXiv:quant-ph/0308120.

[106] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. Reviews of Modern Physics, 77(4):1225–1256, November 2005. arXiv:quant-ph/0511088.

[107] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. In Proceedings of the 19th IEEE Annual Conference on Computational Complexity, pages 275–285. IEEE, June 2004. arXiv:cs/0506068.

[108] John Watrous. Zero-knowledge against quantum attacks. In Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing, pages 296–305, May 2006. arXiv:quant-ph/0511020.

[109] Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M. Wilde. Estimating distinguishability measures on quantum computers. Physical Review A, 108:012409, July 2023. arXiv:2108.08406.

[110] John Watrous. Limits on the power of quantum statistical zero-knowledge. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pages 459–468, November 2002. arXiv:quant-ph/0202111.

[111] Carl W. Helstrom. Detection theory and quantum mechanics. Information and Control, 10(3):254–291, 1967.

[112] Carl W. Helstrom. Quantum detection and estimation theory. Journal of Statistical Physics, 1:231–252, 1969.

[113] Matthew Treinish et al. Qiskit: An open-source framework for quantum computing, 2023. https://doi.org/10.5281/zenodo.2573505.

[114] Xuanqiang Zhao, Benchi Zhao, Zihe Wang, Zhixin Song, and Xin Wang.

Practical distributed quantum information processing with LOCCNet. npj Quantum Information, 7(1):159, November 2021. arXiv:2101.12190.

[115] Brian Doolittle, R. Thomas Bromley, Nathan Killoran, and Eric Chitambar. Variational quantum optimization of nonlocality in noisy quantum networks. IEEE Transactions on Quantum Engineering, 4:1–27, 2023. arXiv:2205.02891.

[116] Yun-Fei Niu, Shuo Zhang, Chen Ding, Wan-Su Bao, and He-Liang Huang. Parameter-parallel distributed variational quantum algorithm. SciPost Physics, 14:132, 2023. arXiv:2208.00450.

[117] Tillmann Baumgratz, Marcus Cramer, and Martin B. Plenio. Quantifying coherence. Physical Review Letters, 113(14):140401, September 2014. arXiv:1311.0275.

[118] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau. Repeated quantum error correction on a continuously encoded qubit by real-time feedback. Nature Communications, 7(1):11526, May 2016. arXiv:1508.01388.

[119] Laird Egan, Dripto M. Debroy, Crystal Noel, Andrew Risinger, Daiwei Zhu, Debopriyo Biswas, Michael Newman, Muyuan Li, Kenneth R. Brown, Marko Cetina, and Christopher Monroe. Fault-tolerant control of an error-corrected qubit. Nature, 598(7880):281–286, October 2021. arXiv:2009.11482.

[120] Rajeev Acharya et al. Suppressing quantum errors by scaling a surface code logical qubit. Nature, 614(7949):676–681, February 2023.

[121] T. M. Graham, L. Phuttitarn, R. Chinnarasu, Y. Song, C. Poole, K. Jooya, J. Scott, A. Scott, P. Eichler, and M. Saffman. Midcircuit measurements on a single-species neutral alkali atom quantum processor. Physical Review X, 13:041051, December 2023.

[122] Aby Philip, Soorya Rethinasamy, Vincent Russo, and Mark M. Wilde. Schrödinger as a quantum programmer: Estimating entanglement via steering. Quantum, 8:1366, June 2024. arXiv:2303.07911.

[123] Guillaume Sagnol and Maximilian Stahlberg. PICOS: A Python interface to conic optimization solvers. Journal of Open Source Software, 7(70):3915, February 2022.

[124] Lieven Vandenberghe. The CVXOPT linear and quadratic cone program solvers, 2010. www.seas.ucla.edu/~vandenbe/publications/coneprog.pdf.

[125] Vincent Russo. TOQITO–theory of quantum information toolkit: A python package for studying quantum information. Journal of Open Source Software, 6(61):3082, 2021.

[126] A. Streltsov, C. Meignant, and J. Eisert. Rates of Multipartite Entanglement Transformations. Physical Review Letters, 125:080502, August 2020.

[127] O. Jiménez Farías, G. H. Aguilar, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn. Observation of the emergence of multipartite entanglement between a bipartite system and its environment. Physical Review Letters, 109:150403, October 2012.

[128] H. Cao, L. M. Hansen, F. Giorgino, L. Carosini, P. Zahálka, F. Zilk, J. C. Loredo, and P. Walther. Photonic Source of Heralded Greenberger-Horne-Zeilinger states. Physical Review Letters, 132:130604, March 2024.

[129] K. S. Christensen, S. E. Rasmussen, D. Petrosyan, and N. T. Zinner. Coherent router for quantum networks with superconducting qubits. Physical Review Research, 2:013004, January 2020.

[130] Youpeng Zhong, Hung-Shen Chang, Audrey Bienfait, Étienne Dumur, Ming-Han Chou, Christopher R Conner, Joel Grebel, Rhys G Povey, Haoxiong Yan, David I Schuster, et al. Deterministic multi-qubit entanglement in a quantum network. Nature, 590(7847):571–575, 2021.

[131] Zhang-qi Yin, W. L. Yang, L. Sun, and L. M. Duan. Quantum network of superconducting qubits through an optomechanical interface. Physical Review A, 91:012333, January 2015.

[132] L. J. Stephenson, D. P. Nadlinger, B. C. Nichol, S. An, P. Drmota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance. High-Rate, High-Fidelity Entanglement of Qubits Across an Elementary Quantum Network. Physical Review Letters, 124:110501, March 2020.

[133] 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.

[134] Ignatius W. Primaatmaja, Koon Tong Goh, Ernest Y.-Z. Tan, John T.-F. Khoo, Shouvik Ghorai, and Charles C.-W. Lim. Security of device-independent quantum key distribution protocols: a review. Quantum, 7:932, March 2023.

[135] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. Advances in device-independent quantum key distribution. npj Quantum Information, 9(1):10, February 2023.

[136] Károly F. Pál, Tamás Vértesi, and Miguel Navascués. Device-independent tomography of multipartite quantum states. Physical Review A, 90:042340, October 2014.

[137] Matthew McKague. Self-Testing Graph States. In Dave Bacon, Miguel Martin-Delgado, and Martin Roetteler, editors, Theory of Quantum Computation, Communication, and Cryptography, pages 104–120. Springer Berlin Heidelberg, 2014.

[138] J.M.K Kaniewski. Analytic and nearly optimal self-testing bounds for the clauser-horne-shimony-holt and mermin inequalities. Physical Review Letters, 117:070402, August 2016.

[139] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. Quantum, 4:337, September 2020.

[140] Sébastien Designolle, Tamás Vértesi, and Sebastian Pokutta. Symmetric multipartite Bell inequalities via Frank-Wolfe algorithms. Physical Review A, 109:022205, February 2024.

[141] Thinh P. Le, Chiara Meroni, Bernd Sturmfels, Reinhard F. Werner, and Timo Ziegler. Quantum Correlations in the Minimal Scenario. Quantum, 7:947, March 2023.

[142] Aby Philip, Eneet Kaur, Peter Bierhorst, and Mark M. Wilde. Multipartite Intrinsic Non-Locality and Device-Independent Conference Key Agreement. Quantum, 7:898, January 2023. arXv:2111.02596.

[143] Karol Horodecki, Marek Winczewski, and Siddhartha Das. Fundamental limitations on the device-independent quantum conference key agreement. Physical Review A, 105:022604, February 2022.

[144] Rotem Arnon-Friedman and Jean-Daniel Bancal. Device-independent certification of one-shot distillable entanglement. New Journal of Physics, 21(3):033010, March 2019.

[145] Frédéric Dupuis, Omar Fawzi, and Renato Renner. Entropy Accumulation. Communications in Mathematical Physics, 379(3):867–913, September 2020.

[146] Marco Tomamichel. Quantum Information Processing with Finite

Resources–Mathematical Foundations. Springer Publishing Company, Incorporated, 1st edition, 2015.

[147] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association, 58(301):13–30, March 1963.

[148] Pau Colomer and Andreas Winter. Decoupling by local random unitaries without simultaneous smoothing, and applications to multi-user quantum information tasks, 2023. arXiv:2304.12114.

[149] Farzin Salek and Andreas Winter. New protocols for conference key and Multipartite Entanglement Distillation, 2023. arXiv:2308.01134.

[150] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. In 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), pages 844–850, 2022.

[151] Valerio Scarani. The device-independent outlook on quantum physics. Acta Physica Slovaca, 62(1), January 2012. arXiv:1303.3081.

[152] Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß. Entropy Bounds for Multiparty Device-Independent Cryptography. PRX Quantum, 2:010308, January 2021.

[153] Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. Journal of Mathematical Physics, 14(12):1938–1941, 12 1973.

[154] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. Physical Review A, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[155] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pages 175–179, March 1984.

[156] Dominic Mayers. Unconditional security in quantum cryptography. Journal of the ACM, 48(3):351–406, May 2001. arXiv:quant-ph/9802025.

[157] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. Physical Review Letters, 106:110506, March 2011. arXiv:1009.2015.

[158] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. Physical Review A, 85:010301, January 2012. arXiv:1109.1435.

[159] Dominic Mayers and Andrew. Yao. Quantum cryptography with imperfect apparatus. In Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), pages 503–509, November 1998. arXiv:quant-ph/9809039.

[160] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Piro-

nio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. Physical Review Letters, 98:230501, June 2007. arXiv:quant-ph/0702152.

[161] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. Nature Communications, 9(1):1–11, January 2018.

[162] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. Nature Communications, 5(1):1–7, October 2014. arXiv:1504.06390.

[163] Eneet Kaur, Mark M. Wilde, and Andreas Winter. Fundamental limits on key rates in device-independent quantum key distribution. New Journal of Physics, 22(2):023039, February 2020. arXiv:1810.05627.

[164] Marek Winczewski, Tamoghna Das, and Karol Horodecki. Limitations on device independent key secure against non signaling adversary via the squashed non-locality. March 2019. arXiv:1903.12154.

[165] Ueli M. Maurer and Stephan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. IEEE Transactions on Information Theory, 45(2):499–514, March 1999.

[166] Matthias Christandl and Andreas Winter. "Squashed entanglement": an additive entanglement measure. Journal of Mathematical Physics, 45(3):829–840, March 2004. arXiv:quant-ph/0308088.

[167] Eneet Kaur, Xiaoting Wang, and Mark M. Wilde. Conditional mutual information and quantum steering. Physical Review A, 96:022332, August 2017. arXiv:1612.03875.

[168] Satosi Watanabe. Information theoretical analysis of multivariate correlation. IBM Journal of Research and Development, 4(1):66–82, January 1960.

[169] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. IEEE Transactions on Information Theory, 55(7):3375–3387, July 2009. arXiv:0704.2236.

[170] David Avis, Patrick Hayden, and Ivan Savov. Distributed compression and multiparty squashed entanglement. Journal of Physics A: Mathematical and Theoretical, 41(11):115301, March 2008. arXiv:0707.2792.

[171] Kaushik P. Seshadreesan, Masahiro Takeoka, and Mark M. Wilde. Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. IEEE Transactions on Information Theory, 62(5):2849–2866, March 2016. arXiv:1503.08139.

[172] David Beckman, Daniel Gottesman, Michael A Nielsen, and John Preskill. Causal and localizable quantum operations. Physical Review A, 64(5):052309, October 2001. arXiv:quant-ph/0102043.

[173] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and

Stephanie Wehner. Bell nonlocality. Reviews of Modern Physics, 86(2):419, April 2014. arXiv:1303.2849.

[174] Ke Li and Andreas Winter. Squashed entanglement, **k**-extendibility, quantum Markov chains, and recovery maps. Foundations of Physics, 48(8):910–924, February 2018. arXiv:1410.4184.

[175] Maksim E. Shirokov. Uniform continuity bounds for characteristics of multipartite quantum systems. Journal of Mathematical Physics, 62(9):092206, September 2021. arXiv:2007.00417.

[176] Itamar Pitowsky. The range of quantum probability. Journal of Mathematical Physics, 27(6):1556–1565, June 1986.

[177] Manuel Forster, Severin Winkler, and Stefan Wolf. Distilling nonlocality. Physical Review Letters, 102:120401, March 2009. arXiv:0809.3173.

[178] Manuel Forster and Stefan Wolf. Bipartite units of nonlocality. Physical Review A, 84:042112, October 2011. arXiv:0808.0651.

[179] Rodrigo Gallego and Leandro Aolita. Nonlocality free wirings and the distinguishability between Bell boxes. Physical Review A, 95:032118, March 2017. arXiv:1611.06932.

[180] Te Sun Han. Linear dependence structure of the entropy space. Information and Control, 29(4):337–368, December 1975.

[181] Te Sun Han. Nonnegative entropy measures of multivariate symmetric correlations. Information and Control, 36(2):133–156, February 1978.

[182] Dong Yang, Michał Horodecki, and Z. D. Wang. An additive and operational entanglement measure: Conditional entanglement of mutual information. Physical Review Letters, 101:140501, September 2008. arXiv:0804.3683.

[183] Eneet Kaur, Karol Horodecki, and Siddhartha Das. Upper bounds on device-independent quantum key distribution rates in static and dynamic scenarios. Physical Review Applied, 18(5):054033, November 2021. arXiv:2107.06411.

[184] Junior R. Gonzales-Ureta, Ana Predojević, and Adán Cabello. Device-independent quantum key distribution based on Bell inequalities with more than two inputs and two outputs. Physical Review A, 103:052436, May 2021. arXiv:2104.00413.

[185] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. Definitions of multipartite nonlocality. Physical Review A, 88(1):014102, July 2013. arXiv:1112.2626.

[186] Tony Metger, Yfke Dulek, Andrea Coladangelo, and Rotem Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. New Journal of Physics, 23(12):123021, December 2021.

[187] Tony Metger and Thomas Vidick. Self-testing of a single quantum device under computational assumptions. Quantum, 5:544, September 2021. arXiv:2001.0916.

[188] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. Physical Review A, 62:062314, November 2000.

[189] J. I. de Vicente, C. Spee, and B. Kraus. Maximally entangled set of multipartite quantum states. Physical Review Letter, 111:110502, September 2013.