Randomized measurements as a tool in quantum information processing

Dissertation
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
Satoya Imai

eingereicht bei der
Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen,
Siegen, 2023

Universität Siegen

TQO Theoretical Quantum Optics

Gutachter:
Prof. Otfried Gühne
Prof. Géza Tóth

Prüfer:
Prof. Otfried Gühne
Prof. Géza Tóth
Prof. Mario Agio
Dr. Stefan Nimmrichter

Datum der mündlichen Prüfung: 20.09.2023

Abstract

With limited control over quantum systems, how can we extract information about them and characterize their properties? This thesis addresses this question from several perspectives. After explaining the basic concepts of quantum information, we investigate various methods for the analysis of quantum states.

In the first part of the thesis, we develop abstract theories of the so-called randomized measurements. The idea is to randomly rotate measurement directions and examine quantum correlations based on the statistical moments of the resulting probability distribution. This method eliminates the need for calibration of measurement devices or a common reference frame between spatially-separated parties. First, we present several criteria for detecting multipartite entanglement and bound entanglement from randomized measurements. Next, we propose hierarchies of multiqubit entanglement criteria and analyze the statistical significance using large deviation bounds. Finally, we provide the complete characterization of two-qubit entanglement from randomized measurements.

In the second part, we explore several applications of randomized measurements. First, we probe the dimensionality of entanglement from work fluctuations in randomized two-point energy measurement protocols in thermodynamic systems. Second, we advance reference-frame-independent quantum metrology to estimate precision under nonlinear Hamiltonian dynamics. Third, we introduce different approaches to characterize spin squeezing by establishing the scheme of collective randomized measurements. Lastly, we advance methods to certify entanglement based on the moments of the partially transposed density matrix.

In the last part, we deepen the understanding of quantum correlations from geometrical viewpoints. First, we study various constraints on three-qubit states in terms of two-body correlations. Second, we offer quantum speed limits describing the divergence of a perturbed open system from its unperturbed trajectory. Finally, we provide a formulation to discuss the sensitivity of multiparticle entanglement under the classicalization of one particle.

Keywords: Quantum information theory, Separability problems, Entanglement detection, Bloch decompositions, Spin squeezing, Randomized measurements, Haar random unitaries, Reference-frame-independent scenarios, Local unitary invariants

Zusammenfassung

Wie können wir bei begrenzter Kontrolle über Quantensysteme Informationen über sie gewinnen und ihre Eigenschaften charakterisieren? In dieser Arbeit wird diese Frage aus verschiedenen Blickwinkeln betrachtet. Nachdem wir die grundlegenden Konzepte der Quanteninformationstheorie erläutert haben, untersuchen wir verschiedene Methoden zur Analyse von Quantenzuständen.

Im ersten Teil der Arbeit entwickeln wir abstrakte Theorien zu den sogenannten randomisierten Messungen. Die Idee besteht darin, die Messrichtungen zufällig zu drehen und Quantenkorrelationen auf der Grundlage der statistischen Momente der resultierenden Wahrscheinlichkeitsverteilung zu untersuchen. Diese Methode macht eine Kalibrierung der Messgeräte oder einen gemeinsamen Bezugsrahmen zwischen räumlich getrennten Parteien überflüssig. Zunächst stellen wir mehrere Kriterien für die Detektierung von Mehrteilchen-Verschränkung und *bound entanglement* mithilfe randomisierter Messungen vor. Als nächstes schlagen wir Hierarchien von Multiqubit-Verschränkungskriterien vor und analysieren die statistische Signifikanz unter Verwendung statistischer Abschätzungen. Schließlich liefern wir eine vollständige Charakterisierung der Zwei-Qubit-Verschränkung aus zufälligen Messungen.

Im zweiten Teil untersuchen wir verschiedene Anwendungen von randomisierten Messungen. Zunächst untersuchen wir die Dimensionalität der Verschränkung anhand von Arbeitsfluktuationen in randomisierten Zwei-Punkt-Energiemessprotokollen in thermodynamischen Systemen. Zweitens entwickeln wir die vom Bezugssystem unabhängige Quantenmetrologie weiter, um die Präzision unter nichtlinearer Hamilton-Dynamik abzuschätzen. Drittens stellen wir verschiedene Ansätze zur Charakterisierung von *Spin-Squeezing* vor, indem wir das Schema kollektiver randomisierter Messungen etablieren. Schließlich entwickeln wir Methoden zum Nachweis der Verschränkung auf der Grundlage der Momente der teilweise transponierten Dichtematrix.

Im letzten Teil vertiefen wir das Verständnis von Quantenkorrelationen unter geometrischen Gesichtspunkten. Erstens untersuchen wir verschiedene Beschränkungen für Drei-Qubit-Zustände in Form von Zwei-Teilchen-Korrelationen. Zweitens leiten wir Quantengeschwindigkeitsgrenzen her, die die Abweichung eines gestörten offenen Systems von seiner ungestörten Trajektorie beschreiben. Schließlich liefern wir eine Formulierung, um die Empfindlichkeit der Mehrteilchen-Verschränkung bei der *Classicalization* eines Teilchens zu diskutieren.

List of Projects

[1] Satoya Imai, Nikolai Wyderka, Andreas Ketterer, Otfried Gühne,
Bound entanglement from randomized measurements,
Physical Review Letters **126**, 150501 (2021).
Preprint: arXiv:2010.08372.
Chapter 2 contains this content.

[2] Andreas Ketterer, Satoya Imai, Nikolai Wyderka, Otfried Gühne,
Statistically significant tests of multiparticle quantum correlations based on randomized measurements,
Physical Review A **106**, L010402 (2022).
Preprint: arXiv:2012.12176.
Chapter 3 contains this content.

[3] Xiao-Dong Yu, Satoya Imai, Otfried Gühne,
Optimal entanglement certification from moments of the partial transpose,
Physical Review Letters **127**, 060504 (2021).
Preprint: arXiv:2103.06897.
Chapter 8 contains this content.

[4] Satoya Imai, Otfried Gühne, Stefan Nimmrichter,
Work fluctuations and entanglement in quantum batteries,
Physical Review A **107**, 022215 (2023).
Preprint: arXiv:2205.08447.
Chapter 5 contains this content.

[5] Zhen-Peng Xu, Satoya Imai, Otfried Gühne,
Fate of multiparticle entanglement when one particle becomes classical,
Physical Review A **107**, L040401 (2023).
Preprint: arXiv:2206.12834.
Chapter 12 contains this content.

[6] Nikolai Wyderka, Andreas Ketterer, Satoya Imai, Jan Lennart Bönsel, Daniel E. Jones, Brian T. Kirby, Xiao-Dong Yu, Otfried Gühne,
Complete characterization of quantum correlations by randomized measurements,
Physical Review Letters **131**, 090201 (2023).
Preprint: arXiv:2212.07894.
Chapter 4 contains this content.

[7] Paweł Cieśliński*, Satoya Imai*, Jan Dziewior, Otfried Gühne, Lukas Knips, Wiesław Laskowski, Jasmin Meinecke, Tomasz Paterek, Tamás Vértesi,
Analysing quantum systems with randomised measurements,
Preprint: arXiv:2307.01251.
*These authors contributed equally as co-first authors.
Sections 1.4 and 1.5 contain this content.

[8] Chao Zhang, Yuan-Yuan Zhao, Nikolai Wyderka, Satoya Imai, Andreas Ketterer, Ning-Ning Wang, Kai Xu, Keren Li, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Otfried Gühne,
Experimental verification of bound and multiparticle entanglement with the randomized measurement toolbox,
Preprint: arXiv:2307.04382.
Chapter 2 contains this content.

[9] Benjamin Yadin, Satoya Imai, Otfried Gühne,
Quantum speed limit for perturbed open systems,
Preprint: arXiv:2307.09118.
Chapter 11 contains this content.

[10] Satoya Imai, Otfried Gühne, Géza Tóth,
Reference-frame-independent quantum metrology,
in preparation.
Chapter 6 contains this content.

[10] Satoya Imai, Géza Tóth, Otfried Gühne,
Collective randomized measurements in quantum information processing,
Preprint: arXiv:2309.10745.
Chapter 7 contains this content.

[11] Shravan Shravan, Simon Morelli, Otfried Gühne, Satoya Imai,
Geometry of two-body correlations in three-qubit states,
Preprint: arXiv:2309.09549.
Chapter 10 contains this content.

Contents

Preface

According to Asher Peres, “The simple and obvious truth is that quantum phenomena do not occur in a Hilbert space. They occur in a laboratory. If you visit a real laboratory, you will never find there Hermitian operators. All you can see are emitters (lasers, ion guns, synchrotrons and the like) and detectors. The experimenter controls the emission process and observes detection events.", as stated in Ref. [12]. This thesis underscores Peres’s standpoint on quantum mechanics and aims to tackle several scenarios with limited control over quantum systems.

Measurement involves extracting information from a system. As the basic unit of information, a classical bit has discrete values of either 0 or 1. In contrast, a quantum bit (qubit) can exist in a superposition of the two different states due to its characterization by continuous parameters. This distinction has profound implications for information processing. At the same time, qubit systems are more susceptible to disruptions. Measuring a quantum system disrupts its superposition.

Entanglement is a superposition of products of states in a composite quantum system. It was initially considered by Einstein, Podolsky, and Rosen [13] and Schrödinger [14] as “spooky action at a distance" and later recognized by Bell [15, 16] as a quantum phenomenon testable in experiments. Its properties underlie the phenomenon of non-locality, which cannot be simulated classically, and attract the attention of physicists not only from fundamental but also operational perspectives, in terms of a valuable resource for enhancing the performance of information processing.

Quantum information processing stands on the existence of entanglement. On the other hand, a crucial challenge is to determine whether a quantum state created in a laboratory is indeed entangled [17]. Despite the rapid development of experimental technologies, detecting the signature of entanglement remains difficult due to unavoidable noise effects or imperfect measurement setups.

Then, how can we extract information about an entangled quantum system under limited control? This thesis delves into the possibilities when measurements are randomly performed. We will see that randomized measurements are potent tools for analyzing quantum systems. In particular, we will develop several strategies for how randomized measurements allow us to detect and characterize entanglement.

This thesis is organized as follows. In Chapter 1, we give basic introductions to quantum information, entanglement, metrology, randomized measurements,

and quantum designs.

In Chapters 2, 3, 4, we advance abstract theories of the randomized measurements. In Chapter 2, we discuss the detection of tripartite entanglement and bound entanglement from randomized measurements. In Chapter 3, we provide criteria for multiqubit entanglement and develop the statistically significant test of randomized measurements. In Chapter 4, we consider two-qubit entangled states and show that they can be completely characterized from randomized measurements.

In Chapters 5, 6, 7, 8, we discuss several applications of randomized measurements. In Chapter 5, we consider randomized two-point energy measurement protocols in thermodynamic systems and verify the dimensionality of entanglement from work fluctuations. In Chapter 6, we discuss quantum metrology in nonlinear Hamiltonian dynamics and show that parameter estimation can be possible in a reference-frame-independent manner. In Chapter 7, we establish the scheme of collective randomized measurements to detect entanglement in quantum ensembles. In Chapter 8, we develop the entanglement detection based on the moments of the partially transposed density matrix. In Chapter 9, we summarize several technical calculations associated with Haar integrals, giving the proofs of Results presented in this thesis.

In Chapter 10, we discuss the geometry of two-body correlations in three-qubit states. In Chapter 11, we propose quantum speed limits describing the divergence of a perturbed open system from its unperturbed trajectory. In Chapter 12, we discuss the sensitivity of multiparticle entanglement under the classicalization of one particle.

Chapter 1

Basic concepts and tools

1.1 Quantum information

In this section, we will give a brief introduction to quantum information. In quantum information processing tasks, the main research interests may be divided into three parts: states, operations, and measurements. This section describes each of the basic concepts which are necessary to understand this thesis. Also, we explain how to analyze quantum systems. Finally, we summarize several mathematical formulas as useful tools for theoretical research in quantum information. For more general introductions to quantum mechanics and quantum information, see [18–24].

1.1.1 States

Formulations: To describe quantum states, there are two formulations: state vectors and density matrices. On the one hand, the state vector formulation describes a quantum state in an isolated physical system. Here, the state is defined as a unit complex column vector $|\psi\rangle$ in a d-dimensional Hilbert space $\mathcal{H}_d$ with $d \geq 2$. This quantum state is called pure. Here we used the bra-ket notation to express the vector, where $\langle\psi|$ denotes the conjugate transpose (Hermitian) of the column vector $|\psi\rangle$, that is, $|\psi\rangle^\dagger = \langle\psi|$. The normalization condition is given by $\langle\psi|\psi\rangle = 1$.

To explain the notation explicitly, the ket is $|a\rangle = (a_1, a_2, \ldots, a_d)^\top \in \mathcal{H}_d$ for complex elements a_i for $i = 1, \ldots, d$, while its bra is $\langle a| = (a_1^*, a_2^*, \ldots, a_d^*)$ with the complex conjugate a_i^* of a_i. The inner product is defined as $\langle a|b\rangle = \sum_{i=1}^d a_i^* b_i$.

The density matrix formulation describes a quantum state in an ensemble of pure states $\{p_i, |\psi_i\rangle\}$. This state is represented as a $d \times d$ matrix given by

$$\varrho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \tag{1.1.1}$$

where p_i implies the probabilities to obtain the state $|\psi_i\rangle$ with $p_i \in [0, 1]$ and $\sum_i p_i = 1$. Then the state is called mixed unless $p_i = 1$ for some i. It is important

to note that the density matrix satisfies

$$\varrho^\dagger = \varrho, \quad \mathrm{tr}(\varrho) = 1, \quad \varrho \geq 0. \tag{1.1.2}$$

The first property means that the matrix has all real eigenvalues. The second one means that the sum of its diagonal elements is equal to one. The third one means that all its eigenvalues are nonnegative (or positive-semidefinite). These properties, respectively, correspond to the fact that the probability is real, normalized, and nonnegative. Often, we call a matrix a quantum state if it satisfies these three conditions. Note that the matrix X is nonnegative $\Leftrightarrow X \geq 0$ $\Leftrightarrow \langle\psi|X|\psi\rangle \geq 0$ for any $|\psi\rangle$ $\Leftrightarrow X = \sum_i \lambda_i |x_i\rangle\langle x_i|$ for the eigenvalues $\lambda_i \geq 0$ for all i.

Rank: Let us consider the eigenvalue decomposition of a state $\varrho \in \mathcal{H}_d$:

$$\varrho = \sum_{i=1}^{r} \lambda_i |\phi_i\rangle\langle\phi_i|, \tag{1.1.3}$$

where λ_i are eigenvalues and $|\psi_i\rangle$ are corresponding eigenvectors. The conditions in Eq. (1.1.2) lead to $\lambda_i \in [0,1]$ and $\sum_{i=1}^{r} \lambda_i = 1$. Here $r \in \{1,2,\ldots,d\}$ is called the rank of the state ϱ. A state with $r = 1$ is pure. Otherwise, it is mixed.

Maximally mixed state: A d-dimensional quantum state is called the maximally (or completely) mixed state if $\varrho_{\mathrm{mm}} = \mathbb{1}_d/d$, where $\mathbb{1}_d$ is the $d \times d$ identity matrix. The maximally mixed state has rank d. This state can be recognized as the noisiest state in the sense that it has no information about the system, similar to white noise.

Qubits and qudits: Let $\{|i\rangle\}_{i=0}^{d-1}$ be the set of computational bases (orthonormal bases) in a d-dimensional system for $|i\rangle \in \mathcal{H}_d$ with $\langle i|j\rangle = \delta_{ij}$. Here, δ_{ij} denotes the Kronecker delta symbol.

In quantum information, a two-dimensional state with $d = 2$ is commonly referred to as a qubit, as the counterpart to the bit in classical information. The computational basis states are given by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.1.4}$$

Using these bases, we can parameterize any single-qubit pure state as

$$|\theta,\phi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{1.1.5}$$

where both real parameters are defined in $\theta \in [0,\pi]$ and $\phi \in [0,2\pi]$. Note that $\langle\theta,\phi|\theta,\phi\rangle = 1$ due to $\cos^2(\theta) + \sin^2(\theta) = 1$. Also, the corresponding density

matrix is given by

$$\varrho(\theta,\phi) = |\theta,\phi\rangle\langle\theta,\phi| = \begin{pmatrix} \cos^2\left(\frac{\theta}{2}\right) & \frac{1}{2}e^{-i\phi}\sin(\theta) \\ \frac{1}{2}e^{i\phi}\sin(\theta) & \sin^2\left(\frac{\theta}{2}\right) \end{pmatrix}. \tag{1.1.6}$$

In general, a d-dimensional state is called the qudit. For instance, a three-dimensional state with $d = 3$ is called a qutrit, where its computational basis states are given by

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{1.1.7}$$

In a similar manner of Eq. (1.1.5), any pure single-qutrit state can be written as

$$|\theta,\phi,\chi_1,\chi_2\rangle = e^{i\chi_1}\sin(\theta)\cos(\phi)\,|0\rangle + e^{i\chi_2}\sin(\theta)\sin(\phi)\,|1\rangle + \cos(\theta)\,|2\rangle\,, \tag{1.1.8}$$

where $\theta,\phi \in [0,\pi/2]$ and $\chi_1,\chi_2 \in [0,2\pi]$ with $\langle\theta,\phi,\chi_1,\chi_2|\theta,\phi,\chi_1,\chi_2\rangle = 1$.

Purity: The amount of the mixedness of a state can be characterized by the purity for a state $\varrho \in \mathcal{H}_d$:

$$\gamma(\varrho) = \mathrm{tr}(\varrho^2) \in [1/d, 1]\,. \tag{1.1.9}$$

The pure state has the maximum value $\gamma(\psi) = 1$, because $\varrho^2 = \varrho$. On the other hand, the mixed state has $\gamma(\varrho) < 1$, and especially, the maximally mixed state has the minimum value $\gamma(\varrho_{\mathrm{mm}}) = 1/d$. Calculating its purity allows us to know whether a given density matrix ϱ is pure or mixed. In the following, we summarize several remarks about the purity.

- Positivity conditions: Recalling the eigenvalue decomposition in Eq. (1.1.3), we can have $\gamma(\varrho) = \sum_{i=1}^{r}\lambda_i^2$, where λ_i are eigenvalues of ϱ and r is the rank. In the case of single qubits, one can conversely determine the two eigenvalues using the purity and the normalization condition $\mathrm{tr}(\varrho) = \lambda_1 + \lambda_2 = 1$. That is, the positive-semidefinite condition of a single-qubit state ϱ can be replaced by $1/2 \le \gamma(\varrho) \le 1$. However, this is not the case in higher dimensions.

- Rank bound: For a rank-r state ϱ_r, the lower bound of the purity is given by

$$\gamma(\varrho_r) \ge \frac{1}{r}, \tag{1.1.10}$$

  where we used the inequality between the arithmetic mean and quadratic mean: $\sum_{i=1}^{n} x_i^2/n \ge [\sum_{i=1}^{n} x_i/n]^2$, for positive x_i.

- Linear entropy: The purity is related to the so-called linear entropy:

$$S_L(\varrho) = \frac{d}{d-1}\left[1 - \gamma(\varrho)\right] \in [0,1]. \tag{1.1.11}$$

The reason we call it entropy is that linear entropy can be derived from von Neumann's entropy (see [19]) using Taylor's expansions of the logarithm of a density matrix.

Thermal states: Let H be a nondegenerate Hamiltonian with the eigenvalues E_i and the corresponding eigenvectors $|E_i\rangle$. In an analogy with the canonical state in statistical physics, we denote the thermal state as

$$\tau = \frac{e^{-\beta H}}{Z}, \qquad Z = \mathrm{tr}(e^{-\beta H}), \tag{1.1.12}$$

where β denotes the inverse temperature. Here we note that the matrix exponential for an operator A is defined by the power series $e^A = \sum_{n=0}^{\infty} A^n/n!$. Thus, the thermal state can be rewritten as

$$\tau = \sum_i p_i \left|E_i\right\rangle\left\langle E_i\right|, \tag{1.1.13}$$

where $p_i = e^{-\beta E_i}/Z \in [0,1]$ and $\sum_i p_i = 1$.

The purity of the thermal state is given by $\gamma(\tau) = \sum_i p_i^2$. For zero temperature $\beta \to \infty$, the thermal state can be pure since $p_i \to 1$. On the other hand, for infinite temperature $\beta \to 0$, it can be maximally mixed, since $p_i \to 1/Z$ and $Z = d$.

Bloch decomposition of single-qubit state: Any single-qubit state $\varrho \in \mathcal{H}_2$ can be decomposed into the following form:

$$\varrho = \frac{1}{2}\left(\mathbb{1}_2 + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right), \tag{1.1.14}$$

where the coefficients a_i are real and obey $a_i \in [-1,1]$. Here, the σ_i for $i = x, y, z$ are called the Pauli matrices given by

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.1.15}$$

satisfying the properties:

$$\sigma_i^\dagger = \sigma_i, \quad \mathrm{tr}(\sigma_i) = 0, \quad \mathrm{tr}(\sigma_i\sigma_j) = 2\delta_{ij}, \quad \sigma_i\sigma_j = \delta_{ij}\mathbb{1}_2 + i\sum_k \epsilon_{ijk}\sigma_k, \tag{1.1.16}$$

where δ_{ij} denotes the Kronecker-delta symbol and ϵ_{ijk} denotes the Levi-Civita symbol. Clearly, the form (1.1.14) satisfies the conditions that $\varrho^\dagger = \varrho$ and $\mathrm{tr}(\varrho) = 1$. Also, the positive-semidefinite condition can be replaced by

$$|\boldsymbol{a}|^2 = a_x^2 + a_y^2 + a_z^2 \in [0,1], \tag{1.1.17}$$

where $\boldsymbol{a} = (a_x, a_y, a_z)^\top$. This is because, as mentioned already, $\varrho \geq 0$ is equivalent to $1/2 \leq \gamma(\varrho) \leq 1$ for qubits, and the purity is given by

$$\gamma(\varrho) = \frac{1}{2}\left(1 + |\boldsymbol{a}|^2\right). \tag{1.1.18}$$

There are relations between the Pauli matrices and the computational bases:

$$\begin{aligned} |0\rangle\langle 0| &= \frac{1}{2}(\mathbb{1}_2 + \sigma_z), & |1\rangle\langle 1| &= \frac{1}{2}(\mathbb{1}_2 - \sigma_z), \\ |0\rangle\langle 1| &= \frac{1}{2}(\sigma_x + i\sigma_y), & |1\rangle\langle 0| &= \frac{1}{2}(\sigma_x - i\sigma_y). \end{aligned} \tag{1.1.19}$$

Using these relations, the pure state $|\theta, \phi\rangle$ in Eq. (1.1.6) has the following Bloch elements: $a_x = \sin(\theta)\cos(\phi)$, $a_y = \sin(\theta)\sin(\phi)$, and $a_z = \cos(\theta)$. This can be interpreted as a point (θ, ϕ) on the three-dimensional unit sphere in spherical coordinates, called the Bloch sphere. This result provides geometrical insights into the Bloch decomposition, which can map every single-qubit state to a point on the Bloch sphere. There, a pure state corresponds to a point on the surface, while a mixed state corresponds to a point inside the Bloch sphere. The value $|\boldsymbol{a}|^2 \in [0, 1]$ represents the length from its origin, which can measure how mixed the state is. It is essential to note that this length remains invariant under any rotation on the Bloch sphere.

Bloch decomposition of single-qudit state: In general, any single-qudit state $\varrho \in \mathcal{H}_d$ can be written in the form of the generalized Bloch decomposition:

$$\varrho = \frac{1}{d}\left(\mathbb{1}_d + \sum_{i=1}^{d^2-1} a_i \lambda_i\right), \tag{1.1.20}$$

where λ_i are called the Gell-Mann matrices and the d-dimensional extensions of Pauli matrices satisfying the properties:

$$\lambda_i^\dagger = \lambda_i, \qquad \mathrm{tr}(\lambda_i) = 0, \qquad \mathrm{tr}(\lambda_i \lambda_j) = d\delta_{ij}, \tag{1.1.21}$$

$$\lambda_i \lambda_j = \frac{1}{2}\left([\lambda_i, \lambda_j] + \{\lambda_i, \lambda_j\}\right) = d\delta_{ij}\mathbb{1}_d + \frac{1}{2}\sum_k (\eta^S_{ijk} + i\eta^A_{ijk})\lambda_k, \tag{1.1.22}$$

$$\eta^S_{ijk} = \frac{1}{d}\mathrm{tr}(\lambda_i\{\lambda_j, \lambda_k\}), \qquad \eta^A_{ijk} = \frac{-i}{d}\mathrm{tr}(\lambda_i[\lambda_j, \lambda_k]), \tag{1.1.23}$$

where $[A, B] = AB - BA$ denotes the commutator and $\{A, B\} = AB + BA$ denotes the anticommutator. Here η^S_{ijk} is a completely symmetric tensor, while η^A_{ijk} is a completely antisymmetric tensor. That is, η^S_{ijk} does not flip the sign under the exchange of each pair of its indices, while η^A_{ijk} flips the sign.

The purity is given by

$$\gamma(\varrho) = \frac{1}{d}\left(1 + |\boldsymbol{a}|^2\right). \tag{1.1.24}$$

This directly leads to the condition $|\boldsymbol{a}|^2 \in [0, d-1]$ with $\boldsymbol{a} = (a_1, \ldots, a_{d^2-1})^\top$ on the (d^2-1)-dimensional unit sphere. In a similar manner to Pauli matrices, there are relations between the Gell-Mann matrices and the computational bases. In fact, the Gell-Mann matrices are divided into three types:

$$\{\lambda_i\}_{i=1}^{d^2-1} = \{\lambda_{jk}^{\mathrm{s}}, \lambda_{jk}^{\mathrm{a}}, \lambda_l^{\mathrm{d}}\}, \tag{1.1.25}$$

where each matrix is respectively called symmetric, antisymmetric, or diagonal Gell-Mann matrix:

$$\lambda_{jk}^{\mathrm{s}} = \sqrt{\frac{d}{2}} \left(|j\rangle\langle k| + |k\rangle\langle j| \right), \qquad \text{for } 0 \le j < k \le d-1, \tag{1.1.26}$$

$$\lambda_{jk}^{\mathrm{a}} = \sqrt{\frac{d}{2}} \left(-i\,|j\rangle\langle k| + i\,|k\rangle\langle j| \right), \qquad \text{for } 0 \le j < k \le d-1, \tag{1.1.27}$$

$$\lambda_l^{\mathrm{d}} = \sqrt{\frac{d}{L}} \left(\sum_{j=0}^{l} \Pi_j - (l+1)\Pi_{l+1} \right), \qquad \text{for } 0 \le l \le d-2, \tag{1.1.28}$$

where $L = (l+1)(l+2)$ and $\Pi_j = |j\rangle\langle j|$. For details about Gell-Mann matrices, see [25–28].

Qutrit Gell-Mann matrices: Here we write the Gell-Mann matrices in qutrit systems with $d = 3$ as follows:

$$\lambda_1 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda_2 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda_3 = \sqrt{\frac{3}{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\lambda_4 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \lambda_5 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \quad \lambda_6 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$
$$\lambda_7 = \sqrt{\frac{3}{2}} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \quad \lambda_8 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}. \tag{1.1.29}$$

Notice that

$$\begin{aligned} \lambda_{01}^{\mathrm{s}} &= \lambda_1, & \lambda_{02}^{\mathrm{s}} &= \lambda_4, & \lambda_{12}^{\mathrm{s}} &= \lambda_6, \\ \lambda_{01}^{\mathrm{a}} &= \lambda_2, & \lambda_{02}^{\mathrm{a}} &= \lambda_5, & \lambda_{12}^{\mathrm{a}} &= \lambda_7, \\ \lambda_0^{\mathrm{d}} &= \lambda_3, & \lambda_1^{\mathrm{d}} &= \lambda_8. \end{aligned} \tag{1.1.30}$$

For the state $|\theta, \phi, \chi_1, \chi_2\rangle$ in Eq. (1.1.8), the elements of the eight-dimensional vector $\boldsymbol{a}$ are given by

$$\begin{aligned}
a_1 &= \sqrt{\frac{3}{2}}\sin^2(\theta)\cos(\Delta)\sin(2\phi), & a_2 &= -\sqrt{\frac{3}{2}}\sin^2(\theta)\sin(\Delta)\sin(2\phi),\\
a_3 &= \sqrt{\frac{3}{2}}\sin^2(\theta)\cos(2\phi), & a_4 &= \sqrt{6}\sin(\theta)\cos(\theta)\cos(\chi_1)\cos(\phi),\\
a_5 &= -\sqrt{6}\sin(\theta)\cos(\theta)\sin(\chi_1)\cos(\phi), & a_6 &= \sqrt{6}\sin(\theta)\cos(\theta)\cos(\chi_2)\sin(\phi),\\
a_7 &= -\sqrt{6}\sin(\theta)\cos(\theta)\sin(\chi_2)\sin(\phi), & a_8 &= -\frac{3\cos(2\theta)+1}{2\sqrt{2}},
\end{aligned} \tag{1.1.31}$$

where $\Delta = \chi_1 - \chi_2$. For details about qutrit systems, see [29–31].

1.1.2 Operations

Definitions: A quantum operation (dynamics) describes a transformation that changes a quantum state to a quantum state. The operation is defined as a map Φ such that $\Phi(\varrho) = \varrho'$, where $\varrho \in \mathcal{H}_d$ and $\varrho' \in \mathcal{H}_{d'}$. We can understand the above as saying that the input state ϱ can be transformed into the output ϱ' via the physical process or channel Φ. Note that d is not necessarily equal to d'. For the sake of simplicity, in the following, we consider the case where $d = d'$.

Mathematically, a quantum operation Φ must satisfy

$$\mathrm{tr}[\Phi(\varrho)] = 1, \qquad \Phi\left(\sum p_i\varrho_i\right) = \sum p_i\Phi(\varrho_i), \qquad \Phi(\varrho) \geq 0. \tag{1.1.32}$$

The first condition is called trace-preserving, the second is called convex-linearity, and the third is called positivity-preserving. That is, we require the quantum operation to preserve the three conditions of quantum states in Eq. (1.1.2). Moreover, in addition to these properties, the quantum operation must satisfy another physical condition: even when Φ acts on a subsystem of ϱ, the positivity of ϱ must hold. This is called complete positivity, which will be explained more precisely in Sec. 1.1.4.

Kraus representations: For a state $\varrho \in \mathcal{H}_d$, any quantum operation can be written as the so-called Kraus representation:

$$\Phi(\varrho) = \sum_{i=1}^{r} K_i\varrho K_i^\dagger. \tag{1.1.33}$$

The trace-preserving condition leads to

$$\mathrm{tr}[\Phi(\varrho)] = \mathrm{tr}\left[\sum_{i=1}^{r} K_i\varrho K_i^\dagger\right] = \mathrm{tr}\left[\sum_{i=1}^{r} K_i^\dagger K_i\varrho\right] = \mathrm{tr}(\varrho). \tag{1.1.34}$$

Thus, Kraus operators K_i should satisfy

$$\sum_{i=1}^{r} K_i^\dagger K_i = \mathbb{1}_d. \tag{1.1.35}$$

Here r is called the Kraus rank with the range $r \in \{1, \ldots, d^2\}$. This is in analogy with the rank of a quantum state. Note that the choice of the K_i is not unique.

Unitary operations: For a state $\varrho \in \mathcal{H}_d$, a quantum operation is called unitary if

$$\Phi(\varrho) = U\varrho U^\dagger, \tag{1.1.36}$$

where U is a unitary matrix such that $U^{-1} = U^\dagger$, that is, $UU^\dagger = U^\dagger U = \mathbb{1}_d$. The unitary operation can be regarded as a rank-one Kraus representation.

Let us note that the unitary matrix can be written as

$$U(\theta) = e^{-i\theta H}, \tag{1.1.37}$$

where θ is a real parameter such as time t and H is a Hermitian matrix such as the Hamiltonian. In general, computing unitary matrices for a given Hamiltonian would be demanding because of nontrivial complicated higher-order terms. On the other hand, if a Hamiltonian is a so-called involutory matrix, that is, $H^2 = \mathbb{1}_d$, then the unitary can be simplified as follows:

$$U(\theta) = \cos(\theta)\mathbb{1}_d - i\sin(\theta)H. \tag{1.1.38}$$

Finally, we note that any unitary operation cannot change the purity of a quantum state: $\gamma(U\varrho U^\dagger) = \mathrm{tr}(U\varrho U^\dagger U\varrho U^\dagger) = \mathrm{tr}(\varrho^2) = \gamma(\varrho)$. In a single-qubit system, the unitary operation can be regarded as a transformation between two points on the surface of the Bloch sphere.

Single-qubit unitary operations: In general, we can write the single-qubit Hamiltonian as

$$H = \sum_{i=x,y,z} u_i\sigma_i = \boldsymbol{u}\cdot\boldsymbol{\sigma}, \tag{1.1.39}$$

where $\boldsymbol{u} = (u_x, u_y, u_z)$ is a unit real vector with $|\boldsymbol{u}|^2 = 1$ and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices. That is, any single-qubit unitary matrix can be given by

$$U(\theta, \boldsymbol{u}) = \cos(\theta)\mathbb{1}_2 - i\sin(\theta)\boldsymbol{u}\cdot\boldsymbol{\sigma}, \tag{1.1.40}$$

where we use $H^2 = \mathbb{1}_2$.

This unitary operation describes not only rotations, but also transformations between any two points on the Bloch sphere. For instance, taking an initial state as $|0\rangle$ and the vector $\boldsymbol{u}_0$ with $u_x = -\sin(\phi), u_y = \cos(\phi), u_z = 0$, we can find the expression in Eq. (1.1.6):

$$\varrho(\theta, \phi) = U(\theta/2, \boldsymbol{u}_0)|0\rangle\langle 0|U(\theta/2, \boldsymbol{u}_0)^\dagger. \tag{1.1.41}$$

In general, for any single-qubit state with the Bloch vector $\boldsymbol{a}$ in Eq. (1.1.14), the unitary operation $U(\theta, \boldsymbol{u})$ can map its element a_i to a_i' as follows:

$$a_i' = \mathrm{tr}\left[\sigma_i U(\theta, \boldsymbol{u})\,\varrho\, U(\theta, \boldsymbol{u})^\dagger\right] \equiv \sum_{j=1}^{3} O_{ij}a_j, \tag{1.1.42}$$

where

$$
\begin{aligned}
O_{ij} &= \frac{1}{2}\mathrm{tr}\left[\sigma_i U(\theta,\boldsymbol{u})\,\sigma_j U(\theta,\boldsymbol{u})^{\dagger}\right] \\
&= \frac{1}{2}\mathrm{tr}\left[\sigma_i\left(\cos(\theta)\mathbb{1}_2 - i\sin(\theta)\boldsymbol{u}\cdot\boldsymbol{\sigma}\right)\sigma_j\left(\cos(\theta)\mathbb{1}_2 + i\sin(\theta)\boldsymbol{u}\cdot\boldsymbol{\sigma}\right)\right] \\
&= \left[\cos^2(\theta) - \sin^2(\theta)\right]\delta_{ij} - \sin(\theta)\cos(\theta)\sum_k u_k\epsilon_{ijk} + 2\sin^2(\theta)u_i u_j. \quad (1.1.43)
\end{aligned}
$$

Connection between SU(2) and SO(3): A set of all $n \times n$ matrices is called the special unitary group $\mathrm{SU}(n)$ if every matrix is unitary with determinant 1. For example, we can notice that $U(\theta,\boldsymbol{u}) \in \mathrm{SU}(2)$, where the single-qubit unitary $U(\theta,\boldsymbol{u})$ given in Eq. (1.1.40) and its determinant can be shown to be 1 using Jacobi's formula $\det e^A = e^{\mathrm{tr}(A)}$ for a matrix A:

$$
\det U(\theta,\boldsymbol{u}) = e^{i\theta\,\mathrm{tr}(\boldsymbol{u}\cdot\boldsymbol{\sigma})} = 1. \quad (1.1.44)
$$

A set of all $n \times n$ matrices is called the special orthogonal group $\mathrm{SO}(n)$ if every matrix is orthogonal with determinant 1, that is, $O^{\top}O = OO^{\top} = \mathbb{1}_n$ and $\det O = 1$ for $O \in \mathrm{SO}(n)$, where $(\cdot)^{\top}$ denotes the transposition. Let us recall that any orthogonal matrix can be written as follows, in a similar manner to Eq. (1.1.37):

$$
O = e^{\omega K} \quad (1.1.45)
$$

where ω is a real parameter and K is a skew-symmetric matrix with $K^{\top} = -K$. In particular, for an orthogonal matrix $O \in \mathrm{SO}(3)$, the matrix K can be given by the so-called cross-product matrix:

$$
K = \begin{pmatrix} 0 & -k_z & k_y \\ k_z & 0 & -k_x \\ -k_y & k_x & 0 \end{pmatrix}, \quad (1.1.46)
$$

where $\mathrm{tr}(K) = 0$, $k_x^2 + k_y^2 + k_z^2 = 1$, and $K^3 = -K$. Using the Taylor expansion, we can rewrite the orthogonal matrix $O \in \mathrm{SO}(3)$ as

$$
O = \mathbb{1}_3 + \sin(\omega)K + [1 - \cos(\omega)]K^2. \quad (1.1.47)
$$

This matrix form is called Rodrigues' rotation formula.

Now it is important to notice that the expression in Eq. (1.1.47) coincides with the matrix given in Eq. (1.1.43) if $\omega = \theta/2$ and $\boldsymbol{k} = \boldsymbol{u}$. That is, the single-qubit $U(\theta/2,\boldsymbol{u}) \in \mathrm{SU}(2)$ can represent the orthogonal rotation $O \in \mathrm{SO}(3)$ of a point on the Bloch sphere by an angle θ about the $\boldsymbol{u}$ axis. On the mathematical side, this relation is known as the isomorphic mapping of $\mathrm{SU}(2)$ onto $\mathrm{SO}(3)$. For details, see [18, 32–35].

Unital operations: A quantum operation is called unital if

$$\Phi_{\mathrm{U}}\left(\frac{\mathbb{1}_d}{d}\right) = \frac{\mathbb{1}_d}{d}. \tag{1.1.48}$$

That is, the maximally mixed state is a fixed point of the unital operation. This condition implies that the Kraus operators obey

$$\sum_i K_i^\dagger K_i = \sum_i K_i K_i^\dagger = \mathbb{1}. \tag{1.1.49}$$

Otherwise, a quantum operation is called non-unital. Such an operation can turn the maximally mixed state into another quantum state, which can increase the amount of purity. A typical example is (generalized) amplitude damping.

Identical operations: A quantum operation is called identical if $\mathrm{id}(\varrho) = \mathbb{1}\varrho\mathbb{1} = \varrho$, for any quantum state ϱ. That is, applying this operation implies that we do not touch the state.

Depolarizing operations: The depolarizing operation describes the state transformation such that an input state is obtained with probability p and the maximally mixed state is obtained with probability $1-p$. That is, for a state $\varrho \in \mathcal{H}_d$,

$$\mathcal{D}(\varrho) = p\varrho + \frac{1-p}{d}\mathbb{1}_d. \tag{1.1.50}$$

By definition, the depolarizing operation is unital.

For single-qubit cases, its Kraus operators are given by

$$K_i = \sqrt{\frac{1-p}{4}}\sigma_i, \qquad K_4 = \sqrt{\frac{3p-1}{4}}\mathbb{1}_2, \tag{1.1.51}$$

with Pauli matrices σ_i for $i = 1, 2, 3$. This follows from the fact that for a single-qubit state ϱ, it holds that

$$\frac{1}{2}\mathbb{1}_2 = \frac{1}{4}\left(\mathbb{1}_2\varrho\mathbb{1}_2 + \sigma_x\varrho\sigma_x + \sigma_y\varrho\sigma_y + \sigma_z\varrho\sigma_z\right). \tag{1.1.52}$$

One can check this relation by substituting the Bloch decomposition in Eq. (1.1.14) into the above form and using the property $\sigma_i\sigma_j\sigma_i = -\sigma_j$ for $i \neq j$. Moreover, in general, it holds

$$\frac{\mathbb{1}_d}{d} = \frac{1}{d}\left(\sum_{i=1}^{d} |i\rangle\langle i|\right)\mathrm{tr}(\varrho) = \frac{1}{d}\sum_{i,j=1}^{d} |i\rangle\langle j|\,\varrho\,|j\rangle\langle i|. \tag{1.1.53}$$

Based on the relation in Eq. (1.1.28), one can then find the form of the Kraus operators of the d-dimensional depolarizing operation.

Finally, we consider the change of purity under the depolarizing operation:

$$\gamma[\mathcal{D}(\varrho)] = \mathrm{tr}\left[\left(p\varrho + \frac{1-p}{d}\mathbb{1}_d\right)^2\right] = p^2\gamma(\varrho) + \frac{1-p^2}{d}. \tag{1.1.54}$$

Thus, the purity monotonically decreases under the depolarizing operation. Using the relation in Eq. (1.1.24) between the purity and the Bloch length $|\boldsymbol{a}|^2$ for an initial state ϱ, we can have

$$p = \sqrt{\frac{d\gamma[\mathcal{D}(\varrho)] - 1}{|\boldsymbol{a}|^2}}. \tag{1.1.55}$$

That is, the noise parameter p can be estimated by measuring the purities of the initial and output states.

Universal state inversions: For a single-qubit state ϱ, a map is called spin-flip if

$$\mathcal{S}_2(\varrho) = \sigma_y\varrho^\top\sigma_y = \frac{1}{2}\left(\mathbb{1}_2 - \sum_{i=x,y,z} a_i\sigma_i\right), \tag{1.1.56}$$

where we use the Bloch decomposition in Eq. (1.1.14) and notice that $\sigma_y^\top = -\sigma_y$ with the transposition $(\cdot)^\top$. It is important to note that this map preserves the positivity condition. Also, we can rewrite the spin-flip as

$$\mathcal{S}_2(\varrho) = \mathrm{tr}(\varrho)\mathbb{1}_2 - \varrho. \tag{1.1.57}$$

In general, for a single-qudit state ϱ, a map is called the universal state inversion if

$$\mathcal{S}_d(\varrho) = \mathrm{tr}(\varrho)\mathbb{1}_d - \varrho. \tag{1.1.58}$$

From the eigenvalue decomposition, one can immediately see that $\mathcal{S}_d(\varrho)$ preserves the positivity condition. Clearly, it thus holds that $\mathrm{tr}[\varrho\mathcal{S}_d(\varrho)] \geq 0$, where $\mathrm{tr}(AB) \geq 0$ for positive operators A, B. This inequality implies that the purity is bounded by one: $\gamma(\varrho) \leq 1$. Finally, we note that in the viewpoint of the Bloch decomposition in Eq. (1.1.20), the universal state inversion can be rewritten as

$$\mathcal{S}_d(\varrho) = \frac{1}{d}\left[(d-1)\mathbb{1}_d - \sum_{i=1}^{d^2-1} a_i\lambda_i\right]. \tag{1.1.59}$$

For details about universal state inversions, see [36–38].

Liouville-von Neumann equation: Consider the infinitesimal time evolution from time t to $t + \Delta t$ in a unitary operation $U(t + \Delta t, t)$, for small Δt:

$$\varrho(t + \Delta t) = U(t + \Delta t, t)\varrho(t)U^\dagger(t + \Delta t, t). \tag{1.1.60}$$

Here we can express the matrix exponential of the unitary in Eq. (1.1.37) using the Taylor expansion:

$$U(t+\Delta t,t) = \mathbb{1} - i\Delta t H + \mathcal{O}[(\Delta t)^2]. \tag{1.1.61}$$

Substituting this form into Eq. (1.1.60), we have

$$\varrho(t+\Delta t) = \varrho(t) - i\Delta t[H,\varrho(t)] + \mathcal{O}[(\Delta t)^2], \tag{1.1.62}$$

where $[A,B] = AB - BA$. Considering the limit $\Delta t \to 0$, we can arrive at the Liouville-von Neumann equation:

$$\frac{d\varrho}{dt} = -i[H,\varrho]. \tag{1.1.63}$$

This dynamics can describe the time-reversal evolution of a quantum state in an isolated system.

Gorini–Kossakowski–Sudarshan–Lindblad (GKSL) equation: Let us consider the infinitesimal time evolution from t to $t+\Delta t$ in a Kraus operation $\Phi_{t+\Delta t,t}$ with an operator $K_i(t+\Delta t,t)$, for small Δt:

$$\varrho(t+\Delta t) = \sum_{i=1}^{r} K_i(t+\Delta t,t)\varrho(t)K_i^\dagger(t+\Delta t,t). \tag{1.1.64}$$

Here we assume that this form is valid for any time $t > 0$. Then we can always write

$$K_1(t+\Delta t,t) = \mathbb{1} - i\Delta t H - \frac{\Delta t}{2}\sum_{i\geq 1}|g_i|^2 L_i^\dagger L_i + \mathcal{O}[(\Delta t)^2], \tag{1.1.65}$$

$$K_{i\neq 1}(t+\Delta t,t) = \sqrt{\Delta t}\, g_i L_i + \mathcal{O}[\Delta t], \tag{1.1.66}$$

where $|g_i|^2$ has units of [1/time] and the dimensionless $(\Delta t)g_i^2$ is kept but its higher orders are neglected, in analogy to the so-called van Hove limit in statistical physics [39]. Note that these Kraus operators satisfy the trace-preserving condition, up to the first order of Δt. Substituting these into Eq. (1.1.64), we have

$$\varrho(t+\Delta t) = \varrho(t) - i\Delta t[H,\varrho(t)] - \frac{\Delta t}{2}\sum_{i\geq 1}|g_i|^2\left(\{L_i^\dagger L_i,\varrho(t)\} - 2L_i\varrho(t)L_i^\dagger\right) + \mathcal{O}[(\Delta t)^{3/2}], \tag{1.1.67}$$

where $[A,B] = AB - BA$ and $\{A,B\} = AB + BA$. Considering the limit $\Delta t \to 0$, we arrive at the Gorini–Kossakowski–Sudarshan–Lindblad equation:

$$\frac{d\varrho}{dt} = -i[H,\varrho] - \frac{1}{2}\sum_{i\geq 1}|g_i|^2\left(\{L_i^\dagger L_i,\varrho\} - 2L_i\varrho L_i^\dagger\right). \tag{1.1.68}$$

Here, the first term on the right-hand side is the same as the Liouville-von Neumann equation and describes the time-reversible effects of the unitary evolution. On the other hand, the other terms represent additional effects and describe the time-irreversible quantum dissipation arising from interaction with the environment in the open system. In particular, this open dynamics may be often called Markovian, which is independent of the history of the process. This memoryless property may stem from the assumption that the form in Eq. (1.1.64) holds for any time $t > 0$. In mathematical words, this assumption means that the Kraus representation forms a one-parameter semi-group. For details about open quantum systems, see [40–44].

1.1.3 Measurements

Experimental facts: Consider a large number of quantum states, where each state is identically the same. Let us perform a measurement for each state in order to know a physical quantity, such as energy, momentum, and angular momentum. After a measurement, the resulting outcome is obtained. Here are four experimental facts in quantum mechanics:

1. Each outcome may be different for the same measurement.
2. Any outcome can have real value.
3. Each outcome can occur with a certain probability, depending on the measurement setting and quantum state.
4. The state after the measurement can be different from the state before the measurement.

In the following, we will describe the theory of quantum measurements that can explain the above experimental facts.

Projective measurements: We call a Hermitian operator M observable if it acts on the quantum state of a system and is associated with a physical quantity that can be measured. Examples are Pauli matrices and Hamiltonians. A projective measurement is described by the observable $M \in \mathcal{H}_d$. Here its eigenvalue decomposition is given by

$$M = \sum_i m_i \Pi_i, \tag{1.1.69}$$

where m_i is an eigenvalue and Π_i are its corresponding projectors with

$$\Pi_i^\dagger = \Pi_i, \qquad \sum_i \Pi_i = \mathbb{1}_d, \qquad \Pi_i \Pi_j = \delta_{ij} \Pi_i, \qquad \Pi_i \geq 0. \tag{1.1.70}$$

Suppose that we perform a measurement of the observable M on a quantum state ϱ. The following rules can explain the experimental facts very well:

1. Each outcome of the measurement is given by one of the eigenvalues $\{m_i\}$.

2. Any outcome m_i has a real value since M is Hermitian.

3. The i-th outcome m_i is known to be obtained with the probability p_i following from the so-called Born rule

$$p_i = \mathrm{tr}(\varrho \Pi_i). \tag{1.1.71}$$

4. After this measurement, the state ϱ becomes

$$\varrho \to \varrho_i' = \frac{1}{\mathrm{tr}(\varrho \Pi_i)} \Pi_i \varrho \Pi_i, \tag{1.1.72}$$

which occurs with the probability p_i. This update is often called the collapse of the quantum state.

Consider a case in which we know that the measurement is performed but we do not know which outcome occurs. In this case, a quantum state can be written as a mixture of possible post-measurement states:

$$\varrho' = \sum_i p_i \varrho_i' = \sum_i \Pi_i \varrho \Pi_i. \tag{1.1.73}$$

This can coincide with the process described by the Kraus representation with $K_i = \Pi_i$ discussed in Eq. (1.1.33). Here the trace-preserving condition corresponds to $\sum_i \Pi_i = \mathbb{1}_d$.

POVM measurements: The notion of quantum measurements can be generalized, to what are known as positive operator-valued measure (POVM) measurements. Roughly speaking, it may be a mixture of projective measurements in analogy with the relation between pure and mixed states. For instance, let us toss a coin and make either of two measurements M_a or M_b, depending on whether it is the head or tail. How can we describe this measurement process?

More mathematically, let $\{M_x\}_{x=a,b,\ldots,z}$ be the collection of observables, where $M_x \in \mathcal{H}_d$ have eigenvalues m_i^x with corresponding projectors Π_i^x. Consider a situation in which a measurement M_x is performed with a probability q_x. For the sake of simplicity, let us assume that every observable M_x has the same outcome values (eigenvalues) m_i for any i, but different projectors. Such examples are the Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$. The probability to obtain the i-th outcome m_i is given by

$$\begin{aligned} p_i &= q_a \mathrm{tr}(\varrho \Pi_i^a) + q_b \mathrm{tr}(\varrho \Pi_i^b) + \cdots + q_z \mathrm{tr}(\varrho \Pi_i^z) \\ &= \mathrm{tr}\left[\varrho \left(q_a \Pi_i^a + q_b \Pi_i^b + \cdots + q_z \Pi_i^z\right)\right]. \end{aligned} \tag{1.1.74}$$

Here we notice the following relations

$$\sum_x q_x \Pi_i^x \geq 0, \qquad \sum_i \sum_x q_x \Pi_i^x = \sum_x q_x \left(\sum_i \Pi_i^x\right) = \mathbb{1}_d, \tag{1.1.75}$$

where we use that the convex combination of positive matrices is positive and q_x is the probability.

General quantum measurements are described by POVM measurements, a collection of operators $\{E_i\}$ with $E_i \in \mathcal{H}_d$, such that

$$E_i^\dagger = E_i, \qquad \sum_i E_i = \mathbb{1}_d, \qquad E_i \geq 0. \tag{1.1.76}$$

In quantum information, the operators E_i are often called effects. The probability to obtain the i-th outcome is given by

$$p_i = \mathrm{tr}(\varrho E_i). \tag{1.1.77}$$

To discuss how the state changes after the POVM measurement, we first recall that a Hermitian matrix X is positive if and only if it can be written as $X = A^\dagger A$ for a matrix A. Thus the effects can be rewritten as

$$E_i = K_i^\dagger K_i, \tag{1.1.78}$$

for operators K_i. After the measurement, the post-measurement state can be given by

$$\varrho \to \varrho_i' = \frac{1}{\mathrm{tr}(\varrho E_i)} K_i \varrho K_i^\dagger. \tag{1.1.79}$$

In a similar manner to projective measurements, if we do not know the outcomes, then the state is mixed between post-measurement states:

$$\varrho' = \sum_i p_i \varrho_i' = \sum_i K_i \varrho K_i^\dagger. \tag{1.1.80}$$

The condition $\sum_i E_i = \sum_i K_i^\dagger K_i = \mathbb{1}_d$ represents the trace-preserving condition in the Kraus representation.

We remark that for effects E_i, there exist unitary matrices U_i such that $K_i = U_i \sqrt{E_i}$. This is the polar decomposition of the operators K_i, which satisfies $K_i^\dagger K_i = M_i$. That is, there is unitary freedom in the Kraus representation, and the operation is not uniquely determined. As a special case, the so-called von Neumann–Lüders rule allows us to describe the post-measurement state as

$$\varrho \to \varrho_i' = \frac{1}{\mathrm{tr}(\varrho E_i)} \sqrt{E_i} \varrho \sqrt{E_i}. \tag{1.1.81}$$

Noisy measurements: Suppose that we perform a projective measurement Π_i with noisy error probability ε and produce a completely random outcome with probability $1 - \varepsilon$. The corresponding POVMs are given by

$$P_i = \varepsilon \Pi_i + \frac{1 - \varepsilon}{d} \mathbb{1}_d \geq 0, \qquad \sum_{i=1}^d P_i = 0, \tag{1.1.82}$$

where we assume that the projectors Π_i have rank 1 and d outcomes. The probability to obtain the outcome i is given by

$$p_i(\varepsilon) = \mathrm{tr}(\varrho P_i). \tag{1.1.83}$$

To see the expression of the post-measurement state, we begin by noting that

$$\sqrt{P_i} = f_\varepsilon \Pi_i + g_\varepsilon \mathbb{1}_d. \tag{1.1.84}$$

Here we used that $\mathbb{1}_d = \Pi_i + \sum_{i \neq j} \Pi_j$ and defined that

$$f_\varepsilon = \sqrt{\varepsilon + \frac{1-\varepsilon}{d}} - \sqrt{\frac{1-\varepsilon}{d}}, \qquad g_\varepsilon = \sqrt{\frac{1-\varepsilon}{d}}, \tag{1.1.85}$$

with the normalization condition

$$f_\varepsilon^2 + 2 f_\varepsilon g_\varepsilon + d g_\varepsilon^2 = 1. \tag{1.1.86}$$

Using the von Neumann–Lüders rule, the post-measurement state is given by

$$\varrho_i'(\varepsilon) = \frac{1}{p_i(\varepsilon)} \sqrt{P_i} \varrho \sqrt{P_i} = \frac{1}{p_i(\varepsilon)} \left[f_\varepsilon^2 \Pi_i \varrho \Pi_i + g_\varepsilon^2 \varrho + f_\varepsilon g_\varepsilon (\Pi_i \varrho + \varrho \Pi_i) \right]. \tag{1.1.87}$$

The first term on the right-hand side represents the post-measurement state by the (noiseless) projective measurement, while the second term represents the state from the measurement that does not touch the state. The third term represents an additional contribution at a finite $\varepsilon \in (0, 1)$.

In particular, this measurement is called sharp if $\varepsilon \to 1$, while it is called weak if $\varepsilon \to 0$. The sharp measurement process can change the state significantly, but a lot of information about the state can be extracted. On the other hand, a weak measurement process can keep the state mostly unchanged, but provide little information about the state. That is, there is a trade-off relation between extractable information and state change. For details about noisy measurements, see [45–47].

In the above noisy measurement scheme, let us consider the mixture of post-measurement states:

$$\varrho'(\varepsilon) = \sum_i p_i(\varepsilon) \varrho_i'(\varepsilon) = f_\varepsilon^2 \xi + \kappa_\varepsilon \varrho, \quad \xi = \sum_i \Pi_i \varrho \Pi_i, \quad \kappa_\varepsilon = g_\varepsilon (2 f_\varepsilon + d g_\varepsilon), \tag{1.1.88}$$

where we use $\sum_i \Pi_i = \mathbb{1}_d$. Now, we can introduce the part of the results proposed in Ref. [4]: For the state's purity, it holds that

$$\gamma[\varrho'(\varepsilon)] \leq \gamma(\varrho), \tag{1.1.89}$$

which is saturated by the limit $\varepsilon \to 0$.

Proof. Here we show the above inequality, following the description of Ref. [4]. The purity of $\varrho'(\varepsilon)$ is given by

$$\gamma[\varrho'(\varepsilon)] = f_\varepsilon^4 \gamma(\xi) + \kappa_\varepsilon^2 \gamma(\varrho) + 2 f_\varepsilon^2 \kappa_\varepsilon \mathrm{tr}(\xi\varrho). \tag{1.1.90}$$

Here we notice that $\gamma(\xi) = \mathrm{tr}\left[\left(\sum_i \Pi_i \varrho \Pi_i\right)^2\right] = \mathrm{tr}(\xi\varrho) = \sum_i \mathrm{tr}\left[\Pi_i \varrho \Pi_i \varrho\right]$. This yields

$$\gamma[\varrho'(\varepsilon)] = \left(f_\varepsilon^4 + 2 f_\varepsilon^2 \kappa_\varepsilon\right) \sum_i \mathrm{tr}\left[\Pi_i \varrho \Pi_i \varrho\right] + \kappa_\varepsilon^2 \gamma(\varrho). \tag{1.1.91}$$

Moreover, we can find the upper bound of the first term in the above equation

$$\sum_i \mathrm{tr}\left[\Pi_i \varrho \Pi_i \varrho\right] \leq \sum_i \mathrm{tr}\left[\Pi_i \varrho^2\right] = \gamma(\varrho). \tag{1.1.92}$$

Here we used the inequality $\mathrm{tr}(ABAB) \leq \mathrm{tr}(A^2B^2)$ for any Hermitian operators A, B, which can be shown in Sec. 1.1.7. Finally, using the normalization condition (1.1.86), we can complete the proof. □

In Chapter 5, we will discuss the extension of Eq. (1.1.89) to two-qudit systems and the application in the scheme of two-point measurements.

Expectation of observable: Consider a quantum state ϱ and perform a measurement with an observable M. Denote the measurement outcome as m_i with its corresponding probability as p_i. The expectation of the observable is defined as

$$\langle M \rangle_\varrho = \sum_i m_i p_i, \tag{1.1.93}$$

where the subscript ϱ is made to stress that the expectation depends on the state. For details about the expectation, see Sec. 1.1.5. In the case of projective measurements, the probability is given by $p_i = \mathrm{tr}(\varrho\Pi_i)$ following from the Born rule in Eq. (1.1.71) with the projector Π_i for the corresponding eigenvalue m_i of M. Then the expectation can be rewritten as

$$\langle M \rangle_\varrho = \sum_i m_i \mathrm{tr}(\varrho\Pi_i) = \mathrm{tr}(\varrho M). \tag{1.1.94}$$

In the case of POVM measurements, one method to define the expectation is to decompose the observable M using POVMs, not projectors. As examples of references, we would like to highlight the works in Refs. [4, 47]. To such POVM decomposition, we consider the noisy POVM measurements $P_i = \varepsilon\Pi_i + (1-\varepsilon)\mathbb{1}_d/d$ in Eq. (1.1.82) with the probability $p_i(\varepsilon) = \mathrm{tr}(\varrho P_i)$. Now one notices that

$$\sum_i m_i p_i(\varepsilon) = \varepsilon \langle M \rangle_\varrho + \frac{1-\varepsilon}{d} \mathrm{tr}(M) \neq \langle M \rangle_\varrho. \tag{1.1.95}$$

To find the form of the expectation $\langle M \rangle_\varrho$, we should rescale and shift the outcome value. Let us assign appropriate values as measurement outcomes to e_i:

$$e_i = \frac{1}{\varepsilon} m_i - \frac{1-\varepsilon}{d\varepsilon} \mathrm{tr}(M). \tag{1.1.96}$$

Then we can have that $\langle M \rangle_\varrho = \sum_i e_i p_i(\varepsilon)$. This result is based on the POVM decomposition of the observable M:

$$M = \sum_i e_i P_i. \tag{1.1.97}$$

1.1.4 Composite quantum systems

Quantum states in composite systems

Reduced states: Quantum states consisting of two or more particles can be described by tensor products in each Hilbert space. For instance, consider two parties, called Alice (A) and Bob (B). The whole system of A and B is described as a quantum state $\varrho_{AB} \in \mathcal{H}^A \otimes \mathcal{H}^B$. This state can contain quantum information about the whole system. On the other hand, the local subsystem A (or B) can be described as its reduced state $\varrho_A \in \mathcal{H}^A$ (or $\varrho_B \in \mathcal{H}^B$), which contains marginal information about the local system. Here the reduced state is obtained by taking a partial trace over the subsystem:

$$\varrho_A = \mathrm{tr}_B(\varrho_{AB}), \qquad \varrho_B = \mathrm{tr}_A(\varrho_{AB}). \tag{1.1.98}$$

In a similar manner, for an N-particle quantum state $\varrho \in \mathcal{H}^1 \otimes \cdots \otimes \mathcal{H}^N$, its k-particle reduced state on system $X = (X_1, \ldots, X_k)$ is obtained by taking a partial trace over subsystem X^c:

$$\varrho_X = \mathrm{tr}_{X^c}(\varrho), \tag{1.1.99}$$

where X^c denotes the complement of X.

Bloch decomposition of N-qudit states: We begin by considering the case with two-qudit states, that is, $\varrho_{AB} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$. In a similar manner to single-qudit states, we can write the state in the Bloch decomposition of a two-qudit state

$$\varrho_{AB} = \frac{1}{d^2} \left(\mathbb{1}_d^{\otimes 2} + \sum_{i=1}^{d^2-1} a_i \lambda_i \otimes \mathbb{1}_d + \sum_{i=1}^{d^2-1} b_i \mathbb{1}_d \otimes \lambda_i + \sum_{i,j=1}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j \right). \tag{1.1.100}$$

Here, each vector $\boldsymbol{a}, \boldsymbol{b}$ respectively describes local quantum system A, B, whereas the matrix $T = (t_{ij})$ describes two-body correlation in the whole system. Clearly, the reduced state $\varrho_A = \mathrm{tr}_B(\varrho_{AB})$ arrives at the same form of the single-qudit state in Eq. (1.1.20).

Similarly, any N-qudit state $\varrho \in \mathcal{H}_d^1 \otimes \cdots \otimes \mathcal{H}_d^N$ can be written as

$$\varrho = \frac{1}{d^N} \sum_{i_1,\ldots,i_N=0}^{d^2-1} \alpha_{i_1,\ldots,i_N} \lambda_{i_1} \otimes \cdots \lambda_{i_N}, \tag{1.1.101}$$

where $\lambda_0 = \mathbb{1}_d$ and $\alpha_{i_1,\ldots,i_N}$ denoted the k-fold tensor $1 \leq k \leq N$ if the number of non-identity terms in $\lambda_{i_1} \otimes \cdots \otimes \lambda_{i_N}$ is k, describing k-body correlation in ϱ. For the sake of simplicity, let us rewrite this form as

$$\varrho = \frac{1}{d^N} \left(\mathbb{1}_d^{\otimes N} + P_1 + P_2 + \cdots + P_N \right), \tag{1.1.102}$$

where the Hermitian operators P_k for $k = 1, 2, \ldots, N$ denote the sum of all terms coming from the basis elements with weight k

$$P_k(\varrho) = \sum_{\substack{i_1,\cdots,i_N=0, \\ \mathrm{wt}(\lambda_{i_1}\otimes\cdots\otimes\lambda_{i_N})=k}}^{d^2-1} \alpha_{i_1\cdots i_N} \lambda_{i_1} \otimes \cdots \otimes \lambda_{i_N}, \tag{1.1.103}$$

where the weight $\mathrm{wt}(\lambda_{i_1} \otimes \cdots \otimes \lambda_{i_N})$ is the number of non-identity Gell-Mann matrices. This expression will be used to define the so-called sector lengths in Eq. (1.4.7).

Quantum operations in composite systems

Complete positivity: Consider a two-particle state ϱ_{AB}. Suppose that we perform the identical operation (nothing) id_A on local subsystem A but apply a quantum operation Φ_B on local subsystem B. This process can be described as

$$\varrho'_{AB} = (\mathrm{id}_A \otimes \Phi_B)(\varrho_{AB}). \tag{1.1.104}$$

Clearly, taking the partial trace over subsystem A leads to that

$$\varrho'_B = \mathrm{tr}_A(\varrho'_{AB}) = \Phi_B(\varrho_B). \tag{1.1.105}$$

Here, we should require the map Φ_B to preserve the positivity of not only the reduced state ϱ'_B but also the whole state ϱ'_{AB}. This additional condition is called the complete positivity (CP). Often a quantum operation is referred to as a completely-positive and trace-preserving (CPTP) map.

Local unitary operations: For an N-qudit quantum state $\varrho \in \mathcal{H}_d^1 \otimes \cdots \otimes \mathcal{H}_d^N$, a quantum operation is called local unitary if

$$\Phi_{\mathrm{LU}}(\varrho) = (U_1 \otimes \cdots \otimes U_N)\varrho(U_1^\dagger \otimes \cdots \otimes U_N^\dagger), \tag{1.1.106}$$

where the unitary U_i acts on the i-th subsystem for $i = 1, \ldots, N$. In a similar way to the exponential form (1.1.37), the local unitary can be generated by the local Hamiltonian H_L:

$$e^{-i\theta H_L} = e^{-i\theta H_1} \otimes \cdots \otimes e^{-i\theta H_N}, \tag{1.1.107}$$

$$H_L = H_1 \otimes \mathbb{1}_{2\ldots N} + \cdots + \mathbb{1}_{1\ldots N-1} \otimes H_N. \tag{1.1.108}$$

A typical example is the collective angular momentum in N-qubit systems:

$$J_l = \frac{1}{2} \sum_{i=1}^{N} \sigma_l^{(i)}, \tag{1.1.109}$$

where $\sigma_l^{(i)}$ is the l-th Pauli matrix acting on the i-th subsystem for $l = x, y, z$. This leads to

$$e^{-i\theta J_l} = \left[\cos\left(\frac{\theta}{2}\right) \mathbb{1}_2 + i \sin\left(\frac{\theta}{2}\right) \sigma_l \right]^{\otimes N}. \tag{1.1.110}$$

In particular, this operation is known as the collective spin rotation, which we will discuss in more detail in Sec. 1.3. We remark that any local unitary operation cannot change the purity of any reduced state. That is, $\gamma(\varrho'_X) = \gamma(U_X \varrho_X U_X^\dagger) = \gamma(\varrho_X)$ for any reduced state $\varrho'_X = \mathrm{tr}_{X^c}[\Phi_{\mathrm{LU}}(\varrho)]$ and X^c the complement of a set X.

Two-qubit local unitary operations: Consider the case where a two-qubit state ϱ_{AB} is transformed by a local unitary operation $U_A \otimes U_B$ into another state ϱ'_{AB}: $\varrho'_{AB} = (U_A \otimes U_B)\varrho_{AB}(U_A \otimes U_B)^\dagger$. The Bloch decomposition of the state ϱ'_{AB} can be written as

$$\varrho'_{AB} = \frac{1}{4} \left(\mathbb{1}_2^{\otimes 2} + \sum_{i=1}^{3} a'_i \sigma_i \otimes \mathbb{1}_2 + \sum_{i=1}^{3} b'_i \mathbb{1}_2 \otimes \sigma_i + \sum_{i,j=1}^{3} t'_{ij} \sigma_i \otimes \sigma_j \right), \tag{1.1.111}$$

where $\boldsymbol{a}' = O_A \boldsymbol{a}$, $\boldsymbol{b}' = O_B \boldsymbol{b}$, and $T' = O_A T O_B^\top$ with the orthogonal matrices O_A and O_B discussed in Eq. (1.1.42). Here the matrix T' can be diagonalized by a specific local unitary

$$T' = \mathrm{diag}(\tau_1, \tau_2, \tau_3), \tag{1.1.112}$$

where τ_i are eigenvalues of T'. Rearranging the notations, we can write any two-qubit state ϱ_{AB} in the following Bloch decomposition, up to local unitaries:

$$\varrho_{AB} = \frac{1}{4} \left(\mathbb{1}_2^{\otimes 2} + \sum_{i=1}^{3} a_i \sigma_i \otimes \mathbb{1}_2 + \sum_{i=1}^{3} b_i \mathbb{1}_2 \otimes \sigma_i + \sum_{i=1}^{3} \tau_i \sigma_i \otimes \sigma_i \right). \tag{1.1.113}$$

Nonlocal unitary operations: In two-qubit systems, one of the most famous nonlocal unitary operations is the controlled-NOT (CNOT) gate:

$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.1.114}$$

This unitary can change a state as follows:

$$U_{\text{CNOT}}\left(a|00\rangle+b\,|01\rangle+c\,|10\rangle+d\,|11\rangle\right)=a|00\rangle+b\,|01\rangle+c\,|11\rangle+d\,|10\rangle\,. \quad (1.1.115)$$

In general, any two-qubit unitary operation can be written in the following form:

$$U_{AB}=(V_A\otimes V_B)e^{-iH}(W_A\otimes W_B), \quad (1.1.116)$$
$$H=c_x\sigma_x\otimes\sigma_x+c_y\sigma_y\otimes\sigma_y+c_z\sigma_z\otimes\sigma_z, \quad (1.1.117)$$

for single-qubit unitaries V_A, V_B, W_A, W_B and $0\leq c_z\leq c_y\leq c_x\leq\pi/4$. Denoting the vector $\boldsymbol{c}=(c_x,c_y,c_z)$, we give the following summary:

- If $U_{AB}=U_A\otimes U_B$, then $\boldsymbol{c}=(0,0,0)$.
- If $U_{AB}=U_{\text{CNOT}}$, then $\boldsymbol{c}=(\pi/4,0,0)$.
- If $U_{AB}=\mathbb{S}$, then $\boldsymbol{c}=(\pi/4,\pi/4,\pi/4)$.

Here $\mathbb{S}$ denotes the SWAP operation that will be explained in the next paragraph. In this way, one can characterize two-qubit nonlocal unitaries, independently of local unitaries. For details about this decomposition, see [48–51].

In N-qubit systems, an example of nonlocal unitary operations is the squeezing operation

$$U=e^{-i\theta J_l^2}, \quad (1.1.118)$$

where J_l is the collective angular momentum for $l=x,y,z$. Note that one can also consider the higher-order extensions such as J_l^k for $k\geq 3$. The squeezing operation is known to create a useful state in quantum parameter estimation tasks, for details see Sec. 1.3.

SWAP operation: The SWAP (flip) operation can exchange two particles:

$$\mathbb{S}\,|a\rangle\otimes|b\rangle=|b\rangle\otimes|a\rangle\,. \quad (1.1.119)$$

The SWAP operator is written as

$$\mathbb{S}=\sum_{i,j=0}^{d^2-1}|i\rangle\langle j|\otimes|j\rangle\langle i|\,. \quad (1.1.120)$$

The eigenvalues of $\mathbb{S}$ are ±1. Note that the SWAP is Hermitian, unitary, and involutory: $\mathbb{S}^\dagger=\mathbb{S}$, $\mathbb{S}^\dagger=\mathbb{S}^{-1}$, and $\mathbb{S}^2=\mathbb{1}_d$. There are many useful formulas related to the SWAP operator, called SWAP tricks, for details see Sec. 1.1.7.

Permutation operations: For a permutation $\pi : abc \to \pi(a)\pi(b)\pi(c)$, a permutation operation $W_\pi \in \mathcal{H}_d^{\otimes 3}$ can exchange a three-particle state as follows:

$$W_\pi |a\rangle \otimes |b\rangle \otimes |c\rangle = |\pi(a)\rangle \otimes |\pi(b)\rangle \otimes |\pi(c)\rangle . \tag{1.1.121}$$

For instance, the permutation $\pi(a) = b, \pi(b) = c, \pi(c) = a$, leads to

$$W_\pi |a\rangle \otimes |b\rangle \otimes |c\rangle = |b\rangle \otimes |c\rangle \otimes |a\rangle . \tag{1.1.122}$$

In total, there are six (= 3!) permutations, including the identical operation.

Let us discuss the permutation operation in N particle systems. Let $\mathrm{Sym}(N)$ be the symmetric group on the set $\{1, 2, \ldots, N\}$ and let $\pi = \pi(1) \ldots \pi(N) \in \mathrm{Sym}(N)$ be a permutation. A permutation operator $W_\pi \in \mathcal{H}_d^{\otimes N}$ is given by

$$W_\pi |i_1, \ldots, i_N\rangle = |i_{\pi(1)}, \ldots, i_{\pi(N)}\rangle . \tag{1.1.123}$$

In the following, we make several remarks about permutation operations:

- Group structure: The set of permutation operators forms a group structure. That is, the product of any two permutations is also a permutation, and there exists an identity and inverse of all operations. Note that there are $N!$ permutations.
- Differences from SWAP: Permutation operators do not mutually commute for $N \geq 3$ in general. Also, permutation operators are not Hermitian for $N \geq 3$ in general.
- Any permutation operator can be (not uniquely) represented as the product of permutations of two particles, that is, SWAP operations.
- Any permutation operator is unitary since SWAP operations are unitary.
- The following permutation operator is called the cyclic operator

$$W_{\mathrm{cyc}} |i_1, i_2, \ldots, i_N\rangle = |i_2, \ldots, i_N, i_1\rangle . \tag{1.1.124}$$

For details about permutation operations, see [52–54] and Sec. 1.1.7.

LOCC operations: Consider the scenario in which Alice and Bob are spatially separated (such as in Germany and Japan), and they share a quantum state $\varrho_{AB} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$. A quantum operation is called a local operation if

$$[\Phi_A \otimes \Phi_B](\varrho_{AB}) = \sum_{i,j} (A_i \otimes B_j) \varrho_{AB} (A_i^\dagger \otimes B_j^\dagger), \tag{1.1.125}$$

where Kraus operators A_i and B_j respectively act on subsystem A and B with $\sum_i A_i^\dagger A_i = \sum_i B_i^\dagger B_i = \mathbb{1}_d$.

A more general class of quantum operations is called local operations and classical communication (LOCC). To be more specific, suppose that Alice starts

by performing a POVM measurement from $\{A_i\}$ locally on the state and obtains an outcome i. Then Alice sends the result to Bob using classical communication such as telephone calls. After Bob receives the result, Bob performs a local POVM measurement $\{B_j^i\}$ depending on i, and then obtains an outcome j. Again, Bob transmits the result back to Alice, and Alice applies POVM measurements $\{A_k^{ij}\}$ depending on i, j. They repeat these local operations and classical communication over many rounds.

Mathematically, the LOCC operations can be written as follows:

$$\Phi_{\mathrm{LOCC}}(\varrho_{AB}) = \sum_{i,j,k,l\ldots} (\cdots A_k^{ij} A_i) \otimes (\cdots B_l^{ijk} B_j^i) \varrho_{AB} (\cdots A_k^{ij} A_i)^\dagger \otimes (\cdots B_l^{ijk} B_j^i)^\dagger, \quad (1.1.126)$$

where each operator follows the trace-preserving condition:

$$\sum_i A_i^\dagger A_i = \sum_j (B_j^i)^\dagger B_j^i = \sum_k (A_k^{ij})^\dagger A_k^{ij} = \sum_l (B_l^{ijk})^\dagger B_l^{ijk} = \cdots = \mathbb{1}_d. \quad (1.1.127)$$

Based on the above properties, we can rewrite the LOCC operation as

$$\Phi_{\mathrm{LOCC}}(\varrho_{AB}) = \sum_x (\tilde{A}_x \otimes \tilde{B}_x) \varrho_{AB} (\tilde{A}_x^\dagger \otimes \tilde{B}_x^\dagger). \quad (1.1.128)$$

Finally, a quantum operation is called separable operation if

$$\Phi_{\mathrm{SEP}}(\varrho_{AB}) = \sum_i (A_i \otimes B_i) \varrho_{AB} (A_i^\dagger \otimes B_i^\dagger), \quad (1.1.129)$$

where $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathbb{1}_d^{\otimes 2}$. It is important to note that there are separable operations that cannot be implemented by LOCC operations even with infinite rounds. For details about LOCC operations, see [55].

SLOCC operations: For a two-particle state $\varrho_{AB} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$, a quantum operation is called stochastic local operation and classical communication SLOCC if it can describe the LOCC transformation with some probability and not necessarily satisfy the trace-preserving condition:

$$\Phi_{\mathrm{SLOCC}}(\varrho_{AB}) = (A \otimes B) \varrho_{AB} (A^\dagger \otimes B^\dagger), \quad (1.1.130)$$

where A, B are arbitrarily invertible matrices with $A^\dagger A \otimes B^\dagger B \leq \mathbb{1}_d^{\otimes 2}$.

Local filtering operations: For a two-particle quantum state $\varrho_{AB} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$, a quantum operation is called local filtering if it maps ϱ_{AB} as follows:

$$\Phi_{\mathrm{LF}}(\varrho_{AB}) = (F_A \otimes F_B) \varrho_{AB} (F_A^\dagger \otimes F_B^\dagger) = \frac{1}{d^2} \left(\mathbb{1}_d^{\otimes 2} + \sum_{i=1}^{d^2-1} t_i \lambda_i \otimes \lambda_j \right), \quad (1.1.131)$$

where F_A, F_B are arbitrary invertible matrices and we use the Bloch decomposition in Eq. (1.1.100). The local filtering operation can make the reduced states maximally mixed, that is, $\mathrm{tr}_X[\Phi_{\mathrm{LF}}(\varrho_{AB})] = \mathbb{1}_d/d$ for $X = A, B$. This is one of the SLOCC operations and provides the analytically tractable expression of the state. For details about local filtering operations, see [56–60].

Generalized universal state inversions: For an N-qubit state $\varrho \in \mathcal{H}_2^{\otimes N}$, we call a map the generalized spin-flip if

$$\bigotimes_{i=1}^{N} \mathcal{S}_2^{(i)}(\varrho) = \sigma_y^{\otimes N} \varrho^{\top} \sigma_y^{\otimes N}, \tag{1.1.132}$$

where $\mathcal{S}_2^{(i)}$ is the spin-flip map in Eq. (1.1.56) on the i-th subsystem. This map preserves the positivity of ϱ since $\mathcal{S}_2^{(i)}$ is the positive map.

In general, a map is called generalized universal state inversion if

$$\bigotimes_{i=1}^{N} \mathcal{S}_d^{(i)}(\varrho) = \left[\prod_{X=1}^{N} \left(\mathrm{tr}_X(\cdot) \otimes \mathrm{id}_X - \mathrm{id} \right) \right] (\varrho), \tag{1.1.133}$$

where $\mathcal{S}_d^{(i)}$ is the universal state inversion in Eq. (1.1.58) on the i-th subsystem. Using the expression in Eq. (1.1.102), we can rewrite

$$\begin{aligned} \bigotimes_{i=1}^{N} \mathcal{S}_d^{(i)}(\varrho) = \frac{1}{d^N} \Big[& (d-1)^N \mathbb{1}_d^{\otimes N} - (d-1)^{N-1} P_1 + (d-1)^{N-2} P_2 \\ & - (d-1)^{N-3} P_3 + \cdots + (-1)^{N-1} (d-1) P_{N-1} + (-1)^N P_N \Big]. \end{aligned} \tag{1.1.134}$$

This operation will be used to characterize the positivity of multipartite quantum states, see Sec. 1.4.2. For details about generalized universal state inversions, see [27, 61–63].

Bell-diagonal states: For a two-qubit state ϱ_{AB}, we consider the following operation:

$$\Phi_{\mathcal{S}_2^{AB}}(\varrho_{AB}) = \frac{1}{2} \varrho_{AB} + \frac{1}{2} \mathcal{S}_2^{(A)} \otimes \mathcal{S}_2^{(B)}(\varrho_{AB}), \tag{1.1.135}$$

where $\mathcal{S}_2^{(X)}$ is the spin-flip map in subsystem $X = A, B$. This mixing operation can eliminate the local Bloch vector, leading to

$$\Phi_{\mathcal{S}_2^{AB}}(\varrho_{AB}) = \frac{1}{4} \left(\mathbb{1}_2^{\otimes 2} + \sum_{i,j=1}^{3} t_{ij} \sigma_i \otimes \sigma_j \right). \tag{1.1.136}$$

We should note that this does not result from local filtering operations.

Recalling that the matrix $T = (t_{ij})$ can be diagonalized by applying a specific local unitary [see Eq. (1.1.113)], we can have the so-called Bell-diagonal state:

$$\varrho_{\mathrm{BD}} = (U_A \otimes U_B) \Phi_{\mathcal{S}_2^{AB}}(\varrho_{AB}) (U_A \otimes U_B)^{\dagger} = \frac{1}{4} \left(\mathbb{1}_2^{\otimes 2} + \sum_{i=1}^{3} \tau_i \sigma_i \otimes \sigma_i \right). \tag{1.1.137}$$

This state has only three parameters, so it is easily analytically tractable. For details about this state, see [64] and Sec. 1.2.3.

Twirling operations: For an N-particle quantum state $\varrho \in \mathcal{H}_d^{\otimes N}$, the twirling operation is defined as

$$\Phi_{\text{Twirl}}(\varrho) = \int dU\, U^{\otimes N} \varrho (U^\dagger)^{\otimes N}, \tag{1.1.138}$$

where the integral taken with respect to the so-called Haar unitary measure. Before proceeding, let us recap the notion of the Haar measure.

Let $\mathcal{U}(d)$ be the group of all $d \times d$ unitary matrices. The Haar unitary measure is the uniform probability measure over the unitary group $\mathcal{U}(d)$. Consider an integral of $f(U)$ over the unitary group $\mathcal{U}(d)$ with respect to the Haar measure dU. One of the most important properties of the Haar measure is the left and right invariance under shifts via multiplication by a unitary $V \in \mathcal{U}(d)$, that is,

$$\int dU = 1, \qquad \int dU\, f(U) = \int dU\, f(VU) = \int dU\, f(UV), \tag{1.1.139}$$

see Refs. [65–69] for further details. A general parametrization of the unitary group $\mathcal{U}(d)$ and the associated Haar measure are known [67, 70]. For instance, any single-qubit unitary ($d = 2$) can be written in the so-called Euler angle representation $U(\alpha, \beta, \gamma) = U_z(\alpha) U_y(\beta) U_z(\gamma)$, where $U_i(\theta) = e^{-i\theta\sigma_i/2}$ for $i = y, z$ and the Haar measure $dU = \sin\beta\, d\alpha\, d\beta\, d\gamma$, see [18].

Let us make several remarks about twirling operations.

- $\Phi_{\text{Twirl}}(\varrho)$ is completely positive and trace preserving.
- For an Hermitian operator $X \in \mathcal{H}_d^{\otimes N}$, it holds that

$$\text{tr}[\Phi_{\text{Twirl}}(\varrho) X] = \text{tr}[\varrho \Phi_{\text{Twirl}}(X)]. \tag{1.1.140}$$

- A quantum state ϱ is called a Werner state [71] if

$$\Phi_{\text{Twirl}}(\varrho_{\text{W}}) = \varrho_{\text{W}}. \tag{1.1.141}$$

  For instance, for $N = 2$, the Werner state can be represented by

$$\varrho_{\text{W}} = a \mathbb{1}_d^{\otimes 2} + b \mathbb{S}, \tag{1.1.142}$$

  for some coefficient a, b and the SWAP in Eq. (1.1.119). Regarding the normalization condition and the positivity constraint, it can be rewritten as

$$\varrho_{\text{W}} = \frac{a}{d^2} \mathbb{1}_d^{\otimes 2} + \frac{1-a}{d} \mathbb{S}, \tag{1.1.143}$$

  for $a \in [d/(d+1), d/(d-1)]$.

- The twirling operation can be investigated using a famous result in representation theory [72, 73], called the Schur–Weyl duality. It leads to

$$\Phi_{\text{Twirl}}(\varrho) = \sum_{\pi \in \text{Sym}(N)} c_\pi W_\pi, \tag{1.1.144}$$

  for coefficients c_π and the permutation operators W_π in Eq. (1.1.123).

For details about twirling operations and Haar unitary integrals, see Ref. [74] and Sec. 1.5 and Chapter 9.

Quantum measurements in composite systems

Collective observables: For a N-particle system, an observable M is called collective if

$$M_{\mathrm{C}} = M_1 \otimes \mathbb{1}_{2\ldots N} + \mathbb{1}_1 \otimes M_2 \otimes \mathbb{1}_{3\ldots N} \cdots + \mathbb{1}_{1\ldots N-1} \otimes M_N = \sum_{i=1}^{N} M_i \otimes \mathbb{1}_{\bar{i}}, \quad (1.1.145)$$

where M_i and $\mathbb{1}_i$ are respectively an observable and an identity acting on the i-th subsystem. Note that often $\mathbb{1}_{\bar{i}}$ is removed for a short notation. Examples are the collective angular moment $J_l = (1/2)\sum_{i=1}^{N} \sigma_l^{(i)}$ in Eq. (1.1.109) or more generally the N-qudit collective operator

$$G_l = \frac{1}{d} \sum_{i=1}^{N} \lambda_l^{(i)}, \quad (1.1.146)$$

with the Gell-Mann matrix $\lambda_l^{(i)}$ for $i = 1, 2, \ldots, d^2 - 1$.

Product and non-product observables: For an N-particle system, an observable M is called product if

$$M_{\mathrm{P}} = M_1 \otimes M_2 \otimes \cdots \otimes M_N, \quad (1.1.147)$$

while it is called non-product if it cannot be written in product form

$$M_{\mathrm{NP}} = \sum_{i=1}^{N} m_i M_1^{(i)} \otimes M_2^{(i)} \otimes \cdots \otimes M_N^{(i)}, \quad (1.1.148)$$

with m_i being real coefficients, not necessarily a minimal decomposition. Examples are respectively given by

$$M_z = \sigma_z \otimes \sigma_z \otimes \cdots \otimes \sigma_z, \qquad M_{xyz} = \sum_{i=x,y,z} \sigma_i \otimes \sigma_i \otimes \cdots \otimes \sigma_i, \quad (1.1.149)$$

where σ_i denotes the Pauli matrix.

For the sake of simplicity, consider the case of $N = 2$. Recall that the eigenvalues of σ_z are ± 1 and the corresponding normalized eigenstates are respectively $|z,+\rangle = |0\rangle$ and $|z,-\rangle = |1\rangle$. Letting the projectors $\Pi_\pm = |z,\pm\rangle\langle z,\pm|$, the product observable M_z can be written as

$$M_z^{AB} = \Pi_+^A \otimes \Pi_+^B - \Pi_-^A \otimes \Pi_+^B - \Pi_+^A \otimes \Pi_-^B + \Pi_-^A \otimes \Pi_-^B, \quad (1.1.150)$$

whereas the non-product observable has a more complicated form. In practice, product observables are typically easily accessible, so they are more commonly considered. On the other hand, non-product observables are also useful to extract further quantum information about the state. For more details, see [22, 75–80].

1.1.5 Classical statistics

In this subsection, we will give a short introduction to classical statistics. For details, see [81–84].

Definitions: Let X be a random variable with a probability of taking a certain value. Let x be the value of a random variable X and let p_x be its corresponding probability to obtain the outcome x. The value x is either continuous or discrete. Here we consider discrete cases, where $p_x \in [0,1]$ and $\sum_x p_x = 1$. Then we define the expectation and variance as

$$\mathbb{E}(X) = \sum_x x p_x, \tag{1.1.151}$$

$$\mathrm{Var}(X) = \mathbb{E}[(X - \mathbb{E}(X))^2] = \mathbb{E}(X^2) - [\mathbb{E}(X)]^2. \tag{1.1.152}$$

Binomial distribution: Suppose that we throw a coin and obtain an outcome that is either heads or tails with corresponding probability p or $1-p$. After repeating n times, the probability of seeing heads k times is given by the binomial distribution $B(n,p)$.

To be more precise, we denote a random variable X as the number of heads counted in n trials. Let us write $X \sim B(n,p)$ if the random variable X follows the binomial distribution $B(n,p)$, where the probability to get k number of heads is given by

$$p_x = \binom{n}{k} p^k (1-p)^{n-k}. \tag{1.1.153}$$

The expectation and variance are given by

$$\mathbb{E}(X) = \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k} = np, \qquad \mathrm{Var}(X) = np(1-p). \tag{1.1.154}$$

Normal distribution: For a random variable X, we write $X \sim \mathcal{N}(\mu, \sigma^2)$ if it follows the normal distribution $\mathcal{N}(\mu, \sigma^2)$ given by

$$p_x = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \tag{1.1.155}$$

where X is a continuous random variable. The expectation and variance are given by

$$\mathbb{E}(X) = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} x e^{-\frac{(x-\mu)^2}{2\sigma^2}} = \mu, \qquad \mathrm{Var}(X) = \sigma^2. \tag{1.1.156}$$

The normal distribution plays a critical role in statistics. One of the main reasons is that many certain distributions tend to the normal distribution according to the central limit theorem that will be explained in Eq. (1.1.168).

Moment problems: For a random variable X following a given probability distribution p_x, the t-th moment is defined as

$$\mu_t \equiv \mathbb{E}(X^t) = \sum_x x^t p_x. \tag{1.1.157}$$

This leads to a sequence of moments, that is, $\boldsymbol{\mu}^{(n)} = (\mu_0, \mu_1, \ldots, \mu_n)$. The moment problems ask the converse: For a given sequence $\boldsymbol{\mu}^{(n)}$, does there exist a probability p_x and a random variable X such that $\mu_t = \sum x^t p_x$ for $t = 0, 1, \ldots, n$? In particular, the so-called Hamburger moment problem considers the case with real x, whereas the so-called Stieltjes moment problem considers the case with positive x.

Dependence and correlation: Let $p_{x,y}$ be the joint probability of two random variables X, Y to obtain the pair (x, y). For the joint probability $p_{x,y}$, its marginal probabilities of X and Y are defined as $p_x = \sum_y p_{x,y}$ and $p_y = \sum_x p_{x,y}$. Two random variables X, Y are called independent if and only if $p_{x,y} = p_x p_y$ for all x, y. Two random variables X, Y are called identically distributed if and only if $p_x = p_y$ for all x, y.

For two random variables X, Y and parameters a, b, c, it holds that

$$\mathbb{E}(aX + bY + c) = a\,\mathbb{E}(X) + b\,\mathbb{E}(Y) + c, \tag{1.1.158}$$

$$\mathrm{Var}(aX + bY + c) = a^2\,\mathrm{Var}(X) + b^2\,\mathrm{Var}(Y) + 2ab\,\mathrm{Cov}(X, Y), \tag{1.1.159}$$

where $\mathrm{Cov}(X, Y)$ is called the covariance

$$\mathrm{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))] = \mathbb{E}[XY] - \mathbb{E}[X]\,\mathbb{E}[Y]. \tag{1.1.160}$$

The covariance can quantify the correlation between random variables X and Y. It is important to note that correlation is different from dependence. In fact, if X and Y are independent, then $\mathrm{Cov}(X, Y) = 0$, that is, they are uncorrelated. On the other hand, even if $\mathrm{Cov}(X, Y) = 0$, they are not always independent.

Finite statistics: Suppose that we are interested in collecting all data on heights in a country. This type of data set is called the population. Let us denote the population probability distribution as p_x and the population expectation (variance) as μ (and σ^2). In practical settings, μ and σ^2 are considered unknown/known. Since it cannot be possible to collect all the data in practical experiments, we should take a finite sample $X_1, X_2, \ldots, X_n$ from the population. This sampling allows us to extract information about μ and σ^2 in the population.

Often this sampling is assumed to be random so that $X_1, X_2, \ldots, X_n$ are recognized as independent and identically distributed (i.i.d.) random variables following the probability distribution p_x. This leads to that $\mathbb{E}(X_i) = \mu$ and $\mathrm{Var}(X_i) = \sigma^2$ for any i. The task is to estimate, for example, μ and σ^2, from a finite number of measurements.

Unbiased estimators: Let us denote the statistical parameter that we want to know as θ such as μ or σ^2 in the population. The so-called estimator $\tilde{\theta}$ is often required to satisfy two properties. The first is consistency, that is, $\widetilde{\theta}$ approaches to θ for a large n. The second is unbiasedness, that is, the expectation of $\widetilde{\theta}$ becomes θ:

$$\mathbb{E}(\widetilde{\theta}) = \theta. \tag{1.1.161}$$

For instance, consider the sample mean of i.i.d. random variables $X_1, \ldots, X_n$

$$\widetilde{X} = \frac{1}{n}\sum_{i=1}^{n} X_i. \tag{1.1.162}$$

This is an unbiased estimator for μ:

$$\mathbb{E}(\widetilde{X}) = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}(X_i) = \frac{1}{n}\sum_{i=1}^{n}\mu = \mu. \tag{1.1.163}$$

In a similar way, let us consider the sample variance

$$\widetilde{S^2} = \frac{1}{n}\sum_{i=1}^{n}(X_i - \widetilde{X})^2. \tag{1.1.164}$$

Naively thinking, one may expect that $\widetilde{S^2}$ can be also the unbiased estimator for σ^2, but this is not correct:

$$\mathbb{E}(\widetilde{S^2}) = \frac{1}{n}\sum_{i=1}^{n}\left[\mathbb{E}(X_i^2) - 2\mathbb{E}(X_i\widetilde{X}) + \mathbb{E}(\widetilde{X}^2)\right] = \frac{n-1}{n}\sigma^2, \tag{1.1.165}$$

where we use that $\mathbb{E}(X_i^2) = \sigma^2 + \mu^2$ and $\mathbb{E}(X_iX_j) = \mathbb{E}(X_i)\mathbb{E}(X_j) = \mu^2$ for $i \neq j$. That is, using the sample variance $\widetilde{S^2}$ can lead to the underestimation for σ^2. Accordingly, the unbiased estimator for σ^2 is given by

$$\widetilde{U^2} = \frac{n}{n-1}\widetilde{S^2}. \tag{1.1.166}$$

Law of large numbers: Consider i.i.d. random variables $X_1, X_2, \ldots, X_n$ with $\mathbb{E}(X_i) = \mu$ for any i. The law of large numbers states that the sample mean converges to the expectation μ for a large n:

$$\widetilde{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \to \mu, \qquad \text{for large } n. \tag{1.1.167}$$

This theorem can be used to guarantee the consistency condition of estimators for a large sample.

Central limit theorem: Consider i.i.d. random variables $X_1, X_2, \ldots, X_n$ with $\mathbb{E}(X_i) = \mu$ and $\mathrm{Var}(X_i) = \sigma^2$ for any i. The central limit theorem states that the sample mean follows the normal distribution with $\mathcal{N}(\mu, \sigma^2/n)$ for a large n:

$$\widetilde{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \sim \mathcal{N}(\mu, \sigma^2/n), \qquad \text{for large } n. \tag{1.1.168}$$

Here we make two important remarks. First, the central limit theorem does not assume anything about the probability distribution. Second, since the variance is given by σ^2/n, the larger the number of samples, the smaller the variance, and therefore the more accurate the estimation. The fact that the variance decreases in order $1/n$ is often called the shot-noise scaling. As we will see Sec. 1.3, in quantum metrology, the variance can scale beyond the shot-noise scaling.

Statistical significance: Suppose that we are interested in a statistical parameter θ in the population and try to create an unbiased estimator $\widetilde{\theta}$ for θ from experimental data. In practice, the estimator should deviate from θ, but we may want to know how far it is. More precisely, we may be concerned with the probability that $\widetilde{\theta}$ deviates from θ by a constant margin δ. This probability is called the p-value, which is characterized by the so-called statistical significance level α:

$$\mathrm{Prob}(|\widetilde{\theta} - \theta| \geq \delta) \leq \alpha. \tag{1.1.169}$$

Often, δ is called the error or accuracy, δ/θ is called the relative error, and $\gamma = 1 - \alpha$ is called the confidence level.

Concentration inequalities: A practical tool to estimate the p-value is the concentration inequalities. A common example is the Markov inequality, which states that for a nonnegative random variable X, the following holds

$$\mathrm{Prob}(X \geq \delta) \leq \frac{\mathbb{E}(X)}{\delta}, \tag{1.1.170}$$

for any $\delta > 0$. For a large δ, the right-hand side becomes small.

Another famous example is known as the Chebyshev inequality, which is the case of the Markov inequality when $X \to (X-\mu)^2$ and $\delta \to (\delta\sigma)^2$. It states for a random variable X with $\mathbb{E}(X) = \mu$ and $\mathrm{Var}(X) = \sigma^2$, it holds that

$$\mathrm{Prob}(|X - \mu| \geq \delta) \leq \frac{\sigma^2}{\delta^2}, \tag{1.1.171}$$

for any $\delta > 0$. As a random variable X, let us take the sample mean $\widetilde{X}$ for n random variables with $\mathbb{E}(\widetilde{X}) = \mu$ and $\mathrm{Var}(\widetilde{X}) = \sigma^2/n$. Then the Chebyshev inequality becomes

$$\mathrm{Prob}(|\widetilde{X} - \mu| \geq \delta) \leq \frac{\sigma^2}{n\delta^2}. \tag{1.1.172}$$

In particular, for a large n, the right-hand side converges to zero. This implies the law of large numbers.

In practice, the Chebyshev inequality can be employed in the following way. Since $n = \sigma^2/(\delta^2\alpha)$ with the statistically significant level α, if we take, e.g., $\mu = 2$, $\sigma^2 = 0.5$, $\alpha = 0.05$, and $\delta/\mu = 0.05$, then the number of measurement times is given by $n = 0.5/(0.05 \times 0.1^2) = 1000$. That is, 1000 measurements are required to conclude that there is at most a 5% probability that the expectation estimation deviates from the true value by at least 10% relative error.

Other examples of concentration inequalities include Cantelli, Bernstein, Hoeffding, and McDiarmid inequalities as well as Chernoff bounds. In Chapter 3, we will apply concentration inequalities for statistically significant tests in randomized measurements.

1.1.6 Analyzing quantum states

State tomography: Consider an experimental situation where we create a quantum state ϱ in a laboratory but we do not know the elements of the density matrix in ϱ. The task is to obtain information about the density matrix ϱ by measuring several observables $M_1, M_2, \ldots$. That is, we want to reconstruct the state ϱ using the expectations $\mathrm{tr}(\varrho M_1), \mathrm{tr}(\varrho M_2) \ldots$. The set of such measurements is called tomographically complete if we can uniquely identify the quantum state.

For instance, the set of the Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$ is tomographically complete to reconstruct a single-qubit state. In fact, we notice that $a_i = \mathrm{tr}(\varrho\sigma_i) = \langle\sigma_i\rangle$ in the Bloch decomposition in Eq. (1.1.14). Knowing all the expectations allows us to reconstruct the state as

$$\varrho_{\mathrm{recs}} = \frac{1}{2}\left(\mathbb{1}_2 + \sum_{i=x,y,z} \langle\sigma_i\rangle\sigma_i\right). \tag{1.1.173}$$

Since the Pauli matrix σ_i has ± 1 eigenvalues with the corresponding eigenstates $|i,\pm\rangle$ for $i = x, y, z$, one can express the expectation as $\langle\sigma_i\rangle = p(i,+) - p(i,-)$, for the probabilities given by $p(i,\pm) = \langle i,\pm|\varrho|i,\pm\rangle$. Note that due to the normalization condition $p(i,+) + p(i,-) = 1$, the expectation can be estimated by repeating projective measurements on only one basis. Suppose that we perform N times measurements in total to estimate $\langle\sigma_z\rangle$. Now the number of outcomes to get $+1$ value, say N_+, is a random variable following the binomial distribution with probability p_+: $N_+ \sim B(N, p_+)$, see Sec. 1.1.5. Using the result that $\mathbb{E}(N_+) = Np_+$, it turns out that the quantity $\tilde{Z} = [(2N_+/N) - 1]$ is an unbiased estimator for $\langle\sigma_z\rangle$. That is, it holds that $\mathbb{E}(\tilde{Z}) = \langle\sigma_z\rangle$. According to the central limit theorem, for large N, one can estimate the expectation with high precision.

Quantum state tomography has two major downsides. First, a reconstructed state ϱ_{recs} can have negative eigenvalues. This is because the number of measurements is finite in practice, and it is not possible to know the exact values of all expectations due to statistical errors. Second, when the number of particles

increases, the number of necessary measurements grows exponentially. In an N-qubit state, 3^N measurements are required for the complete reconstruction of the state. For details about quantum state tomography, see [85–87].

Fidelity and trace distance: For two quantum states ϱ and σ, there are two common ways to quantify how much they are close to each other. One way is to use the fidelity $F(\varrho, \sigma)$ defined as

$$F(\varrho, \sigma) = \mathrm{tr}\left[\sqrt{\sqrt{\sigma}\varrho\sqrt{\sigma}}\right]. \tag{1.1.174}$$

This can be equivalently expressed as $F(\varrho, \sigma) = \mathrm{tr}(|\sqrt{\varrho}\sqrt{\sigma}|)$, where the absolute value of an operator A is defined as $|A| = \sqrt{A^\dagger A}$. The range is given by $0 \leq F(\varrho, \sigma) \leq 1$. Here $F(\varrho, \sigma) = 1$ if and only if $\varrho = \sigma$, while $F(\varrho, \sigma) = 0$ if and only if ϱ are σ live on orthogonal subspaces. Note that the fidelity is symmetric: $F(\varrho, \sigma) = F(\sigma, \varrho)$. For two pure states $|\psi\rangle$ and $|\phi\rangle$, it can be rewritten as

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|. \tag{1.1.175}$$

Another way to distinguish two states is to use the trace distance $D(\varrho, \sigma)$ defined as

$$D(\varrho, \sigma) = \frac{1}{2}\|\varrho - \sigma\|_{\mathrm{Tr}} = \frac{1}{2}\mathrm{tr}(|\varrho - \sigma|), \tag{1.1.176}$$

where $\|X\|_{\mathrm{Tr}}$ is the sum of the singular values of X. The range is given by $0 \leq D(\varrho, \sigma) \leq 1$. The trace distance satisfies the triangle inequality

$$D(\varrho, \sigma) \leq D(\varrho, \xi) + D(\xi, \sigma), \tag{1.1.177}$$

for states ϱ, σ, ξ.

A common property between the fidelity and the trace distance is called the contractivity under completely positive (CP) operations: For a CP map Φ, it holds that

$$F(\varrho, \sigma) \leq F(\Phi(\varrho), \Phi(\sigma)), \tag{1.1.178}$$
$$D(\varrho, \sigma) \geq D(\Phi(\varrho), \Phi(\sigma)). \tag{1.1.179}$$

This property implies that when two states are acted on a CP operation, it becomes more difficult to distinguish between them.

It may be useful to note the so-called Fuchs–van de Graaf inequalities [88]:

$$1 - F(\varrho, \sigma) \leq D(\varrho, \sigma) \leq \sqrt{1 - F^2(\varrho, \sigma)}. \tag{1.1.180}$$

Using these inequalities allows us to estimate the trace distance from the fidelity, and vice versa.

Let us introduce the distance measures based on fidelity. For two quantum states ϱ and σ, the Bures distance and angle are respectively defined as

$$D_B(\varrho,\sigma) = \sqrt{2(1-F(\varrho,\sigma))}, \tag{1.1.181}$$

$$A_B(\varrho,\sigma) = \arccos F(\varrho,\sigma), \tag{1.1.182}$$

$$D_B(\varrho,\sigma) \leq A_B(\varrho,\sigma), \tag{1.1.183}$$

where $F(\varrho,\sigma)$ is the fidelity defined in Eq. (1.1.174). Note that the Bures distance and angle obey the triangle inequality and the contractivity under CP operations. For details about the fidelity and trace distance, see [19, 89, 90].

Fubini-Study metric: For pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, the Bures distance is given by

$$D_B^2(|\psi_1\rangle, |\psi_2\rangle) = 2(1 - |\langle\psi_1|\psi_2\rangle|). \tag{1.1.184}$$

Letting $|\psi_1\rangle = |\psi(t)\rangle\,(= |\psi\rangle)$ and $|\psi_2\rangle = |\psi(t+dt)\rangle$ for time $t > 0$, one has

$$\langle\psi(t)|\psi(t+dt)\rangle = 1 + dt\,\langle\psi|\partial_t\psi\rangle| + \frac{(dt)^2}{2!}\langle\psi|\partial_t^2\psi\rangle| + \mathcal{O}((dt)^3), \tag{1.1.185}$$

where $|\partial_t\psi\rangle = \frac{\partial}{\partial t}|\psi\rangle$ and $|\partial_t^2\psi\rangle = \frac{\partial^2}{\partial t^2}|\psi\rangle$. This leads to

$$|\langle\psi(t)|\psi(t+dt)\rangle| = 1 - \frac{(dt)^2}{2}\langle\partial_t\psi|(1-|\psi\rangle\langle\psi|)|\partial_t\psi\rangle, \tag{1.1.186}$$

where we used that $\partial_t\langle\psi|\psi\rangle = 0$, $\langle\partial^2\psi|\psi\rangle + \langle\psi|\partial^2\psi\rangle = -2\langle\partial\psi|\partial\psi\rangle$, and $(1+x)^{1/2} \approx 1 + x/2$. Finally, the Bures distance is given by

$$D_B^2(|\psi(t)\rangle, |\psi(t+dt)\rangle) = g_{\rm FS}(dt)^2, \tag{1.1.187}$$

where we ignore terms in at least $\mathcal{O}((dt)^3)$ and $g_{\rm FS} = \langle\partial_t\psi|(1-|\psi\rangle\langle\psi|)|\partial_t\psi\rangle$ is the so-called Fubini-Study metric.

The Fubini-Study metric is a measure of how much a quantum state changes under unitary dynamics for an infinitesimally short time. That is, a large $g_{\rm FS}$ implies that the two states $|\psi(t)\rangle$ and $|\psi(t+dt)\rangle$ become more distinguishable under a parameter shift t. For more details about the Fubini-Study metric, see [23].

Quantum Fisher metric: The quantum Fisher metric is the generalization of the Fubini-Study metric for mixed quantum states. Now suppose that a quantum state $\varrho(\theta)$ is changed to $\varrho(\theta+d\theta)$ under the unitary operation $U_\theta = \exp(-i\theta A)$ and the corresponding Hermitian generator A. One can show that the Bures distance is given by

$$D_B^2[\varrho(\theta), \varrho(\theta+d\theta)] = \frac{1}{4}\mathcal{F}_Q(\theta)(d\theta)^2, \tag{1.1.188}$$

where we ignore terms in at least $\mathcal{O}((d\theta)^3)$ and $\mathcal{F}_Q(\theta)$ is called the quantum Fisher metric that will be defined below. For details about the quantum Fisher metric, see [91–93].

Proof. Here we explain the proof of Eq. (1.1.188), following the description of Ref. [94]. We begin by writing the fidelity in Eq. (1.1.174) as

$$F[\varrho(\theta), \varrho(\theta + d\theta)] = \mathrm{tr}[\sqrt{M}], \qquad M \equiv \sqrt{\varrho(\theta)}\varrho(\theta + d\theta)\sqrt{\varrho(\theta)}. \tag{1.1.189}$$

Hereafter we denote that $\varrho(\theta) = \varrho$. Expanding $\varrho(\theta + d\theta)$ in terms of $(d\theta)$, one can represent $\sqrt{M}$ as

$$\sqrt{M} = \sqrt{\varrho^2 + (d\theta)A + \frac{(d\theta)^2}{2!}B}, \quad A \equiv \sqrt{\varrho}(\partial_\theta \varrho)\sqrt{\varrho}, \quad B \equiv \sqrt{\varrho}(\partial_\theta^2 \varrho)\sqrt{\varrho}, \tag{1.1.190}$$

where we ignore terms in at least $\mathcal{O}((d\theta)^3)$. To proceed, let us suppose that $\sqrt{M}$ can be also rewritten as

$$\sqrt{M} = \varrho + (d\theta)X + (d\theta)^2 Y, \tag{1.1.191}$$

for some operators X, Y. Now one can immediately find the relation

$$A = \varrho X + X\varrho, \qquad \frac{B}{2} = \varrho Y + Y\varrho + X^2. \tag{1.1.192}$$

To complete the derivation, it is sufficient to find the expressions of $\mathrm{tr}(X)$ and $\mathrm{tr}(Y)$. For the eigenvalue decomposition $\varrho(\theta) = \sum_i p_i(\theta)\,|\psi_i(\theta)\rangle\langle\psi_i(\theta)|$ with the eigenvalue $p_i(\theta)$ and $\langle\psi_i(\theta)|\psi_j(\theta)\rangle = \delta_{ij}$, the above relation Eq. (1.1.192) leads to

$$X_{ij} = \frac{A_{ij}}{p_i + p_j} = \frac{\sqrt{p_i}\sqrt{p_j}}{p_i + p_j}(\partial_\theta \varrho)_{ij}, \tag{1.1.193}$$

$$Y_{ii} = \frac{B_{ii}}{4p_i} - \frac{1}{2p_i}\sum_j X_{ij}X_{ji} = \frac{(\partial_\theta^2 \varrho)_{ii}}{4} - \frac{1}{2}\sum_j \frac{p_j}{(p_i + p_j)^2}(\partial_\theta \varrho)_{ij}(\partial_\theta \varrho)_{ji}, \tag{1.1.194}$$

where we denote $p_i(\theta) = p_i$. A straightforward calculation can yield

$$(\partial_\theta \varrho)_{ij} = (\partial_\theta p_i)\delta_{ij} + (p_j - p_i)\,\langle\psi_i|\partial_\theta\psi_j\rangle\,, \tag{1.1.195}$$

$$\begin{aligned}(\partial_\theta^2 \varrho)_{ij} = {} & (\partial_\theta^2 p_i)\delta_{ij} + 2(\partial_\theta p_j - \partial_\theta p_i)\,\langle\psi_i|\partial_\theta\psi_j\rangle + p_j\,\langle\psi_i|\partial_\theta^2\psi_j\rangle + p_i\,\langle\partial_\theta^2\psi_i|\psi_j\rangle \\ & + 2\sum_j p_j\,\langle\psi_i|\partial_\theta\psi_j\rangle\,\langle\partial_\theta\psi_j|\psi_j\rangle\,.\end{aligned} \tag{1.1.196}$$

Thus we can obtain

$$\mathrm{tr}(X) = \frac{1}{2}\sum_i(\partial_\theta p_i) = 0, \tag{1.1.197}$$

$$\begin{aligned}\mathrm{tr}(Y) &= -\frac{1}{8}\sum_i \frac{(\partial_\theta p_i)^2}{p_i} - \frac{1}{2}\sum_i p_i\,\langle\partial_\theta\psi_i|\partial_\theta\psi_i\rangle + \sum_{i,j}\frac{2p_i p_j^2}{(p_i + p_j)^2}|\,\langle\psi_i|\partial_\theta\psi_j\rangle\,|^2 \\ &= -\frac{1}{8}\left\{\sum_i \frac{(\partial_\theta p_i)^2}{p_i} + 4\sum_{i,j}\left[p_j - \frac{2p_i p_j}{p_i + p_j}\right]|\,\langle\psi_i|\partial_\theta\psi_j\rangle\,|^2\right\} \\ &= -\frac{1}{8}\left\{\sum_i \frac{(\partial_\theta p_i)^2}{p_i} + 4\sum_{i,j}\frac{p_i(p_i - p_j)^2}{(p_i + p_j)^2}|\,\langle\psi_i|\partial_\theta\psi_j\rangle\,|^2\right\},\end{aligned} \tag{1.1.198}$$

where we used that

- $(\partial_\theta \varrho)_{ij}(\partial_\theta \varrho)_{ji} = (\partial_\theta p_i)^2 \delta_{ij} + (p_i - p_j)^2 |\langle \psi_i | \partial_\theta \psi_j \rangle|^2$,
- $\langle \psi_i | \partial_\theta^2 \psi_i \rangle + \langle \partial_\theta^2 \psi_i | \psi_i \rangle = -2 \langle \partial_\theta \psi_i | \partial_\theta \psi_i \rangle$,
- $\sum_{i,j} [2 p_i p_j^2 / (p_i + p_j)^2] |\langle \psi_i | \partial_\theta \psi_j \rangle|^2 = \sum_{i,j} [p_i p_j / (p_i + p_j)] |\langle \psi_i | \partial_\theta \psi_j \rangle|^2$.

Finally, we can arrive at:

$$\begin{aligned} D_B^2[\varrho(\theta), \varrho(\theta + d\theta)] &= 2(1 - F[\varrho(\theta), \varrho(\theta + d\theta)]) \\ &= 2[1 - \mathrm{tr}(\sqrt{M})] \\ &= 2\left\{1 - [1 + (d\theta)\mathrm{tr}(X) + (d\theta)^2 \mathrm{tr}(Y)]\right\} \\ &= \frac{1}{4} \mathcal{F}_Q(\theta) (d\theta)^2, \end{aligned} \tag{1.1.199}$$

where the quantum Fisher metric is defined as

$$\begin{aligned} \mathcal{F}_Q(\theta) &= \sum_i \frac{(\partial_\theta p_i)^2}{p_i} + 4 \sum_{i,j} \frac{p_i (p_i - p_j)^2}{(p_i + p_j)^2} |\langle \psi_i | \partial_\theta \psi_j \rangle|^2 \\ &= \sum_{i,j} \frac{4 p_i |(\partial_\theta \varrho)_{ij}|^2}{(p_i + p_j)^2} = 2 \sum_{i,j} \frac{|(\partial_\theta \varrho)_{ij}|^2}{p_i + p_j}. \end{aligned} \tag{1.1.200}$$

□

Quantum Fisher information (QFI): Consider the case where the initial state is independent of the parameter θ and the time evolution is unitary $U_\theta = \exp(-i\theta A)$: $\varrho(0) \to \varrho(\theta) = U_\theta \varrho(0) U_\theta^\dagger$. Then the first term in the quantum Fisher metric in Eq.(1.1.200) vanishes and the QFI can be simplified to

$$\mathcal{F}_Q(\varrho, A) = 2 \sum_{i,j} \frac{(p_i - p_j)^2}{p_i + p_j} |\langle \psi_i | A | \psi_j \rangle|^2. \tag{1.1.201}$$

This quantity is often called the quantum Fisher information (QFI), which can characterize how much a state ϱ is sensitive against the parameter shifting θ by the unitary transformation. The QFI plays an important role in quantum metrology, for details see Sec. 1.3. Note that the term QFI can also be used outside of the unitary case.

Uncertainty relations: Suppose that we perform measurements of an observable A on a quantum state ϱ. As explained in Sec. 1.1.3, the expectation is given by $\langle A \rangle_\varrho = \mathrm{tr}(\varrho A)$. Here we introduce the variance as

$$(\Delta A)_\varrho^2 = \langle (A - \langle A \rangle_\varrho)^2 \rangle_\varrho = \langle A^2 \rangle_\varrho - \langle A \rangle_\varrho^2, \tag{1.1.202}$$

where hereafter we take out the subscript ϱ. This implies a variation in the measurement outcome of the observable A. For two observables A, B, the well-known Kennard-Robertson inequality states that

$$(\Delta A)^2 (\Delta B)^2 \geq \frac{1}{4} |\langle [A, B] \rangle|^2. \tag{1.1.203}$$

This inequality can be understood as follows: In the case where one prepares N copies of ϱ and measures A with $N/2$ particles and B with $N/2$ particles, if the variance of A is small, then the variance of B should be large, and vice versa. For details about uncertainty relations, see [18, 95].

Quantum speed limits: How fast can a quantum state evolve in time? This question asks about the ultimate limit of time evolution in quantum mechanics. Often this limitation is referred to as the quantum speed limit. Historically, this was addressed by Mandelstam and Tamm in Ref. [96], and later Margolus and Levitin made another formulation Ref. [97]. Here we will explain the description of the work by Mandelstam and Tamm, following the description of Ref. [98].

Let us begin by considering the projector $A = \Pi_0 = |\psi_0\rangle\langle\psi_0| = A^2$, the Hamiltonian $B = H$, and the state $\varrho = |\psi_t\rangle\langle\psi_t|$ with $|\psi_t\rangle = e^{-iHt/\hbar} |\psi_0\rangle$. Letting $\langle X \rangle_t = \langle \psi_t | X | \psi_t \rangle$ for $X = A, B$, we have that $(\Delta A)_t^2 = \langle A \rangle_t (1 - \langle A \rangle_t)$ and $|\langle [A, B] \rangle_t| = \hbar |\partial_t \langle A \rangle_t|$. Inserting this into the Kennard-Robertson inequality leads to

$$(\Delta H) \geq \frac{\hbar}{2} \frac{|\partial_t \langle A \rangle_t|}{\sqrt{\langle A \rangle_t (1 - \langle A \rangle_t)}}. \tag{1.1.204}$$

Taking a time integral from 0 to Δt and assuming that $|\psi_{\Delta t}\rangle$ is orthogonal to $|\psi_0\rangle$, one can straightforwardly derive the so-called Mandelstam-Tamm bound:

$$\Delta t \geq \frac{\pi \hbar}{2(\Delta H)} \equiv \tau_{\mathrm{QSL}}. \tag{1.1.205}$$

Note that Δt is a physical time scale. An interpretation of this bound is as follows: A larger energy variance implies the fast time evolution of a quantum state, and the minimal time is given by $\tau_{\mathrm{QSL}} = \pi \hbar / 2(\Delta H)$.

The Mandelstam-Tamm bound can be understood from the geometrical viewpoint. Denote γ as the actual trajectory path that the initial state $|\psi_0\rangle$ takes to its orthogonal state $|\psi_{\Delta t}\rangle$. For a qubit system, this can be understood as a path on the surface of the Bloch sphere. The length of the path γ can be described using the Bures distance in Eq. (1.1.187):

$$\gamma = \int_0^{\Delta t} ds \sqrt{g_{\mathrm{FS}}}, \tag{1.1.206}$$

with Fubini-Study metric g_{FS}. Due to the triangle inequality, the path γ can be larger than or equal to the (minimal) shortest path denoted as $\mathcal{L}(|\psi_0\rangle, |\psi_{\Delta t}\rangle)$.

Letting the speed $v = \sqrt{g_{\mathrm{FS}}}$ and its the time-average $\langle v \rangle_{\Delta t} = (1/\Delta t) \int_0^{\Delta t} ds\, v$, it holds that

$$\Delta t \geq \frac{\mathcal{L}(|\psi_0\rangle, |\psi_{\Delta t}\rangle)}{\langle v \rangle_{\Delta t}}. \tag{1.1.207}$$

This results in the fact that $\Delta t = \tau_{\mathrm{QSL}}$ if and only if $\mathcal{L}(|\psi_0\rangle, |\psi_{\Delta t}\rangle)$ is the shortest, that is, geodesic. We remark that for mixed states, instead of the Fubini-Study metric g_{FS}, the quantum Fisher metric can be considered. For details about quantum speed limits, see [98, 99].

Reference frames: Here let us briefly explain the concept of quantum reference frames, following the description of Ref. [100]. Any information, whether classical or quantum, can be classified into two types. The first type is known as speakable (fungible) information, which can be described independently of its encoding/decoding within any physical system and with any degree of freedom. Examples of speakable information include simple communication using 'yes' or 'no,' or classical bits represented as '0' or '1.' On the other hand, the second type is unspeakable (non-fungible) information, which cannot be communicated verbally and relies on a physical system for its description. Examples of unspeakable information include spatial direction, spin rotation, or timing of an event. The concept of a reference frame serves as an abstract coordinate system to transform unspoken information into speakable information, similar to the way gyroscopes and clocks work.

In quantum mechanics, a system possessing a reference frame can be converted to another system with a different reference frame through a transformation involving an element denoted as $g \in G$. Typically, G represents a finite, continuous, compact Lie group with a group-invariant (Haar unitary) measure. For instance, a phase reference in the group $\mathrm{U}(1)$ involves phase shifts, while a Cartesian frame in $\mathrm{SO}(3)$ is represented by the group $\mathrm{SU}(2)$, corresponding to spin rotations.

In this thesis, we will frequently employ the notion of a reference frame based on the group $\mathrm{SU}(d)$ for a d-dimensional state. It is essential to note that aligning local reference frames between parties can be considered a quantum resource in information processing tasks [101]. Consequently, reference frame-independent measurement schemes (the randomized measurement schemes that we will discuss later) can offer many practical advantages in the analysis of quantum states compared to standard techniques.

1.1.7 Mathematical tools

In this subsection, we will give a summary of useful mathematical formulas. For details about further formulas and inequalities, see Refs. [102–104]. For details about Haar unitary integrals, see Sec. 1.5 and Chapter 9.

Trace formuals

- The Cauchy-Schwarz inequality:

$$|\mathrm{tr}(A^\dagger B)|^2 \leq \mathrm{tr}(A^\dagger A)\mathrm{tr}(B^\dagger B), \tag{1.1.208}$$

  for matrices A, B.

- The von Neumann inequality:

$$|\mathrm{tr}(AB)| \leq \sum_i a_i b_i, \tag{1.1.209}$$

  where a_i and b_i are respectively singular values of matrices A and B with $a_1 \geq a_2 \geq \cdots$ and $b_1 \geq b_2 \geq \cdots$.

- For Hermitian A and $n \geq 2$, it holds that $|\mathrm{tr}(X^n)| \leq [\mathrm{tr}(X^2)]^{n/2}$.

- For Hermitian A, B, it holds that $\mathrm{tr}(ABAB) \leq \mathrm{tr}(A^2B^2)$. This comes from the fact that $\mathrm{tr}(X^2) \geq 0$ for $X = AB - BA$.

- For a positive A and $n \geq 1$, it holds that $\mathrm{tr}(A^n) \leq [\mathrm{tr}(A)]^n$.

- For positive A and B, it holds that $\mathrm{tr}(AB) \geq 0$.

- The inequalities of the harmonic mean, geometric mean, arithmetic mean, and quadratic mean: for a positive A, it holds that

$$\frac{n}{[\mathrm{tr}(A^{-1})]} \leq (\det A)^{1/n} \leq \frac{1}{n}\mathrm{tr}(A) \leq \sqrt{\frac{1}{n}\mathrm{tr}(A^2)} \tag{1.1.210}$$

- For a positive A with $\mathrm{tr}(A) = 1$, it holds that

$$[\mathrm{tr}(A^2)]^2 \leq \mathrm{tr}(A^3), \tag{1.1.211}$$

  which was introduced in [105].

- $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B)$ and $\mathrm{tr}(A^{\otimes n}) = [\mathrm{tr}(A)]^n$.

SWAP formulas

- The SWAP operator $\mathbb{S}$ in Eq. (1.1.120) can be also rewritten as

$$\mathbb{S} = \frac{1}{d}\sum_{i=0}^{d^2-1} \lambda_i \otimes \lambda_i, \tag{1.1.212}$$

  where λ_i are the Gell-Mann matrices discussed in Subsection (1.1.1).

- Since $\mathbb{S}^2 = \mathbb{1}_d$, this leads to the formula

$$\sum_{i=1}^{d^2-1} \lambda_i^2 = (d^2-1)\mathbb{1}_d. \tag{1.1.213}$$

- For the structure constants of Gell-Mann matrices in Eq. (1.1.23), it holds that

$$\sum_{i,j=1}^{d^2-1} \eta^S_{ijk}\eta^S_{ijm} = 2(d^2-4)\delta_{km}, \qquad \sum_{i,j=1}^{d^2-1} \eta^A_{ijk}\eta^A_{ijm} = 2d^2\delta_{km}. \tag{1.1.214}$$

  For details, see [106].

- The SWAP operator $\mathbb{S}$ can be also rewritten as

$$\mathbb{S} = d\,|\Psi^+\rangle\langle\Psi^+|^{\top_A}, \tag{1.1.215}$$

  where $|\Psi^+\rangle = (1/\sqrt{d})\sum_{i=0}^{d-1}|i\rangle\otimes|i\rangle$ and $(\cdot)^\top_A$ denotes the partial transposition on A.

- For $X = (x_1, x_2, \cdots, x_n)$ and $Y = (y_1, y_2, \cdots, y_n)$, the SWAP $\mathbb{S}_{XY}$ can be decomposed into

$$\mathbb{S}_{X,Y} = \mathbb{S}_{x_1,y_1}\otimes\mathbb{S}_{x_2,y_2}\otimes\cdots\otimes\mathbb{S}_{x_n,y_n}, \tag{1.1.216}$$

  which was discussed in [107].

- For matrices A, B, the following is often called the SWAP trick:

$$\mathrm{tr}[(A\otimes B)\mathbb{S}] = \mathrm{tr}(AB). \tag{1.1.217}$$

  Also it holds that

$$\mathrm{tr}_2[(A\otimes B)\mathbb{S}] = AB, \qquad \mathrm{tr}_1[(A\otimes B)\mathbb{S}] = BA, \tag{1.1.218}$$
$$\mathrm{tr}_2[\mathbb{S}(A\otimes B)] = BA, \qquad \mathrm{tr}_1[\mathbb{S}(A\otimes B)] = AB. \tag{1.1.219}$$

  For details, see [27].

- For states ϱ and σ, it holds that

$$\mathrm{tr}_1[e^{-it\mathbb{S}}(\varrho\otimes\sigma)e^{it\mathbb{S}}] = (\cos^2 t)\sigma + (\sin^2 t)\varrho - i(\sin t)(\varrho\sigma - \sigma\varrho), \tag{1.1.220}$$

  which was introduced in [108].

- The cyclic operator $W_{\mathrm{cyc}} \in \mathcal{H}_d^{\otimes k}$ in Eq. (1.1.124) can be written as

$$W_{\mathrm{cyc}} = \frac{1}{d^{k-1}} \sum_{i_1,i_2,\ldots,i_{k-1}=1}^{d^2-1} \lambda_{i_1}\otimes\lambda_{i_2}\otimes\cdots\otimes\lambda_{i_{k-1}}\otimes\nu^\dagger \tag{1.1.221}$$

  with $\nu = \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_{k-1}}$, which was explicitly written in Ref. [109]. The cyclic operator can be decomposed into $k-1$ pairwise SWAP operators, see Refs. [107, 110, 111].

- Consider the other cyclic operator W_{inv} as

$$W_{\text{inv}} |i_1, i_2, \ldots, i_k\rangle = |i_k, i_1, \ldots, i_{k-1}\rangle . \tag{1.1.222}$$

  Then it holds that $W_{\text{inv}} = W_{\text{cyc}}^{-1} = W_{\text{cyc}}^{\top}$.

- Let W_{cyc}^X be the cyclic operator with $W_{\text{cyc}}^X |i,j,k\rangle_X = |j,k,i\rangle_X$ acting on the subsystem $X = A, B$ of the three copies. Then it holds that

$$2\left(W_{\text{cyc}}^A \otimes W_{\text{inv}}^B + W_{\text{inv}}^A \otimes W_{\text{cyc}}^B\right) = M_+^A \otimes M_+^B - M_-^A \otimes M_-^B, \tag{1.1.223}$$

  where $M_{\pm}^X = W_{\text{cyc}}^X \pm W_{\text{inv}}^X$ for $X = A, B$. For details, see [112].

- For matrices $A_1, A_2, \ldots, A_k$, the generalization of the SWAP trick is given by

$$\text{tr}[(A_1 \otimes A_2 \otimes \cdots \otimes A_k) W_{\text{cyc}}] = \text{tr}(A_1 A_2 \ldots A_k). \tag{1.1.224}$$

  For details, see [107, 113–115].

Other useful formulas

- Consider a set of observables $\{A_i\}_{i=1}^n$ such that $A_i A_j + A_j A_i = 0$ and $A_i^2 = \mathbb{1}$ for all $i, j = 1, 2, \ldots, n$, that is, the A_i anti-commute pairwise and have ± 1 eigenvalues. For this set, it holds that $\sum_{i=1}^n \langle A_i \rangle_\varrho^2 \leq 1$ for a quantum state ϱ. For details, see Ref. [116].

- For real x, y, it holds that

$$\max(x,y) = \frac{x+y}{2} + \frac{|x-y|}{2} \qquad \min(x,y) = \frac{x+y}{2} - \frac{|x-y|}{2}. \tag{1.1.225}$$

- For real x, y, it holds that $|x+y| \leq |x| + |y|$ and $||x| - |y|| \leq |x-y|$.

- Baker–Campbell–Hausdorff formula:

$$e^A B e^{-A} = B + [A,B] + \frac{1}{2!}[A,[A,B]] + \frac{1}{3!}[A,[A,[A,B]]] + \cdots . \tag{1.1.226}$$

  For details, see [117].

1.2 Quantum entanglement

In this section, we will give a brief introduction to quantum entanglement. In the theory of quantum entanglement, the major interest may be its detection and quantification. This section describes each of the basic concepts which are necessary to understand this thesis. For more general introductions to quantum entanglement, see [17, 60, 118–123].

1.2.1 Bipartite entanglement

Definitions: A pure bipartite quantum state $|\psi\rangle_{AB}$ is called a product state if it can be written in the product form

$$|\psi\rangle_{\text{prod}} = |a\rangle \otimes |b\rangle \,. \tag{1.2.1}$$

A state is called entangled if it cannot be written in any product form. For example, a two-qubit product state is given by $|0\rangle \otimes |0\rangle = |00\rangle$, while a two-qubit entangled state is given by

$$|\psi\rangle_{\text{ent}} = (|00\rangle + |11\rangle)/\sqrt{2}. \tag{1.2.2}$$

In practice, quantum states cannot be often assumed to be pure due to noise effects, so we next define entanglement in mixed states.

A mixed state ϱ_{AB} is called separable if it can be written as

$$\varrho_{\text{sep}} = \sum_i p_i \varrho_i^A \otimes \varrho_i^B, \tag{1.2.3}$$

where ϱ_i^A, ϱ_i^B are quantum states and p_i is the probability with $p_i \in [0,1]$ and $\sum_i p_i = 1$. Note that the set of separable states is compact and convex. A state is entangled if it cannot be written in the separable form. An example of two-qubit mixed states is given by

$$\varrho(p) = p\,|\psi\rangle\langle\psi|_{\text{ent}} + \frac{1-p}{4}\mathbb{1}_2^{\otimes 2}. \tag{1.2.4}$$

For $p = 1$ this is the entangled state, while for $p = 0$ it is the maximally mixed state (separable state). A natural question arises: What is the transition point p between entanglement and separability? In Sec. 1.2.3, we will address this question.

High-dimensional entanglement: Consider a $d \otimes d$-dimensional pure quantum state $|\psi\rangle_{AB}$. According to the so-called Schmidt decomposition, any $|\psi\rangle_{AB}$ can be written as follows, up to local unitaries:

$$|\psi\rangle_{AB} = \sum_{i=1}^{r} \sqrt{\lambda_i}\,|e_i\rangle \otimes |f_i\rangle \,, \tag{1.2.5}$$

with $\langle e_i|e_j\rangle = \langle f_i|f_j\rangle = \delta_{ij}$ and $\sum_{i=1}^{r}\lambda_i = 1$. The number $r = r(\psi_{AB})$ is called the Schmidt rank, which is equal to the rank of the reduced state $\varrho_X = \mathrm{tr}_{X^c}(|\psi\rangle\langle\psi|_{AB})$ for $X = A, B$. The state $|\psi\rangle_{AB}$ is separable if and only if $r = 1$, while it is entangled if and only if $r > 1$. In particular, the entanglement with $r \gg 2$ is often called high-dimensional entanglement. Note that $1 \leq r \leq d$.

The generalization of the Schmidt rank to mixed states ϱ_{AB} is known as the Schmidt number:

$$\mathrm{SN}(\varrho_{AB}) = \min_{\{p_i,\psi_i\}} \max_{\{\psi_i\}} r(\psi_i), \tag{1.2.6}$$

where $\{p_i, \psi_i\} = \{p_i, \psi_i : \varrho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|\}$ is the set of all ensemble realizations of ϱ_{AB}. The sets $\mathcal{S}_k$ of all bipartite states with $\mathrm{SN} \leq k$ form a hierarchy of convex and compact subsets in state space, $\mathcal{S}_k \subset \mathcal{S}_{k+1}$, (the structure of Russian dolls), where $\mathcal{S}_1$ is the set of separable states. For details about Schmidt number, see [124].

Maximal entanglement: Consider the Schmidt decomposition of $|\psi\rangle_{AB} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B$. A pure state is called maximally entangled if its $\sqrt{\lambda_i} = 1/\sqrt{d}$, that is,

$$|\psi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle\,, \tag{1.2.7}$$

where $|ii\rangle = |i\rangle \otimes |i\rangle$. Here, we express the basis using the computational bases. Since the Schmidt decomposition has the form up to local unitary, the maximally entangled state is not uniquely determined.

For $d = 2$, we have four orthonormal bases of maximally entangled states. Commonly, they are called the Bell states:

$$|\Phi^\pm\rangle = \frac{1}{2}\left(|00\rangle \pm |11\rangle\right), \qquad |\Psi^\pm\rangle = \frac{1}{2}\left(|01\rangle \pm |10\rangle\right). \tag{1.2.8}$$

Note that the convex combination of these four Bell states are called the Bell-diagonal states defined in Eq. (1.1.137).

Another definition of the maximally entangled states is as follows: A pure state is maximally entangled if its reduced states are maximally mixed, that is,

$$\varrho_X = \mathrm{tr}_{X^c}(|\psi\rangle\langle\psi|_{AB}) = \frac{\mathbb{1}_d}{d}, \tag{1.2.9}$$

for $X = A, B$. That is, the purity of the reduced state is given by $\gamma(\varrho_X) = 1/d$.

Operational definition: A state is called separable if it can be created by LOCC operations $\Phi_{\mathrm{LOCC}}(\varrho)$ given in Eq. (1.1.126). On the other hand, the state is called entangled if it cannot be created by LOCC operations. We note that entangled states can be created by non-LOCC operations, while all non-LOCC operations (all nonlocal operations) cannot always create entanglement. For instance, the SWAP operation $\mathbb{S}$ defined in Eq. (1.1.119) is one of the nonlocal operations but it cannot create entanglement for a product state $|00\rangle$.

On the operational side, the maximally entangled state is known as a state that can create any bipartite quantum state using LOCC operations. This is based on the concept of majorization, which plays an important role in the resource theory [125, 126]. That is, the maximally entangled state can be recognized as a quantum state that has maximally useful resource for state generation.

Quantum teleportation: Here we discuss the usefulness of entanglement in information-processing tasks. Consider a situation where Alice and Bob are spatially separated and they share a two-qubit entangled state, say the Bell state $|\Phi^+\rangle_{AB}$ defined in Eq. (1.2.8). Suppose that Alice has another unknown single-qubit state in subsystem A' and Alice wants to send this state to Bob. Here assume that Alice does not know the state, that is, Alice does not know the parameters α, β for $|\psi\rangle_{A'} = \alpha |0\rangle_{A'} + \beta |1\rangle_{A'}$. Now the total state is a three-qubit state and given by: $|\Phi^+\rangle_{AB} \otimes |\psi\rangle_{A'}$.

Quantum teleportation is a protocol allowing Alice to teleport the state in the system A' to the state in system B by performing measurements for the basis of Bell states in Eq. (1.2.8) on the system A and A'. More precisely, consider the measurement basis $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}_{AA'}$ in Eq. (1.2.8). Then the straightforward calculation leads to

$$(|\Phi^\pm\rangle\langle\Phi^\pm|_{AA'} \otimes \mathbb{1}_B) |\Phi^+\rangle_{AB} \otimes |\psi\rangle_{A'} = \frac{1}{2} |\Phi^\pm\rangle_{AA'} \otimes |\psi^\pm\rangle_B , \tag{1.2.10}$$

$$(|\Psi^\pm\rangle\langle\Psi^\pm|_{AA'} \otimes \mathbb{1}_B) |\Phi^+\rangle_{AB} \otimes |\psi\rangle_{A'} = \frac{1}{2} |\Psi^\pm\rangle_{AA'} \otimes |\phi^\pm\rangle_B , \tag{1.2.11}$$

where $|\psi^\pm\rangle_B = \alpha |0\rangle_B \pm \beta |1\rangle_B$ and $|\phi^\pm\rangle_B = \alpha |1\rangle_B \pm \beta |0\rangle_B$. According to the measurement rule, the probability to obtain the outcome can be computed by the squared norm of the post-measurement state. Then Alice can find either of $|\Phi^\pm\rangle, |\Psi^\pm\rangle$ with probability $1/4$.

Clearly, Bob does not know the result that Alice obtained from the measurement. So, Alice has to tell the message about the two-bit result to Bob. Depending on the result, Bob performs a local operation with the unitary Pauli operation $U = \sigma_i$ to Bob's state for $i = 0, 1, 2, 3$. Then Bob can obtain the state $|\psi\rangle_B$ that is the same as the state in Alice's system A' at the beginning. This means that Alice teleported the state $|\psi\rangle_{A'}$ to Bob.

In the following, we make several remarks, for details see [127, 128].

- Typical misconceptions:

  Quantum teleportation does not occur faster than the speed of light. This is because Alice has to send the measurement result to Bob classically via telephone or other ways.

  Quantum teleportation does not teleport actual physical objects. It teleports quantum information as unknown coefficients of superposition.

  Quantum teleportation does not mean copying/cloning an unknown state. In fact, this is consistent with the so-called no-cloning theorem, stating that an arbitrary unknown quantum state cannot be copied/cloned [129, 130].

- Entanglement swapping: Quantum teleportation transfers an unknown state but destroys the initial entanglement. More precisely, it swaps the entangled state on system AB to the one on AA'.

- Generalizations: Quantum teleportation can be possible even if an initial entangled state on system AB is not the Bell state, that is, not necessarily maximally entangled. Also, it can be generalized to high-dimensional cases. For details, see [131] and Eq. (1.2.60).

- Experiments: Quantum teleportation has been realized experimentally [132, 133] and also the ground-to-satellite demonstration has been conducted over distances of 1,400 kilometers [134].

1.2.2 Multipartite entanglement

Genuine tripartite entanglement: Consider a three-particle state $|\psi\rangle_{ABC}$. A state is called fully separable if

$$|\psi\rangle_{\text{fs}} = |a\rangle \otimes |b\rangle \otimes |c\rangle \,. \tag{1.2.12}$$

A three-qubit example is given by $|000\rangle$. If the state is not fully separable, then it is entangled. For instance, a state is called biseparable for a bipartition $A|BC$ if

$$|\psi\rangle_{A|BC} = |\phi\rangle_A \otimes |\phi\rangle_{BC} \,. \tag{1.2.13}$$

Here the state $|\phi\rangle_{BC} \in \mathcal{H}_d^B \otimes \mathcal{H}_d^C$ may be entangled, but the total state is separated with respect to A versus BC. A three-qubit example is $|0\rangle \otimes |\Phi^+\rangle$ with the Bell state $|\Phi^+\rangle$. Similarly, we can define the biseparable states for bipartitions $B|CA$ and $C|AB$. A state is called genuine tripartite entangled if it cannot be written in any biseparable form. Typical examples of genuine three-qubit entangled states: the so-called Greenberger–Horne–Zeilinger (GHZ) state and W state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right), \tag{1.2.14}$$

$$|\text{W}\rangle = \frac{1}{\sqrt{3}} \left(|001\rangle + |010\rangle + |100\rangle\right). \tag{1.2.15}$$

Consider a mixed quantum state $\varrho_{ABC} \in \mathcal{H}_d^A \otimes \mathcal{H}_d^B \otimes \mathcal{H}_d^C$. A state is called fully separable if

$$\varrho_{\text{fs}} = \sum_i p_i \varrho_i^A \otimes \varrho_i^B \otimes \varrho_i^C, \tag{1.2.16}$$

where the p_i form a probability distribution. Also, a state is called biseparable for a bipartition $A|BC$ if

$$\varrho_{A|BC} = \sum_i q_i^A \varrho_i^A \otimes \varrho_i^{BC}, \tag{1.2.17}$$

where the q_i^A form a probability distribution and ϱ_i^{BC} may be entangled. Similarly, one can define biseparable states with respect to the two other bipartitions as $B|CA$ and $C|AB$. Moreover, one can define mixtures of biseparable states with respect to different partitions, i.e., states of the form

$$\varrho_{\text{bs}} = p_A \varrho_{A|BC} + p_B \varrho_{B|CA} + p_C \varrho_{C|AB}, \tag{1.2.18}$$

where the p_A, p_B, p_C form convex weights. A mixed state is called genuine tripartite entangled if it cannot be written in the form of ϱ_{bs}. A typical example of three-qubit mixed states is given by

$$\varrho(g,w) = g\varrho_{\text{GHZ}} + w\varrho_{\text{W}} + \frac{1-g-w}{8}\mathbb{1}_2^{\otimes 3}, \tag{1.2.19}$$

where $0 \leq g, w \leq 1$ and $\varrho_{\text{GHZ}} = |\text{GHZ}\rangle\langle\text{GHZ}|$ and $\varrho_{\text{W}} = |\text{W}\rangle\langle\text{W}|$. In Chapter 2, we will discuss the detailed analysis of the state $\varrho(g,w)$.

Difference between GHZ and W states: There are several differences between the three-qubit GHZ and W states. First, their reduced states are different. That is,

$$\varrho_{XY}^{\text{GHZ}} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \varrho_X^{\text{GHZ}} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{1.2.20}$$

$$\varrho_{XY}^{\text{W}} = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \varrho_X^{\text{W}} = \frac{1}{3}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \tag{1.2.21}$$

where $\varrho_{XY} = \text{tr}_Z(\varrho)$ and $\varrho_X = \text{tr}_{YZ}(\varrho)$ are respectively two-qubit and single-qubit states for any $X, Y, Z = A, B, C$. In fact, $\varrho_{XY}^{\text{GHZ}}$ is separable but ϱ_{XY}^{W} is entangled. This implies that the entanglement of the GHZ state is sensitive to particle losses, while the entanglement of the W state is robust.

Genuine N-partite entanglement: Consider a N-particle state ϱ. A state is fully separable if

$$\varrho_{\text{fs}} = \sum_i p_i \varrho_i^1 \otimes \varrho_i^2 \otimes \cdots \varrho_i^N, \tag{1.2.22}$$

where p_i forms the probability distribution. A state is called biseparable for a bipartition $M|\bar{M}$ for $M = \{1, 2, \ldots, N\}$ if

$$\varrho_{M|\bar{M}} = \sum_i q_i^M \varrho_i^M \otimes \varrho_i^{\bar{M}}, \tag{1.2.23}$$

where p_i^M forms the probability distribution and $\bar{M}$ is the complement of M. In a similar manner to the three-particle case, one can define mixtures of biseparable states for all bipartitions:

$$\varrho_{\text{bs}} = \sum_M p_M \varrho_{M|\bar{M}}, \tag{1.2.24}$$

where this summation includes at most $2^{N-1}-1$ terms. A state is called genuine N-partite entangled if it cannot be written the form of ϱ_{bs}. As an example, the N-qudit GHZ state can be given by

$$|\text{GHZ}(N,d)\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N}. \tag{1.2.25}$$

For $d=2$, this is equivalent to the maximally entangled state $|\psi^+\rangle$ in Eq. (1.2.7).

k-separability: Let us discuss another different form of multiparticle entanglement. The idea is to extend the concept of fully separability to k-separability (or k-partitionability) by taking into account the number of separable partitions. For a N-particle state $|\psi\rangle \in \mathcal{H}_d^{\otimes N}$, a state is k-separable if it can be written as

$$|\psi_{k\text{-sep}}\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_k\rangle. \tag{1.2.26}$$

The mixed state can be also defined using the convex mixture of pure k-separable states. Here for $k=N$, this is equivalent to the full separability. If a state is not 2-separable, then it is called genuinely N-particle entangled. For example, the following state is 100-qubit 12-separable:

$$|\psi_{100,12}\rangle = |\text{GHZ}_{20}\rangle^{\otimes 3} \otimes |\text{GHZ}_{10}\rangle^{\otimes 2} \otimes |\text{GHZ}_5\rangle^{\otimes 2} \otimes |\Phi^+\rangle^{\otimes 5}, \tag{1.2.27}$$

where we denote that $|\text{GHZ}_N\rangle = |\text{GHZ}(N,2)\rangle$ in Eq. (1.2.25).

GHZ and W states: Consider a N-qubit GHZ state and W state

$$|\text{GHZ}_N\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N} \right), \tag{1.2.28}$$

$$|\text{W}_N\rangle = \frac{1}{\sqrt{N}} \left(|100\ldots0\rangle + |010\ldots0\rangle \cdots + |00\ldots01\rangle \right). \tag{1.2.29}$$

Let us take a partial trace over the subsystem 1. Then their reduced states are given by

$$\text{tr}_1[|\text{GHZ}_N\rangle\langle\text{GHZ}_N|] = \frac{1}{2} \left(|0\rangle\langle 0|^{\otimes(N-1)} + |1\rangle\langle 1|^{\otimes(N-1)} \right), \tag{1.2.30}$$

$$\text{tr}_1[|\text{W}_N\rangle\langle\text{W}_N|] = \frac{1}{N} |0\rangle\langle 0|^{\otimes(N-1)} + \frac{N-1}{N} |\text{W}_{N-1}\rangle\langle\text{W}_{N-1}|. \tag{1.2.31}$$

As a result, we can see that the reduced state of the GHZ state is separable but the reduced state of the W state is entangled, similarly with the result in the three-qubit case. That is, the entanglement of the GHZ state is fragile under the loss of a particle, while the entanglement of the W state is robust.

Dicke states: For a N-qubit system, the Dicke state with m excitations is defined as

$$|D_{N,m}\rangle = \binom{N}{m}^{-\frac{1}{2}} \sum_k \pi_k \left(|1\rangle^{\otimes m} \otimes |0\rangle^{\otimes (N-m)} \right), \tag{1.2.32}$$

where the summation in $\sum_k \pi_k$ is overall different permutations between the qubits and integer m with $0 \leq m \leq N$.

There are three remarks. First, the Dicke state can be the generalization of the W state in Eq. (1.2.29): $|D_{N,1}\rangle = |W_N\rangle$. Second, the two-qubit reduced states are given by

$$\varrho_{N,m}^{(2)} = \frac{1}{N(N-1)} \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & b & 0 \\ 0 & b & b & 0 \\ 0 & 0 & 0 & c \end{pmatrix}, \tag{1.2.33}$$

where $\varrho_{N,m}^{(2)} = \mathrm{tr}_{\{1,2,\ldots,N\}/\{a,b\}}(|D_{N,m}\rangle\langle D_{N,m}|)$ for any $a, b = 1, 2, \cdots, N$ with $a + 2b + c = N(N-1)$, $a = (N-m)(N-m-1), b = m(N-m)$, and $c = m(m-1)$. For $N = 3$ and $m = 1$, this state coincides with Eq. (1.2.21). In fact, the reduced state $\varrho_{N,m}^{(2)}$ is entangled for any $N \geq 3$ and $m \in [1, N-1]$ (this can be checked using the so-called PPT criterion, which will be explained in the next subsection). Third, the Dicke state is one of the so-called spin-squeezed states, which have metrologically important meanings. For details about Dicke states, see [135] and Sec. 1.3.

Multipartite maximal entanglement: In multipartite systems, the structure of entanglement becomes much richer and more complicated than in bipartite systems. In the state space of a bipartite system, there is an ordering structure in terms of quantum resource theories [101]. In this sense, the maximally entangled state can be defined as an entangled state in which any bipartite state can be created by LOCC operations.

On the other hand, in multipartite systems, such an ordering structure no longer exists, and the concept of maximally entangled states cannot be uniquely defined. In fact, three-qubit pure states are divided into two classes: the GHZ class and the W class. As mentioned already, the GHZ state cannot be transformed to the W state and vice versa with LOCC operations, even if they are not required to reach the state with probability one SLOCC operations in Eq. (1.1.130) [136, 137]. This distinction leads to different roles the GME states play in information processing tasks [138–140]. For four-qubit states, there is already an infinite collection of such classes, which can be grouped into nine families [141].

In addition to the GHZ state and Dicke state, several notions of genuinely multipartite entanglement were discussed. Examples are cluster states [142], graph states [143], hypergraph states [144], absolutely maximally entangled states [145, 146], phased Dicke states [147–152], singlet states (1.3.23), and totally antisymmetric states (1.3.30).

1.2.3 Entanglement detection

Separability problem: The separability problem is as follows: Given a quantum state, is it separable or entangled? There are many studies to address this question, but still, the general solution is unknown. Here we summarize several issues about the separability problem.

- Complexity: In general, determining whether a state is entangled is a complicated mathematical problem, even if the density matrix is completely known. In fact, the separability problem is known to belong to the NP-hard class of computational complexity [153].

- Practical issues: In the case of pure states, the separability problem is rather straightforward, but the situation becomes much more complicated when mixed states are considered. In practical scenarios, quantum states created in a lab are mixed due to the irreducible presence of noise, lack of experimental control, and environmental decoherence. Moreover, large quantum states may not be completely analyzed due to the exponentially increasing dimension of the Hilbert space, and then their density matrices are supposed to be unknown. Therefore, it is desirable to find efficient experimental methods to estimate the entanglement of such imperfect and unknown states.

- Limited quantum control: In experiments, sometimes only partial information about the state is accessible. If some a priori information about the state is available, such as that an experiment is aimed at producing a certain entangled state, then so-called entanglement witnesses may allow for efficient detection using directly measurable observables [154, 155], which will be explained in this section. In other situations where one cannot be sure about the appropriate description of measurements and cannot trust the underlying quantum devices, it is still possible to certify entanglement in a device-independent manner [156], using, e.g. Bell-type inequalities, based only on the measurement data observed from input-output statistics [157, 158]. Moreover, when considering ensembles of quantum particles, such as cold atoms, individual control over local subsystems may be lost, but entanglement can still be characterized by measuring collective angular momenta and applying spin-squeezing inequalities [159–161], which will be explained in Sec. 1.3.

- Meaningful entanglement: Addressing the separability problem can highlight the differences in correlations between quantum and classical physics. The features of entanglement, such as the negativity of conditional entropy [162, 163], monogamy of entanglement [164, 165], and the presence of bound entanglement [166, 167], are associated with entanglement conditions from fundamental and operational viewpoints. In fact, whether a given entangled state is useful or not, can be decided by certain thresholds

in terms of several quantum communication protocols [127, 131, 168] and quantum metrology [169–171].

- Generalizations: As a generalization of the separability problem, one can ask, for example, how many partitions are separated in a multipartite state based on the concept of k-separability [172, 173], or how many particles are entangled based on the concept of k-producibility [174–177]. Other interesting concepts are given by k-stretchability [178–180], tensor rank [181], and the bipartite and multipartite dimensionality [182–184] of entanglement. Genuine multipartite entanglement can in turn again be classified into several types, such as the W class or GHZ class of states. More recently, also different notions of network entanglement came into the focus of attention [185–187].

Introduction to Bell inequalities: To better understand the quantum world, let us begin by considering the limitations of the classical world. Note that classical mechanics is just one type of classical theory among many classical theories, so simply listing its laws does not fully explain the classical world.

Consider a situation where Alice and Bob are spatially separated and each receives a black box sent from a source. Inside the black box is a ball that cannot be seen from the outside. Balls have different properties: $A_1 = (\text{Black}, \text{White})$, $A_2 = (\text{Big}, \text{Small})$, $B_1 = (\text{Hard}, \text{Soft})$, and $B_2 = (\text{Elastic}, \text{Plastic})$. Alice and Bob should ask questions to know its properties. In fact, Alice can choose to ask a question for either A_1, A_2, whereas Bob can choose to ask a question for either B_1, B_2. When the results of Black, Big, Hard, Elastic are obtained, they label $+1$, whereas when the results of White, Small, Soft, Plastic are obtained, they label -1. That is, $A_1, A_2, B_1, B_2 = \pm 1$.

Clearly, $B_1 + B_2 = -2, 0, 2$ as well as $B_1 - B_2 = -2, 0, 2$. Since $A_1, A_2 = \pm 1$, one can notice that $S \equiv A_1(B_1 + B_2) + A_2(B_1 - B_2) = \pm 2$. Suppose that this scheme is repeated many times, and Alice and Bob randomly choose their measurements every time, independent of their respective choices. Now one can have that the expectation $\langle S \rangle$ is bounded as

$$-2 \leq \langle S \rangle \leq 2. \tag{1.2.34}$$

Such an inequality is called Bell's inequality [15, 16], which holds when we also consider other scenarios with two outcomes in the classical world. Note here that asking questions corresponds to performing measurements with two outcomes. It is essential that quantum mechanics can violate Bell's inequality.

Let us discuss this more precisely. Now one can notice that this inequality can be derived by implicitly imposing two assumptions in the classical world: (i) Locality: Any operation on Alice's system should not immediately affect the measurement results of Bob's system located far away. That is, the properties of Alice's ball are independent of the properties measured of Bob's ball, and vice versa (ii) Reality: Properties of balls have predetermined values even before they are measured. That is, each ball has properties, independent of whether

it is measured or not. If either Locality or Reality is violated, the inequality is violated.

Clauser-Horne-Shimony-Holt (CHSH) inequality: To formulate the Bell inequality in more detail, consider a scenario in which Alice and Bob share a state that can be characterized by a parameter variable λ. They perform measurements in this state, where each measurement direction can be respectively controlled by a parameter θ_A or θ_B. Let us denote Alice's measurement result as a function $\mathfrak{A}_\lambda(\theta_A)$, as well as Bob's one $\mathfrak{B}_\lambda(\theta_B)$. The measurement result depends on the state with the parameter λ and the measurement setting with θ_A, θ_B.

Let us assume the following on this model: (i) $-1 \leq \mathfrak{A}_\lambda(\theta_A), \mathfrak{B}_\lambda(\theta_B) \leq 1$ (ii) $\mathfrak{A}_\lambda(\theta_A), \mathfrak{B}_\lambda(\theta_B)$ are deterministically determined by λ and θ. (iii) the variable λ is hidden and occurs with a probability p_λ. (iv) After the many measurements, the expectation of $\mathfrak{A}_\lambda(\theta_A)\mathfrak{B}_\lambda(\theta_B)$ can be written

$$\langle A_1 B_1 \rangle = \int dp_\lambda \, \mathfrak{A}_\lambda(\theta_A)\mathfrak{B}_\lambda(\theta_B). \tag{1.2.35}$$

This is known as a local hidden variable (LHV) model. By changing the measurement direction as ϕ_A, ϕ_B, we consider the following quantity:

$$\langle S \rangle = \langle A_1 B_1 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle - \langle A_2 B_2 \rangle, \tag{1.2.36}$$

$$\langle A_1 B_2 \rangle = \int dp_\lambda \, \mathfrak{A}_\lambda(\theta_A)\mathfrak{B}_\lambda(\phi_B), \tag{1.2.37}$$

$$\langle A_2 B_1 \rangle = \int dp_\lambda \, \mathfrak{A}_\lambda(\phi_A)\mathfrak{B}_\lambda(\theta_B), \tag{1.2.38}$$

$$\langle A_2 B_2 \rangle = \int dp_\lambda \, \mathfrak{A}_\lambda(\phi_A)\mathfrak{B}_\lambda(\phi_B). \tag{1.2.39}$$

In the LHV model, the expectation $\langle S \rangle$ is bounded as

$$-2 \leq \langle S \rangle \leq 2. \tag{1.2.40}$$

This is the so-called Clauser-Horne-Shimony-Holt (CHSH) inequality as the simplest Bell inequality [188].

Let us take four observables with ± 1 eigenvalues: A_1, A_2, B_1, B_2. For simplicity, we take $A_1 = \sigma_x \otimes \mathbb{1}_2$, $A_2 = \sigma_y \otimes \mathbb{1}_2$, $B_1 = \mathbb{1}_2 \otimes \sigma_x$, and $B_2 = \mathbb{1}_2 \otimes \sigma_y$, where σ_x, σ_y are Pauli matrices. For the observable $S \equiv A_1(B_1 + B_2) + A_2(B_1 - B_2) = (2 - 2i)\,|00\rangle\langle 11| + (2 + 2i)\,|11\rangle\langle 00|$, since the eigenvalues of S are $0, \pm 2\sqrt{2}$, the absolute value of the expectation can be larger than 2. This suggests that CHSH inequality can be violated in quantum mechanics.

To elaborate on this point explicitly, we write the eigenstates with $\pm 2\sqrt{2}$ as

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}\left(e^{-i\frac{\pi}{4}}\,|00\rangle + |11\rangle\right), \qquad |\psi_-\rangle = \frac{1}{\sqrt{2}}\left(e^{i\frac{3\pi}{4}}\,|00\rangle + |11\rangle\right). \tag{1.2.41}$$

These states are entangled, so the violation of the Bell inequality implies the presence of entanglement. This is one of the examples of detecting quantum entanglement. Note that any separable state obeys the Bell inequality, while all mixed entangled states cannot always violate the Bell inequality. That is, the Bell inequality cannot be a necessary and sufficient condition for entanglement in general. For details about Bell inequalities, see [189, 190].

Bell operator: Let us discuss another formulation of the CHSH inequality. For this aim, we define the so-called Bell operator as

$$\mathcal{B} = \sum_{i,j=1}^{3} [a_i(c_j + d_j) + b_i(c_j - d_j)]\sigma_i \otimes \sigma_j, \tag{1.2.42}$$

where $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, and $\boldsymbol{d}$ are real unit vectors. The CHSH inequality can be reformulated as the expectation $\langle \mathcal{B} \rangle \leq 2$ for separable states. In Ref. [191], it has been shown that the maximum expectation value over all parameters is given by

$$\max_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}} \langle \mathcal{B} \rangle = 2\sqrt{\lambda_1^2 + \lambda_2^2}, \tag{1.2.43}$$

where λ_1 and λ_2 are the two largest singular values of the correlation matrix $T = (t_{ij})$ in the Bloch decomposition in Eq. (1.1.100). If this is bigger than 2, it means that the state is entangled. In fact, the Bell state has $\lambda_1 = \lambda_2 = 1$, and therefore $\max_{\langle \mathcal{B} \rangle} = 2\sqrt{2}$. For details, see [192, 193] and Chapter 4.

Positive partial transpose (PPT) criterion: Let X be a $d \times d$ matrix and $X^\top$ be its transposition. Since $\det(X) = \det(X^\top)$, they have the same characteristic polynomial: $\det(\lambda \mathbb{1}_d - X) = \det(\lambda \mathbb{1}_d - X^\top)$. This implies that the eigenvalues of X are equal to the eigenvalues of $X^\top$. Therefore, if X is a positive matrix, then its transpose is also positive. For a product matrix $X = X_A \otimes X_B$, let us denote the partial transposition as $X^{\top_B} = X_A \otimes X_B^\top$. Clearly, if X is positive, then its partial transpose is also positive.

The well-known positive partial transpose (PPT) criterion [194] states as follows: If a bipartite quantum state is separable, then its partial transpose is positive:

$$\varrho_{AB} \in \text{SEP} \rightarrow \varrho_{AB}^{\top_B} \geq 0. \tag{1.2.44}$$

In the following we make several remarks about the PPT criterion.

- Proof: The proof of the PPT criterion is very straightforward:

$$\varrho_{\text{sep}}^{\top_B} = \sum_i p_i \varrho_i^A \otimes (\varrho_i^B)^\top = \sum_i p_i \varrho_i^A \otimes \sigma_i^B \geq 0, \tag{1.2.45}$$

  where σ_i^B is also a quantum state since the transposition is a positive map.

- NPT entanglement: The violation of the PPT criterion implies that the state is entangled. Such an entangled state is called the negative partial transpose (NPT) state, while the quantum state that obeys the PPT criterion is called a PPT state.

- Low dimensions: For a quantum state $\varrho_{AB} \in \mathcal{H}_{d_A} \otimes \mathcal{H}_{d_B}$ with $d_A \times d_B \leq 6$, if the state ϱ_{AB} is PPT, then it is separable. That is, for a two-qubit state or $2 \otimes 3$-dimensional state, the PPT criterion is necessary and sufficient for separability [195].

- Reformulation 1: In the case of two-qubit entangled states, exactly one eigenvalue becomes negative under the partial transposition [196]. Thus, for two-qubit states, the PPT criterion becomes equivalent to

$$\det\left(\varrho_{AB}^{\top_B}\right) \geq 0, \tag{1.2.46}$$

  which was discussed in [197], and see Eq. (1.4.40).

- Reformulation 2: For the Bell-diagonal state in Eq. (1.1.137), the PPT criterion can be simply written as

$$\sum_{i=1}^{3} |\tau_i| \leq 1, \tag{1.2.47}$$

  which was discussed in [64] and see Sec 1.4.

- Reformulation 3: For a symmetric state ϱ_{AB} such that $\mathbb{S}\varrho_{AB} = \varrho_{AB}\mathbb{S} = \varrho_{AB}$ for the SWAP operator $\mathbb{S}$, the PPT criterion becomes equivalent to

$$\langle A \otimes A \rangle_{\varrho_{AB}} \geq 0, \tag{1.2.48}$$

  for all observables A. For two-qubit systems, the equivalent conditions are given by

$$\varrho_{AB} \in \text{SEP} \Leftrightarrow \varrho_{AB} \in \text{PPT} \Leftrightarrow X \geq 0 \Leftrightarrow C \geq 0, \tag{1.2.49}$$

  where and X is defined from the Bloch representation $\varrho_{AB} = \frac{1}{4}\sum_{i,j=0}^{3} X_{ij}\sigma_i \otimes \sigma_j$ and C is the Schur complement of X given by $C_{\mu\nu} = X_{\mu\nu} - X_{\mu 0}X_{0\nu}$ for $\mu, \nu = 1, 2, 3$. For details, see [198, 199] and Chapter 7.

- Reformulation 4: For a three-qubit symmetric state ϱ_{ABC} such that $\mathbb{S}_{xy}\varrho_{ABC} = \varrho_{ABC}\mathbb{S}_{xy} = \varrho_{ABC}$ for the SWAP operator $\mathbb{S}_{xy}$ with $x, y = A, B, C$ [for details see in Eq. (1.3.27)], it holds that

$$\varrho_{ABC} \in \text{Full-SEP} \Leftrightarrow \varrho_{ABC} \in \text{PPT} \Leftrightarrow Z \geq 0. \tag{1.2.50}$$

  where Z is a 8×8 matrix defined by $Z_{(\mu a),(\nu b)} = \sum_{\tau=0}^{3} X_{\tau\mu\nu}(\sigma_\tau)_{a,b}$ for $\mu, \nu = 0, 1, 2, 3$ and $a, b = 0, 1$ and X is defined from $\varrho_{ABC} = \frac{1}{8}\sum_{i,j,k=0}^{3} X_{ijk}\sigma_i \otimes \sigma_j \otimes \sigma_k$. Here $\varrho_{ABC} \in \text{PPT}$ means that it is PPT for all bipartitions. The

reason that this condition becomes equivalent to the full separability is that the state lives in the so-called symmetric subspace. In this space, the 2×4-separability condition turns out to be the 2×3-separability condition, which is equivalent to the PPT criterion. For details, see [199]. For further extensions, see [200–202].

- PPT entanglement: The set of PPT states is an outer approximation of the set of separable states in general. Then, in higher dimensions, there exist entangled states that cannot be detected by the PPT criterion: PPT entanglement. For details, see Sec. 1.2.4 and Chapter 2.

- Practical issues: To employ the PPT criterion, we have to know all the elements of the density matrix. This requirement could be challenging in experiments, especially for a large quantum state, since state tomography could be demanding.

- Lesson: One important lesson from the PPT criterion is that one can turn the separability problem into a positivity problem. This can relax separability issues/conditions in terms of moment problems [105] that will be discussed in Chapter 8, and quantum marginal problems [203].

Reduction criterion: We begin by recalling that the universal state inversion is a positive map, discussed in Eq. (1.1.58): $\mathcal{S}_d(\varrho) = \mathrm{tr}(\varrho)\mathbb{1}_d - \varrho \geq 0$ for a state ϱ. The reduction criterion [37, 204] states the following: If a bipartite quantum state ϱ_{AB} is separable, then

$$(\mathrm{id}_A \otimes \mathcal{S}_d)(\varrho_{AB}) = \mathbb{1} \otimes \varrho_A - \varrho_{AB} \geq 0. \tag{1.2.51}$$

Similarly, it holds that $(\mathcal{S}_d \otimes \mathrm{id}_B)(\varrho_{AB}) = \varrho_B \otimes \mathbb{1} - \varrho_{AB} \geq 0$.

The violation of the reduction criterion implies that the state is entangled. It is important to note that the reduction criterion is strictly weaker than the PPT criterion. That is, if an entangled state is detected by the reduction criterion, then it must be also detected by the PPT criterion, while even if the entangled state is detected by the PPT criterion, it is not necessarily detected by the reduction criterion. This is because the reduction map is decomposable using the transpose map [37].

Entropic criterion: Let $\gamma(\varrho) = \mathrm{tr}(\varrho^2)$ be the purity of a state ϱ. The (second-order) entropic criterion [64] can state as follows: If a bipartite quantum state ϱ_{AB} is separable, then

$$\gamma(\varrho_{AB}) \leq \gamma(\varrho_A), \qquad \gamma(\varrho_{AB}) \leq \gamma(\varrho_B). \tag{1.2.52}$$

This violation implies that the state is entangled. In the following, we make several remarks.

- Proof: This can be proven using the reduction criterion. Since $\mathrm{tr}(AB) \geq 0$ for positive matrices A, B, one can find the inequality for a separable state:

$$\mathrm{tr}\left[\varrho_{AB}(\mathrm{id}_A \otimes \mathcal{S}_d)(\varrho_{AB})\right] \geq 0. \tag{1.2.53}$$

  This directly leads to the expression of the entropic criterion. Therefore, the second-order entropic criterion is strictly weaker than the reduction criterion (therefore weaker than the PPT criterion).

- Reformulation 1: This criterion can be rewritten in other forms based on the linear (or Tsallis) entropy or the so-called second-order Rényi entropy [205]:

$$H_2(\varrho_A) \leq H_2(\varrho_{AB}), \quad H_2(\varrho_A) \leq H_2(\varrho_{AB}), \quad H_2(\varrho) = -\log\left[\mathrm{tr}(\varrho^2)\right]. \tag{1.2.54}$$

- Generalizations: This criterion was extended to higher-order cases [206–208] [also see Eq. (1.4.30)] and moreover the so-called majorization criterion using the state's spectrum [23, 209]. It has been shown that the majorization criterion is strictly weaker than the reduction criterion [210].

- Reformulation 2: One can rewrite the entropic criterion using the SWAP trick discussed in Sec. 1.1.7:

$$\mathrm{tr}[\varrho_{AB}^{\otimes 2} W_{AB}] \geq 0, \qquad W_{AB} = \mathbb{S}_A \otimes \mathbb{1}_B^{\otimes 2} - \mathbb{S}_{AB}. \tag{1.2.55}$$

  This reformulation can be understood as follows: The expectation of the observable W_{AB} acting on two copies of the system is nonnegative for all separable states. This reformulation was generalized to higher-order cases, for details see [211].

- Practical issues: The entropy criterion is weaker than the PPT criterion, but it is not necessary to know all the elements of the density matrix. Once the purities of the reduced state and the global state, one can apply this criterion to detect entanglement. This could allow for more experimentally friendly relaxation in practical situations.

Entanglement witnesses: An observable $\mathcal{W}$ is called the entanglement witness if $\mathrm{tr}(\mathcal{W}\varrho_{\mathrm{sep}}) \geq 0$ for all separable states ϱ_{sep}, but $\mathrm{tr}(\mathcal{W}\varrho_{\mathrm{ent}}) < 0$ for some entangled states ϱ_{ent}. Therefore, for an observable, if its expectation is negative, we can detect entanglement. In the following, we make several remarks.

- Mathematical side: For any entangled state, there exists an entanglement witness. More mathematically, for a compact convex set (separable set) and its outer point (entangled state), there exists a hyperplane that separates them, according to the so-called Hahn–Banach separation theorem, for details see [17].

- Practical side: Since $\mathrm{tr}(\mathcal{W}\varrho)$ is the expectation of the observable, it is a directly measurable quantity in practice. In experimental setups, the method of entanglement witnesses is then frequently employed to detect entanglement. For example, let us suppose that we have prior knowledge about the state of an experiment, specifically that it is intended to generate a particular entangled state. In such cases, entanglement witnesses can effectively verify the presence of entanglement.

- Equivalence: However, it is not easy to construct entanglement witnesses in general. Following the so-called Choi-Jamiolkowski isomorphism [212–214], connecting quantum states and channels, this problem is equivalent to the problem of distinguishing positive and completely positive maps, for details see [17, 154, 155].

- CHSH inequality: An example of the entanglement witnesses is the CHSH inequality. Recalling the Bell operator $\mathcal{B}$ in Eq. (1.2.42), the witness $\mathcal{W}_{\mathrm{CHSH}}$ is given by

$$\mathcal{W}_{\mathrm{CHSH}} = 2\mathbb{1}_2^{\otimes 2} - \mathcal{B}. \tag{1.2.56}$$

  For details see [215].

Fidelity witnesses: As discussed in Sec. 1.1, the method to know how close a given quantum state ϱ is to a known target entangled state $|\psi\rangle$ is the fidelity:

$$F_\psi(\varrho) \equiv \langle\psi|\varrho|\psi\rangle\,. \tag{1.2.57}$$

Note that this fidelity is the squared fidelity defined in Eq. (1.1.174). Now an observable $\mathcal{W}_\alpha$ is called the fidelity-based entanglement witness if

$$\mathcal{W}_\alpha = \alpha\mathbb{1} - |\psi\rangle\langle\psi|\,, \tag{1.2.58}$$

such that

$$\alpha = \max_{\varrho_{\mathrm{sep}}} F_\psi(\varrho_{\mathrm{sep}}) = \max_{\phi\in\mathrm{SEP}} |\langle\phi|\psi\rangle|^2. \tag{1.2.59}$$

Clearly, it holds that $\mathrm{tr}(\mathcal{W}_\alpha\varrho_{\mathrm{sep}}) \geq 0$. Using the Schmidt decomposition of $|\psi\rangle$ in Eq. (1.2.5), the parameter α can be simply evaluated as $\alpha = \lambda_1$ with the maximal coefficient λ_1 [78]. Here we make several remarks.

- Detectability: In Ref. [216], the method of fidelity-based witnesses was shown to have limited power to detect entanglement. More precisely, the notion of faithful entangled states was considered as the entangled states that can be detected by fidelity-based witnesses, and in the numerical approaches, such faithful entangled states were found to rarely exist in higher dimensional systems. More systematic approaches were discussed in Ref. [217].

- Teleportation: For the fidelity-based entanglement witness $\mathcal{W}_\alpha$, the value α of the maximally entangled state $|\psi^+\rangle$ in Eq. (1.2.7) is given by $1/d$. Similarly, one can consider other types of maximally entangled states which are equivalent to $|\psi^+\rangle$ under locally unitary transformations. In Ref. [218], fidelity-based witnesses were studied from operational viewpoints by introducing the so-called maximal singlet fraction (or fully entangled fraction):

$$\mathcal{F}(\varrho_{AB}) \equiv \max_{\psi\in \mathrm{ME}} \langle\psi|\varrho_{AB}|\psi\rangle = \max_{U_A,U_B} \langle\psi^+|U_A\otimes U_B\varrho_{AB}U_A^\dagger\otimes U_B^\dagger|\psi^+\rangle\,, \tag{1.2.60}$$

where ME is the set of maximally entangled (ME) states. It has been shown that an entangled state has $\mathcal{F}(\varrho_{AB}) > 1/d$ if and only if it shows usefulness beyond the classical regime in teleportation protocols. For details, see [120, 219].

- Simplifications: In Ref. [220], it has been shown that an entangled state ϱ_{AB} is faithful if and only if there are local unitaries $U_A\otimes U_B$ such that

$$\mathcal{F}_U(\varrho_{AB}) \equiv \langle\psi^+|U_A\otimes U_B\varrho_{AB}U_A^\dagger\otimes U_B^\dagger|\psi^+\rangle > \frac{1}{d}. \tag{1.2.61}$$

Moreover, for a two-qubit ϱ_{AB}, the quantity $\mathcal{F}_U(\varrho_{AB})$ can become analytically tractable and can be given by

$$\mathcal{F}_U(\varrho_{AB}) = \lambda_{\max}. \tag{1.2.62}$$

Here $\lambda_{\max}$ is the maximal eigenvalues of the operator $X_2(\varrho_{AB})$ defined as

$$\begin{aligned} X_2(\varrho_{AB}) &= \varrho_{AB} - \frac{1}{2}\left(\varrho_A\otimes\mathbb{1}_2 + \mathbb{1}_2\otimes\varrho_B\right) + \frac{1}{4}\mathbb{1}_2^{\otimes 2} \\ &= \frac{1}{4}\left(\mathbb{1}_2^{\otimes 2} + \sum_{i,j=1}^{3} t_{ij}\sigma_i\otimes\sigma_j\right), \end{aligned} \tag{1.2.63}$$

where t_{ij} denotes the elements of the two-body correlation matrix based on the Bloch decomposition in Eq. (1.1.100). Thus, a two-qubit entangled ϱ_{AB} is faithful if and only if $\lambda_{\max} > 1/2$. Now it is important to notice that one can transform the operator $X_2(\varrho_{AB})$ into the Bell diagonal form in Eq. (1.1.137) by applying local unitary operators. Letting $\varrho'_{AB} = U_A\otimes U_B\varrho_{AB}U_A^\dagger\otimes U_B^\dagger$ with the diagonal entries τ_i for $i = 1,2,3$, one can find that

$$\mathcal{F}_U(\varrho_{AB}) = \frac{1}{4}\max\{1-\tau_1-\tau_2-\tau_3, 1-\tau_1+\tau_2+\tau_3, 1+\tau_1-\tau_2+\tau_3, 1+\tau_1+\tau_2-\tau_3\}. \tag{1.2.64}$$

This scheme has been experimentally implemented [221]. In Chapter 4, this expression of $\mathcal{F}_U(\varrho_{AB})$ will be used in randomized measurements.

Several detections of two-qubit entanglement: Let us consider the two-qubit mixed state $\varrho(p)$ in Eq. (1.2.4) and test several criteria using the CHSH inequality (1.2.43), the PPT criterion (1.2.44), the entropic criterion (1.2.52), and the fidelity witness (1.2.64). Let us denote the respective transition points between the separable and entanglement of $\varrho(p)$ as $p_{\text{CHSH}}, p_{\text{PPT}}, p_{\text{ent}}, p_{\text{fid}}$. Straightforward calculation leads to

$$p_{\text{PPT}} = \frac{1}{3} \approx 0.33 < p_{\text{ent}} = \frac{1}{\sqrt{3}} \approx 0.577 < p_{\text{fid}} = \frac{2}{3} \approx 0.66 < p_{\text{CHSH}} = \frac{1}{\sqrt{2}} \approx 0.71. \tag{1.2.65}$$

1.2.4 Bound entanglement

Concepts: Suppose that we have k copies of a bipartite quantum state: $\varrho_{AB}^{\otimes k}$. The task is to distill (convert) these copies into the maximally entangled state $|\psi^+\rangle$ via LOCC operations. If this is possible, a state is called distillable. Otherwise, it is called undistillable [166]. In the following, we summarize several known facts, for details see [120, 219, 222, 223].

- Pure states: First of all, clearly, all separable states are undistillable. Then distillable states should be entangled. Also, all pure entangled states are distillable. Therefore a mixed state is sometimes called distillable if it can be distilled into pure entangled states.

- Dimensionality: All entangled two-qubit mixed states are distillable. Then undistillable entanglement, often called bound entanglement, exists only in high-dimensional systems.

- PPT states: If an entangled state violates the reduction criterion (1.2.51), the state is distillable. In fact, all PPT entangled states are bound entangled. This suggests that bound entanglement has a weak form of high-dimensional entanglement. This raises the converse question of whether all bound entangled states are PPT entangled? In other words, are all NPT entangled states distillable? The existence of NPT-bound entanglement is known as one of the most challenging and important open problems in quantum information [224].

- Peres conjecture: Asher Peres conjectured that all bound entangled states cannot violate Bell inequalities [225]. This problem is still open, while in the multipartite case, this conjecture is known to be wrong [226, 227]. Furthermore, the term stronger Peres conjecture was introduced in the sense that all bound entangled states cannot violate the so-called steering inequalities [228, 229]. This stronger Peres conjecture was disproved in [230], that is, there exist steering bound entangled states.

- Specific cases: The Werner state in Eq. (1.1.143) cannot be bound entangled. This is because it is separable if and only if PPT. Also, rank-two bound entangled states do not exist. For details, see [167, 231].

- Usefulness: Bound entanglement seems useless in information processing tasks. However, its utility has been demonstrated in quantum cryptography [232, 233] and metrology [234, 235].
- Multipartite systems: In an analogy with bipartite states, the notion of multipartite bound entanglement can be defined. Importantly, there are several multipartite states that are PPT (or bound) entangled for a bipartition but NPT entangled for other bipartitions [120]. Thus, the definition cannot be uniquely determined. It might be standard to call a multipartite state bound entangled if it is PPT (or bound) for all bipartitions but not fully separable.
- Remark: As a more restricted class, there exist multipartite states that are separable for all bipartitions but not fully separable [236]. The GHZ diagonal states that are PPT for any bipartition are separable for any bipartition [237].

Detection of PPT (bound) entanglement: Given a quantum state, how can we prove that it is PPT (bound) entangled? There are two steps. First, we apply the PPT criterion. If it is violated, then it is NPT entangled. If not, we have to show that the state is still entangled. For this purpose, several criteria are considered.

Here we summarize their terms and references, for details see [17, 120, 238]: Range criterion [239], Computable cross norm or realignment (CCNR) criterion [240–242], Its extensions [243], de Vicente criterion [244] that will be explained below, Permutation criteria [245], Criteria based on uncertainty relations [246–248], Covariance matrix criterion [59, 249], Criterion based on symmetric informationally complete positive operator valued measure (SIC POVM) [250], The whole family of entanglement criteria [251], Breuer–Hall map criterion [62, 63], Spin-squeezing inequalities [160], Criteria using the Cauchy-Schwarz and the Hölder inequality [252] Stronger criteria based on quantum Fisher information [253, 254], E_4 criterion [255], and Polytope adaption technique [256].

de Vicente criterion: The de Vicente criterion states that any bipartite separable ϱ_{AB} in $d_A \otimes d_B$ systems obeys

$$\|T\|_{\mathrm{tr}} \leq \sqrt{(d_A - 1)(d_B - 1)}, \tag{1.2.66}$$

where T is a correlation matrix in Eq. (1.1.100) in the case of asymmetric dimensions and $\|X\|_{\mathrm{tr}}$ is the trace norm of a matrix X, that is, the sum of its singular values. The violation of this inequality implies that the state is entangled. In the following, we make three important remarks, for details see [60, 244].

- Detection of PPT entanglement: The de Vicente criterion is complementary to the PPT criterion. More precisely, the de Vicente criterion sometimes can detect entangled states which cannot be detected by the PPT criterion,

while the PPT criterion sometimes can detect entangled states which cannot be detected by the de Vicente criterion. Neither is strictly stronger than the other. Thus, if one wants to detect bound entangled states, it makes sense to apply the de Vicente criterion.

- Hierarchy: In the case with $d_A = d_B$, the de Vicente criterion is strictly weaker than the CCNR criterion. On the other hand, the de Vicente criterion becomes strictly stronger than the CCNR criterion if the reduced states ϱ_A and ϱ_B are maximally mixed and $d_A \neq d_B$. Both are equivalent if the reduced states $\varrho_A = \varrho_B = \mathbb{1}_d/d$ and $d_A = d_B = d$.

- Generalizations: The de Vicente criterion is based only on the two-body correlation matrix. In a similar manner, its multipartite extensions have been proposed in terms of correlation tensors [257]. Also, it has been generalized to criteria for Schmidt numbers [258].

List of bound entangled states

In this subsubsection, we will make the list of bound entangled states. Other examples are given in [166, 256, 259–264]. In Table 1.1, we describe several properties of bound entangled states.

States	Rank	$\gamma(\varrho_{AB})$	$\gamma(\varrho_A)$, $\gamma(\varrho_B)$	$\varrho_{AB} \stackrel{?}{=} \varrho_{AB}^{\top_B}$	$\|T\|_{\mathrm{tr}}$
$\varrho(E_{\mathrm{ch}})$	4	$1/4$	$11/32 \approx 0.344$	No	2.37
ϱ_{cb}	4	$1/4$	$1/3$	Yes	2.5
ϱ_{UPB}	4	$1/4$	$35/96 \approx 0.365$	Yes	2.11
$\sigma(p)$	7	$h_1(p)$	$1/3$	No	$h_2(p)$
$\varrho_{\mathrm{steering}}$	4	0.295	0.395, 0.452	Yes	2.18
ϱ_{MS}	9	$m_1(\alpha)$	$1/3$	No	$m_2(\alpha)$

Table 1.1: Results for several bound entangled states discussed in $3 \otimes 3$-dimensional systems. For the state ϱ_{cb}, each parameter is $m = n = b = -3/5$, $a = 3/5$, $c = -d = 6/5$. For the state $\sigma(p)$, for $p \in (3,4]$, $h_1(p) = [2(p-5)p + 37]/147 \in (0.170, 0.197]$, and $h_2(p) = (2/7)\left(\sqrt{3(p-5)p+19}+6\right) \in (2, 2.47]$. For the state ϱ_{MS}, $\beta = -0.025$ and $\gamma = 0$, for $\alpha \in (0.175, 0.225)$ $m_1(\alpha) = \alpha(80\alpha - 1)/90 + 67/600 \in (0.137, 0.154)$ and $m_2(\alpha) = \left(40\alpha - 1 + \sqrt{40\alpha(40\alpha+1)+1}\right)/10 \in (0.137, 0.154)$.

Quantum grid states: For $d \otimes d$-dimensional systems, consider a pure entangled state forming

$$|i,j;k,l\rangle = \frac{1}{\sqrt{2}}\left(|ij\rangle - |kl\rangle\right), \tag{1.2.67}$$

with $0 \leq i,j,k,l < d$. A quantum $d \otimes d$-dimensional grid state is defined as the uniform mixture of pure states $|i,j;k,l\rangle$. That is, for a given set $E = \{|i,j;k,l\rangle\}$,

it can be defined as

$$\varrho(E) = \frac{1}{|E|} \sum_{|e\rangle \in E} |e\rangle\langle e| \,. \tag{1.2.68}$$

Note that not all quantum grid states are separable, and moreover, there are some grid states that can have bound entanglement. In particular, a $3 \otimes 3$-dimensional bound entangled grid state is called the cross-hatch state with the set

$$E_{\text{ch}} = \{|0,0;1,2\rangle\,, |1,0;2,2\rangle\,, |0,1;2,0\rangle\,, |0,2;2;1\rangle\}. \tag{1.2.69}$$

For details, see Fig. 2 (a) in [265]. Note that the density matrix is given by

$$\varrho(E_{\text{ch}}) = \frac{1}{8} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.2.70}$$

Chessboard states: For $3 \otimes 3$-dimensional systems, consider a family of quantum states

$$\varrho_{\text{cb}} = N \sum_{i=1}^{4} |V_i\rangle\langle V_i| \,, \tag{1.2.71}$$

where $N = 1/\sum_i \langle V_i \,|\, V_i\rangle$ is a normalization factor and

$$|V_1\rangle = (m,0,s;0,n,0;0,0,0), \qquad |V_2\rangle = (0,a,0;b,0,c;0,0,0), \tag{1.2.72}$$

$$|V_3\rangle = (n,0,0;0,-m,0;t,0,0), \qquad |V_4\rangle = (0,b,0;-a,0,0;0,d,0), \tag{1.2.73}$$

with free real parameters a, b, c, d, m, n and $s = \frac{ac}{n}, t = \frac{ad}{m}$. The matrix form of this state can then be expressed as

$$\varrho_{\text{cb}} = N \begin{pmatrix} m^2+n^2 & 0 & ms & 0 & 0 & 0 & nt & 0 & 0 \\ 0 & a^2+b^2 & 0 & 0 & 0 & ac & 0 & bd & 0 \\ sm & 0 & s^2 & 0 & sn & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a^2+b^2 & 0 & bc & 0 & -ad & 0 \\ 0 & 0 & ns & 0 & m^2+n^2 & 0 & -mt & 0 & 0 \\ 0 & ac & 0 & cb & 0 & c^2 & 0 & 0 & 0 \\ tn & 0 & 0 & 0 & -tm & 0 & t^2 & 0 & 0 \\ 0 & bd & 0 & -da & 0 & 0 & 0 & d^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{1.2.74}$$

where $N = 2a^2 + 2b^2 + c^2 + d^2 + 2m^2 + 2n^2 + s^2 + t^2$. The states ϱ_{cb} are called the chessboard states because their 8×8 matrix form looks like a chessboard,

originally introduced by Dagmar Bruß and Asher Peres [266]. The state is invariant under the partial transposition. On the other hand, according to the range criterion [239], $\varrho_{\rm cb}$ is entangled. Thus, the chessboard states are bound entangled.

Unextendible product bases: For $3 \otimes 3$-dimensional systems, let us consider five product states

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} |0\rangle (|0\rangle - |1\rangle), \qquad |\psi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) |2\rangle , \tag{1.2.75}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} |2\rangle (|1\rangle - |2\rangle), \qquad |\psi_3\rangle = \frac{1}{\sqrt{2}} (|1\rangle - |2\rangle) |0\rangle , \tag{1.2.76}$$

$$|\psi_4\rangle = \frac{1}{3} (|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle). \tag{1.2.77}$$

Notice that all of these five product states are orthogonal to all pairs, and another product state cannot be orthogonal to all pairs. These product states are said to form an unextendible product basis (UPB) [267]. From these states, one can construct the mixed state

$$\varrho_{\rm UPB} = \frac{1}{4} \left(\mathbb{1} - \sum_{i=0}^{4} |\psi_i\rangle\langle\psi_i| \right) . \tag{1.2.78}$$

Here, $\varrho_{\rm UPB}$ is the state on the space that is orthogonal to the space spanned by the UPB. Then, $\varrho_{\rm UPB}$ has no product states in the range. According to the range criterion [239], $\varrho_{\rm UPB}$ should be entangled. On the other hand, one can notice that $\varrho_{\rm UPB}$ is invariant under the partial transposition: $\varrho_{\rm UPB} = \varrho_{\rm UPB}^{\top_B} \geq 0$. Hence, $\varrho_{\rm UPB}$ is a bound entangled state. Note that the density matrix is given by

$$\varrho_{\rm UPB} = \frac{1}{72} \begin{pmatrix} 7 & 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ 7 & 7 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -2 & -2 & 7 & -2 & -2 & 7 & -2 & -2 & -2 \\ -2 & -2 & -2 & 7 & -2 & -2 & 7 & -2 & -2 \\ -2 & -2 & -2 & -2 & 16 & -2 & -2 & -2 & -2 \\ -2 & -2 & 7 & -2 & -2 & 7 & -2 & -2 & -2 \\ -2 & -2 & -2 & 7 & -2 & -2 & 7 & -2 & -2 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 & 7 \\ -2 & -2 & -2 & -2 & -2 & -2 & -2 & 7 & 7 \end{pmatrix} . \tag{1.2.79}$$

$3 \otimes 3$ **Horodecki state:** For $3 \otimes 3$-dimensional systems, consider the mixed state

$$\sigma(p) = \frac{2}{7} |\psi^+\rangle\langle\psi^+| + \frac{p}{7} \sigma_+ + \frac{5-p}{7} \sigma_-, \qquad 2 \leq p \leq 5, \tag{1.2.80}$$

where the two-qutrit maximally entangled state $|\psi^+\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ and

$$\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|), \tag{1.2.81}$$

$$\sigma_- = \frac{1}{3}(|10\rangle\langle 10| + |21\rangle\langle 21| + |02\rangle\langle 02|). \tag{1.2.82}$$

It turns out that the state $\sigma(p)$ is PPT in the range $2 \leq p \leq 4$. To characterize this state further, one can employ a non-decomposable positive map Λ such that $(\mathbb{1} \otimes \Lambda)\sigma \not\geq 0$. An example is

$$\Lambda \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & -a_{12} & -a_{13} \\ -a_{21} & a_{22} & -a_{23} \\ -a_{31} & -a_{32} & a_{33} \end{pmatrix} + \begin{pmatrix} a_{22} & 0 & 0 \\ 0 & a_{33} & 0 \\ 0 & 0 & a_{11} \end{pmatrix}. \tag{1.2.83}$$

This non-decomposable map allows us to classify this state as follows [268]: the state $\sigma(p)$ is not detected as entangled for $2 \leq p \leq 3$, PPT (bound) entangled for $3 < p \leq 4$, and NPT entangled for $4 < p \leq 5$. Note that the density matrix is given by

$$\sigma(p) = \frac{1}{21}\begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5-p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5-p & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5-p & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \end{pmatrix}. \tag{1.2.84}$$

Steering bound entangled state: For $3 \otimes 3$-dimensional systems, consider the mixed state

$$\varrho_{\text{steering}} = \lambda_1 |\psi_1\rangle\langle\psi_1| + \lambda_2 |\psi_2\rangle\langle\psi_2| + \lambda_3(|\psi_3\rangle\langle\psi_3| + |\tilde{\psi}_3\rangle\langle\tilde{\psi}_3|), \tag{1.2.85}$$

where the normalized states are

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|12\rangle + |21\rangle), \qquad |\psi_2\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle - |22\rangle), \tag{1.2.86}$$

$$|\psi_3\rangle = m_1 |01\rangle + m_2 |10\rangle + m_3(|11\rangle + |22\rangle), \tag{1.2.87}$$

$$|\tilde{\psi}_3\rangle = m_1 |02\rangle - m_2 |20\rangle + m_3(|21\rangle - |12\rangle), \tag{1.2.88}$$

with $m_i \geq 0$ and

$$\lambda_1 = 1 - \frac{2 + 3m_1m_2}{4 - 2m_1^2 + m_1m_2 - 2m_2^2}, \qquad \lambda_3 = \frac{1}{4 - 2m_1^2 + m_1m_2 - 2m_2^2}, \tag{1.2.89}$$

and $\lambda_2 = 1 - \lambda_1 - 2\lambda_3$. In this choice of parameter, the state $\varrho_{\text{steering}}$ is invariant under the partial transposition. If $m_1 = 0.2162$ and $m_2 = 0.4363$, this state is steerable. For details, see [230].

Magic simplex states: For $3 \otimes 3$-dimensional systems, consider the mixed state

$$\varrho_{\mathrm{MS}} = \frac{1-\alpha-\beta-\gamma}{8}\mathbb{1}_9 + \alpha\,|\psi_{00}\rangle\langle\psi_{00}| + \beta\,|\psi_{01}\rangle\langle\psi_{01}| + \gamma\,|\psi_{02}\rangle\langle\psi_{02}|\,, \tag{1.2.90}$$

where

$$|\psi_{ij}\rangle = (\mathbb{1}_3 \otimes X^i Z^j)\,|\psi_{00}\rangle\,, \qquad |\psi_{00}\rangle = \frac{1}{\sqrt{3}}\sum_{i=0}^{2}|ii\rangle\,, \tag{1.2.91}$$

with

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & w \end{pmatrix}, \qquad w = e^{2\pi i/3}. \tag{1.2.92}$$

Note that the density matrix is given by

$$\varrho_{\mathrm{MS}} = \frac{1}{9}\begin{pmatrix} 2M+1 & 0 & 0 & 0 & 3G_2 & 0 & 0 & 0 & 3G_2 \\ 0 & \bar{M} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \bar{M} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \bar{M} & 0 & 0 & 0 & 0 & 0 \\ 3G_1 & 0 & 0 & 0 & 2M+1 & 0 & 0 & 0 & 3M \\ 0 & 0 & 0 & 0 & 0 & \bar{M} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \bar{M} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \bar{M} & 0 \\ 3G_1 & 0 & 0 & 0 & 3M & 0 & 0 & 0 & 2M+1 \end{pmatrix}, \tag{1.2.93}$$

where $M = \alpha+\beta+\gamma$, $\bar{M} = 1-M$, $G_1 = \alpha + \beta i^{2/3} - \gamma\sqrt[3]{i}$, and $G_2 = \alpha + \beta i^{2/3} - \gamma\sqrt[3]{i}$. For $\alpha \in (0.175, 0.225)$, $\beta \in (-0.075, -0.025)$, and $\gamma = 0$, this state can be bound entangled. For details, see [269, 270].

$4 \otimes 4$ **Piani state:** For $4 \otimes 4$-dimensional systems, consider the orthogonal projections

$$P_{ij} = |\Psi_{ij}\rangle\langle\Psi_{ij}|\,, \tag{1.2.94}$$

where $|\Psi_{ij}\rangle = (\mathbb{1} \otimes \sigma_{ij})\,|\Psi_+^4\rangle$, $|\Psi_+^4\rangle = \frac{1}{2}\sum_{k=0}^{3}|kk\rangle$, and $\sigma_{ij} = \sigma_i \otimes \sigma_j$ with Pauli matrices. With these projections, one can construct the state

$$\begin{aligned} \varrho_{\mathrm{BE}} &= \frac{1}{6}\left(P_{02} + P_{11} + P_{23} + P_{31} + P_{32} + P_{33}\right) \\ &= \frac{1}{6}\Big(\Phi^+_{AB}\Psi^-_{A'B'} + \Psi^+_{AB}\Psi^+_{A'B'} + \Psi^-_{AB}\Phi^-_{A'B'} + \Phi^-_{AB}\Psi^+_{A'B'} + \Phi^-_{AB}\Psi^-_{A'B'} + \Phi^-_{AB}\Phi^-_{A'B'}\Big), \end{aligned} \tag{1.2.95}$$

where $\Phi^+, \Phi^-, \Psi^+, \Psi^-$ are also projectors on the Bell states. It has been shown that the state ϱ_{BE} is the $4 \otimes 4$ bound entangled under the bipartition of $AA'|BB'$. For details, see [271].

$4 \otimes 2$ **Horodecki state:** For $4 \otimes 2$-dimensional systems, consider the state

$$\varrho_{\mathrm{HDK}} = \frac{1}{h} \begin{pmatrix} 2t & 0 & 0 & 0 & 0 & 0 & 2t & 0 \\ 0 & 2t & 0 & 0 & 0 & 0 & 0 & 2t \\ 0 & 0 & t+1 & 0 & 0 & 0 & 0 & t' \\ 0 & 0 & 0 & 2t & 2t & 0 & 0 & 0 \\ 0 & 0 & 0 & 2t & 2t & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2t & 0 & 0 \\ 2t & 0 & 0 & 0 & 0 & 0 & 2t & 0 \\ 0 & 2t & t' & 0 & 0 & 0 & 0 & t+1 \end{pmatrix}, \tag{1.2.96}$$

where $t' = \sqrt{1-t^2}$, $h = 2(1+7t)$ and $0 < t < 1$. Note that this state can be also regarded as a three-qubit state. Then the parties AB are in 4-dimensional systems and the party C is in 2-dimensional systems. This state is NPT entangled for $A|BC$ and $AC|B$, but PPT entangled for $AB|C$. For details, see [239].

$2 \otimes 2 \otimes 2$ **bound entangled states:** For $2 \otimes 2 \otimes 2$-dimensional systems, consider the followings unnormalized states:

$$\varrho_{\mathrm{UPB}} \propto \begin{pmatrix} 7 & 1 & 1 & \bar{1} & 1 & \bar{1} & \bar{1} & 1 \\ 1 & 3 & \bar{1} & 1 & \bar{1} & \bar{3} & 1 & \bar{1} \\ 1 & \bar{1} & 3 & \bar{3} & \bar{1} & 1 & 1 & \bar{1} \\ \bar{1} & 1 & \bar{3} & 3 & 1 & \bar{1} & \bar{1} & 1 \\ 1 & \bar{1} & \bar{1} & 1 & 3 & 1 & \bar{3} & \bar{1} \\ \bar{1} & \bar{3} & 1 & \bar{1} & 1 & 3 & \bar{1} & 1 \\ \bar{1} & 1 & 1 & \bar{1} & \bar{3} & \bar{1} & 3 & 1 \\ 1 & \bar{1} & \bar{1} & 1 & \bar{1} & 1 & 1 & 7 \end{pmatrix}, \varrho_{\mathrm{ADMA}} \propto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/a & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{1.2.97}$$

$$\varrho_{\mathrm{AK}} \propto \begin{pmatrix} x & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & y & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & y & 0 & 0 & \bar{2} & 0 & 0 \\ 0 & 0 & 0 & y & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & y & 0 & 0 & 0 \\ 0 & 0 & \bar{2} & 0 & 0 & y & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & y & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & x \end{pmatrix}, \varrho_{\mathrm{PH}} \propto \begin{pmatrix} 2z & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/z & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/z & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/z & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{1.2.98}$$

where $\bar{1} = -1, \bar{2} = -2, \bar{3} = -3$, $a, b, c, x, y, z > 0$, $abc \neq 1$, and $x = y + 4$. These states have been already known: ϱ_{UPB} in Ref. [267], ϱ_{ADMA} in Ref. [137], ϱ_{AK} in Ref. [272], and the Hyllus state ϱ_{PH} in Eq. (2.105) in Ref. [273]. Note that ϱ_{AK} is entangled for $2 \leq y \leq 2.828$ but separable for $y \geq 2\sqrt{2}$. Also ϱ_{UPB} is permutationally symmetric.

Let us summarize the property of these states. The first common property of them is that they are separable for any bipartition, but not fully separable. In that sense, they are not multipartite distillable and then bound entangled [236]. Second, their matrix ranks are, respectively, given by $\mathrm{Rank}(\varrho_{\mathrm{UPB}}) = 4$,

$\text{Rank}(\varrho_{\text{ADMA}}) = 7$, $\text{Rank}(\varrho_{\text{AK}}) = 8$, and $\text{Rank}(\varrho_{\text{PH}}) = 5$. Finally, these bound entangled states can be detected with the help of the previously presented entanglement criteria in Refs. [236, 245, 274].

Also consider the following three-qubit thermal state with the Heisenberg chain model:

$$\varrho_H = e^{(-H_H/T)}/Z, \qquad H_H = \sum_{i=1,2,3} \sigma_X^i \sigma_X^{i+1} + \sigma_Y^i \sigma_Y^{i+1} + \sigma_Z^i \sigma_Z^{i+1}, \tag{1.2.99}$$

with temperature T and $Z = \text{tr}[\exp(-H_H/T)]$. This thermal state has been shown to be bound entangled in the temperature range $T \in [4.33, 5.46]$, in the sense that they are separable for any bipartition but not fully separable in Refs. [160, 275] and Table II in [276], where the bound entanglement can be detected by the optimal spin squeezing inequality.

1.2.5 Entanglement measures

Requirements: For a bipartite quantum state ϱ_{AB}, an entanglement measure $E(\varrho_{AB})$ is required to satisfy the following conditions:

- Entanglement cannot increase under LOCC:

$$E[\Phi_{\text{LOCC}}(\varrho_{AB})] \leq E(\varrho_{AB}), \tag{1.2.100}$$

  for any LOCC operation Φ_{LOCC} in Eq. (1.1.126). It is also usual to require the stronger requirement: $E(\varrho_{AB})$ cannot increase on average under LOCC operations:

$$\sum_i p_i E(\sigma_i) \leq E(\varrho_{AB}), \tag{1.2.101}$$

  where $\sigma_i = (1/p_i) K_i \varrho_{AB} K_i^\dagger$ with the Kraus operators K_i of Φ_{LOCC} and $p_i = \text{tr}(K_i \varrho_{AB} K_i^\dagger)$ is the probability to obtain an outcome i.

- Entanglement vanishes in separable states:

$$E(\varrho_{AB}) = 0, \qquad \text{for any } \varrho_{AB} \in \text{SEP}. \tag{1.2.102}$$

- As an additional requirement, the convex property is often imposed:

$$E\left(\sum_i p_i \varrho_i\right) \leq \sum_i p_i E(\varrho_i), \tag{1.2.103}$$

  where $\varrho_{AB} = \sum_i p_i \varrho_i$ is a mixed state.

In particular, an entanglement measure $E(\varrho_{AB})$ is called LOCC monotone if it satisfies Eqs. (1.2.101, 1.2.102, 1.2.103).

FLAGS condition: There is a simple test to know whether an entanglement measure is LOCC monotone or not. An entanglement measure $E(\varrho_{AB})$ is LOCC monotone if and only if

- it is invariant under any local unitary:
$$E(U_A \otimes U_B \varrho_{AB} U_A^\dagger \otimes U_B^\dagger) = E(\varrho_{AB}), \tag{1.2.104}$$
for all unitaries U_A, U_B.
- it satisfies the so-called FLAGS condition:
$$E\left(\sum_i p_i \varrho_{AB}^i \otimes |i\rangle\langle i|_X\right) = \sum_i p_i E(\varrho_{AB}^i), \tag{1.2.105}$$
where $|i\rangle_X$ are local orthogonal bases (flags) for $X = A', B'$.

Notice that the LOCC monotone inequalities are replaced by the two equalities. The FLAGS condition can be understood as follows: Given a mixture of states with local flags, the entanglement of the mixture is equivalent to the average entanglement of the individual states. For details about FLAGS conditions, see [277, 278].

Concurrence: For a two-qubit state ϱ_{AB}, the concurrence is defined as
$$C(\varrho_{AB}) = \max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\}, \tag{1.2.106}$$
where λ_i are, in decreasing order, the eigenvalue of the matrix R:
$$R = \sqrt{\sqrt{\varrho_{AB}}(\sigma_y \otimes \sigma_y)\varrho_{AB}^*(\sigma_y \otimes \sigma_y)\sqrt{\varrho_{AB}}}, \tag{1.2.107}$$
and ϱ_{AB}^* is the complex conjugation of ϱ_{AB}. Then one can analytically compute the concurrence for a two-qubit entangled state [36].

It is important to note that concurrence is directly connected to the so-called entanglement of formation:
$$E_F(\varrho_{AB}) = h\left(\frac{1 + \sqrt{1 - C^2(\varrho_{AB})}}{2}\right), \tag{1.2.108}$$
where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Here, the entanglement of formation is a LOCC monotone entanglement measure and has a clear operational meaning. It quantifies how many singlet states we require to create the state ϱ_{AB} in the asymptotic sense.

Negativity: Negativity is an entanglement measure defined as
$$N(\varrho_{AB}) = \sum_{\lambda_i < 0} |\lambda_i|, \tag{1.2.109}$$
where λ_i are eigenvalues of the partial transpose state $\varrho_{AB}^{\top_B}$ [279]. We remark that $N(\varrho_{AB}) = 0$ if a state ϱ_{AB} is PPT. Thus, negativity cannot quantify the amount of PPT entanglement. On the other hand, one can straightforwardly compute negativity.

Squashed entanglement: Squashed entanglement is an entanglement measure defined as

$$E_{\mathrm{sq}}(\varrho_{AB}) = \min_{\gamma_{ABX}} \frac{1}{2} I(A:B|X), \tag{1.2.110}$$

where $I(A:B|X) = S(AX) + S(BX) - S(ABX) - S(X)$ is the quantum conditional mutual information. Here, γ_{ABX} is any extension of ϱ_{AB}, that is, $\varrho_{AB} = \mathrm{tr}_X(\gamma_{ABX})$, and $S(M)$ is the von Neumann entropy of system M. Squashed entanglement is known to be LOCC monotone. For details, see [280, 281].

Monogamy relation and three-tangle: For any three-qubit pure state $|\psi_{ABC}\rangle$, it holds that

$$C^2(A:BC) \geq C^2(A:B) + C^2(A:C), \tag{1.2.111}$$

where this is permutationally invariant. Here, $C^2(A:BC)$ is the squared concurrence between A and BC, which can be expressed as $C^2(A:BC) = 4 \det \varrho_A$. Also, $C^2(X:Y)$ are squared concurrence of the reduced state $\varrho_{XY} = \mathrm{tr}_Z(\varrho_{ABC})$ for $X, Y, Z = A, B, C$.

For instance, if ϱ_{XY} is maximally entangled, then $C^2(A:B) = 1$. On the other hand, since ϱ_A is maximally mixed, one has that $C^2(A:BC) = 1$. Therefore, $C^2(A:C)$ turns out to be zero. This implies that when A and B are maximally entangled, each system cannot be entangled with C. In general, this inequality indicates the fundamental limitation between three-qubit correlations. Often this is called Coffman-Kundu-Wootters (CKW) monogamy relation [164].

Motivated by the CKW relation, the entanglement of a three-qubit state ϱ_{ABC} can be quantified:

$$\tau_3(\varrho_{ABC}) = C^2(A:BC) - C^2(A:B) - C^2(A:C), \tag{1.2.112}$$

where $\tau_3(\varrho_{ABC})$ is called the three-tangle. It is common to call $C^2(A:BC)$ the one-tangle and $C^2(A:B) + C^2(A:C)$ the two-tangle. For instance, the GHZ state has a nonzero three-tangle but a zero two-tangle, while the W state has a zero three-tangle but a nonzero two-tangle.

Lockable entanglement: For a multipartite state in system $S_1 S_2 \cdots S_N$, let us consider a bipartite entanglement between S and $S_2 \cdots S_N$. A nontrivial question arises: How much does the entanglement decrease with the loss of one particle? An entanglement measure $E(S_1|S_2 \cdots S_N)$ is called lockable if the entanglement change can be arbitrarily large after one particle is discarded, that is,

$$E(S_1|S_2 \cdots S_N) \gg E(S_1|S_2 \cdots S_{N-1}). \tag{1.2.113}$$

This may happen when a particle S_N plays a key role in controlling the whole entanglement. For instance, the entanglement of formation and the squashed entanglement is known as lockable. Also, all measures based on the so-called convex-roof method are known as lockable. For details, see [282].

1.3 Quantum metrology

In this section, we will give a brief introduction to quantum metrology. In quantum metrology, the two main topics of interest are spin squeezing and quantum Fisher information. This section describes each of the basic concepts which are necessary to understand this thesis. For more general introductions to quantum metrology, see [92, 161, 170, 171, 283–289].

1.3.1 General schemes

A general scheme of quantum metrology consists of three stages: preparation of an initial probe state, state transformation to encode a parameter θ, and readout measurement to extract information about θ, as illustrated in Fig. 1.1. Each stage can be designed to be either quantum or classical, offering various possibilities, such as entangled or separable initial states, entangling or non-entangling state transformations, and measurement observables in the form of real multipartite operators or direct products of single-particle operators. The achievable precision $(\Delta\theta)^2$ in parameter estimation tasks depends on the chosen design.

The central task is to improve the metrological scheme so that it reaches an optimal precision beyond the classical regime. When all stages are classical, the best achievable precision in a probe system of N particles is called the shot-noise limit, $(\Delta\theta)^2 \propto N^{-1}$. However, the presence of initial entanglement in the preparation stage can allow scaling beyond the shot-noise limit, ultimately reaching the so-called Heisenberg limit, $(\Delta\theta)^2 \propto N^{-2}$. Furthermore, even without initial entanglement, entangling transformations can lead to quantum scalings much better than the Heisenberg limit. Examples include the so-called super-Heisenberg limit, $(\Delta\theta)^2 \propto N^{-2k+1}$ for integers k [290–294], and the exponential enhancement proposed by Roy and Braunstein, $(\Delta\theta)^2 \propto 4^{-N}$ [295], also see [296, 297].

In general, there are two well-known methods to characterize the precision of the estimation. One is to use the so-called error propagation formula [288, 298, 299]:

$$(\Delta\theta)^2 = \frac{(\Delta M)^2}{|\partial_\theta \langle M\rangle|^2}, \tag{1.3.1}$$

where $\langle M\rangle$ is the expectation of the measurement observable M, and $(\Delta M)^2 = \langle M^2\rangle - \langle M\rangle^2$ is its variance. This formula allows us to estimate θ from measurement results of M, for details see Eq. (1.3.3). This approach is practically useful since the precision can be directly calculated from measurements, while finding the optimal measurement scheme would be challenging.

A more general approach is to employ the quantum Cramér–Rao bound [91, 300]:

$$(\Delta\theta)^2 \geq \frac{1}{\mathcal{F}_Q(\varrho, A)}, \tag{1.3.2}$$

where we suppose that an initial state ϱ can be transformed by a unitary operator $U_\theta = \exp(-i\theta A)$ with a Hermitian operator A, and $\mathcal{F}_Q(\varrho, A)$ denotes the

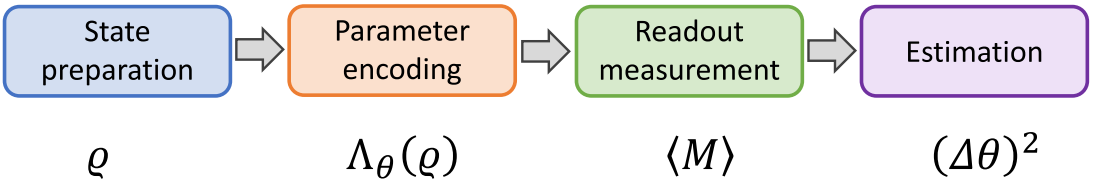

Figure 1.1: Sketch of quantum metrology, consisting of three stages: the preparation stage of a state ϱ, the parameter encoding stage by a parameter-dependent channel Λ_θ, and the readout measurement stage with an observable M.

quantum Fisher information in Eq. (1.1.201). This method allows for a discussion of the fundamental limit on the precision in quantum mechanics, but it may lead to overestimation since the inequality saturates only for optimal measurements.

In this section, we will describe these two methods more precisely and explain the concepts of spin squeezing or quantum Fisher information and their relations with entanglement. Finally, it should be noted that other areas of interest in quantum metrology include Bayesian estimation [301], multiparameter scenarios [94, 302–306], quantum networks [307–309], and temperature estimation in quantum thermodynamics [310].

1.3.2 Spin squeezing

Error propagation formula: Consider a scenario where we aim to determine the value of a parameter θ encoded in a physical system. Information about the value can be extracted from measurements on the system, allowing us to estimate the parameter's value. The estimation is performed indirectly via a function $\langle M \rangle = f(\theta)$ directly obtained from measurements. For instance, the area of a square can be estimated by measuring the length of one side, or the time on an unscaled clock can be determined by looking at the length of the clock hand projected horizontally.

In practice, due to intrinsic noise, which includes measurement errors or quantum fluctuations, the experimentally observed values can deviate from the true values as follows:

$$\langle M \rangle_{\text{Exp}} = \langle M \rangle_{\text{True}} \pm (\Delta M), \qquad \theta_{\text{Exp}} = \theta_{\text{True}} \pm (\Delta\theta), \tag{1.3.3}$$

where (ΔM) and $(\Delta\theta)$ represent the standard deviations.

The error propagation formula in Eq. (1.3.1) indicates how the error in M propagates to θ. Higher precision can be achieved by having a larger slope $|\partial_\theta \langle M \rangle|$ and a smaller variance $(\Delta M)^2$.

Collective Bloch sphere: Any N-qubit collective local unitary can be written as

$$U^{\otimes N} = e^{i\boldsymbol{u}\cdot\boldsymbol{J}}, \qquad \boldsymbol{u} = (u_x, u_y, u_z), \qquad \boldsymbol{J} = (J_x, J_y, J_z), \tag{1.3.4}$$

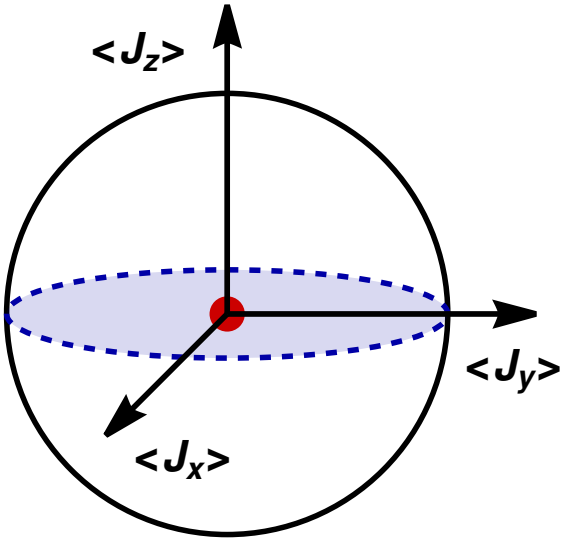

Figure 1.2: Sketch of the collective Bloch sphere with the coordinates (J_x, J_y, J_z), where many-body spin singlet states are at the Red center and the Dicke state is $|D_{N,N/2}\rangle$ shown as the Blue circle.

where $\boldsymbol{u}$ is a three-dimensional unit vector and $\boldsymbol{J}$ is a vector of collective angular momenta in Eq. (1.1.109). A three-dimensional sphere in the coordinates (J_x, J_y, J_z) is known as the collective Bloch sphere [123, 161, 171] in analogy with Bloch sphere in a single-qubit system, illustrated in Fig. 1.2. As we will discuss later, several quantum states are visualized in this sphere, for example, the many-body singlet states are at the Red center and the Dicke state with $m = N/2$ is shown as the Blue circle.

Shot-noise limit: Consider a metrological scenario where an N-qubit state $|0_N\rangle = |0\rangle^{\otimes N}$ is transformed by the dynamics $U_\theta = e^{-i\theta J_y}$ for the collective angular momentum J_y. Here we want to estimate the rotation angle θ, which may be given by, for example, $\theta = \gamma B t$ with the gyromagnetic ratio or a magnetic moment γ, the strength of a magnetic field B pointing to y-direction, and the evolution time t.

By measuring the observable $M = J_x$ on this state, one can obtain the precision in the proximity of $\theta = 0$:

$$(\Delta\theta)^2 \to \frac{1}{N}, \qquad \text{for } \theta \to 0. \tag{1.3.5}$$

This result is known as the shot-noise limit, which is achieved by the so-called fully polarized state (pure product state) $|0_N\rangle$. This result coincides with the scaling of the central limit theorem in Eq. (1.1.168).

Proof. Here we explain this derivation, following the description of Ref. [170].

We begin by writing

$$
\begin{aligned}
e^{+i\theta J_y} J_x e^{-i\theta J_y} &= J_x + (i\theta)[J_y, J_x] + \frac{(i\theta)^2}{2!}[J_y,[J_y, J_x]] + \frac{(i\theta)^3}{3!}[J_y[J_y,[J_y, J_x]]] + \cdots \\
&= \left(1 - \frac{\theta^2}{2!} + \cdots\right) J_x + \left(\theta - \frac{\theta^3}{3!} + \cdots\right) J_z \\
&= \cos(\theta) J_x + \sin(\theta) J_z, \qquad (1.3.6)
\end{aligned}
$$

where we used the Baker–Campbell–Hausdorff formula in Eq. (1.1.226) and the well-known commutation relation $[J_a, J_b] = i\sum_{c=x,y,z} \varepsilon_{abc} J_c$ for $a, b = x, y, z$. Also one has

$$
\begin{aligned}
e^{+i\theta J_y} J_x^2 e^{-i\theta J_y} &= J_x^2 + (i\theta)[J_y, J_x^2] + \frac{(i\theta)^2}{2!}[J_y,[J_y, J_x^2]] + \frac{(i\theta)^3}{3!}[J_y[J_y,[J_y, J_x^2]]] + \cdots \\
&= J_x^2 + \theta(J_z J_x + J_x J_z) - \frac{2\theta^2}{2!}(J_x^2 - J_z^2) - \frac{4\theta^3}{3!}(J_z J_x + J_x J_z) + \cdots \\
&= \left(1 - \frac{2\theta^2}{2!} + \frac{8\theta^4}{4!} + \cdots\right) J_x^2 + \left(\theta^2 - \frac{8\theta^4}{4!} + \cdots\right) J_z^2 \\
&\quad + \left(\theta - \frac{4\theta^3}{3!} + \cdots\right)(J_z J_x + J_x J_z) \\
&= \cos^2(\theta) J_x^2 + \sin^2(\theta) J_z^2 + \frac{1}{2}\sin(2\theta)(J_z J_x + J_x J_z), \qquad (1.3.7)
\end{aligned}
$$

where we used

$$
\begin{aligned}
[J_y, J_x^2] &= [J_y, J_x] J_x + J_x [J_y, J_x] = (-i)(J_z J_x + J_x J_z), \qquad (1.3.8) \\
[J_y,[J_y, J_x^2]] &= (-i)[J_y, J_z J_x + J_x J_z] = \cdots = 2(J_x^2 - J_z^2), \\
[J_y,[J_y,[J_y, J_x^2]]] &= 2[J_y, J_x^2 - J_z^2] = \cdots = 4[J_y, J_x^2],
\end{aligned}
$$

based on the formulas: $[A, BC] = [A, B]C + B[A, C]$ and $[A, B + C] = [A, B] + [A, C]$. These results lead to

$$
\langle M \rangle = \cos(\theta)\langle J_x \rangle_{|0_N\rangle} + \sin(\theta)\langle J_z \rangle_{|0_N\rangle}, \qquad (1.3.9)
$$

$$
\langle M^2 \rangle = \cos^2(\theta)\langle J_x^2 \rangle_{|0_N\rangle} + \sin^2(\theta)\langle J_z^2 \rangle_{|0_N\rangle} + \frac{1}{2}\sin(2\theta)\langle J_z J_x + J_x J_z \rangle_{|0_N\rangle}, \qquad (1.3.10)
$$

where $\langle X \rangle_{|0_N\rangle} \equiv \langle 0_N | X | 0_N \rangle$. Now a straightforward calculation yields

$$
\langle J_x \rangle_{|0_N\rangle} = 0, \qquad \langle J_z \rangle_{|0_N\rangle} = \frac{N}{2}, \qquad (1.3.11)
$$

$$
\langle J_x^2 \rangle_{|0_N\rangle} = \frac{N}{4}, \qquad \langle J_z^2 \rangle_{|0_N\rangle} = \frac{N^2}{4}, \qquad \langle J_z J_x + J_x J_z \rangle_{|0_N\rangle} = 0. \qquad (1.3.12)
$$

Substituting these into the error propagation formula in Eq. (1.3.1), we can arrive the shot-noise limit:

$$
\lim_{\theta \to 0} (\Delta\theta)^2 = \frac{(\Delta J_x)^2_{|0_N\rangle}}{\langle J_z \rangle^2_{|0_N\rangle}} = \frac{1}{N}. \qquad (1.3.13)
$$

□

Spin-squeezed states: Roughly speaking, a state can be called spin-squeezed if it can go beyond the shot-noise limit in collective measurements. Recall the previous metrological setting with the unitary dynamics $U_\theta = e^{-i\theta J_y}$ and the measurement observable $M = J_x$. A higher precision $(\Delta\theta)^2$ can be achieved by a N-qubit spin-squeezed state, which has a smaller variance $(\Delta J_x)^2$ compared with the fully polarized state $|0_N\rangle$.

For the uncertainty relation in Eq. (1.1.203), taking $A = J_x$ and $B = J_y$ leads to

$$(\Delta J_x)^2 (\Delta J_y)^2 \geq \frac{1}{4}|\langle J_z\rangle|^2. \tag{1.3.14}$$

Notice that the fully polarized state saturates this inequality and obeys $(\Delta J_x)^2 = (\Delta J_y)^2 = (1/2)|\langle J_z\rangle| = N/4$. On the other hand, spin-squeezed states can have a smaller variance

$$(\Delta J_x)^2 < \frac{1}{2}|\langle J_z\rangle|. \tag{1.3.15}$$

More generally, the notion of such spin-squeezed states can be defined as

$$\frac{2(\Delta J_{\boldsymbol{m}})^2}{|\langle J_{\boldsymbol{n}}\rangle|} < 1, \tag{1.3.16}$$

for mutually orthogonal unit vectors $\boldsymbol{m}$ and $\boldsymbol{n}$ [311, 312]. To avoid confusion, we should stress that this condition cannot be a unique definition of spin-squeezed states. As discussed below, there are several works that extend the concept of spin squeezing.

The relation between spin squeezing and entanglement can be seen by introducing a parameter

$$\xi = \frac{N(\Delta J_{\boldsymbol{l}})^2}{|\langle J_{\boldsymbol{m}}\rangle|^2 + |\langle J_{\boldsymbol{n}}\rangle|^2}, \tag{1.3.17}$$

where $\boldsymbol{l}$, $\boldsymbol{m}$, and $\boldsymbol{n}$ are orthogonal. In Ref. [159], it has been shown that any N-qubit fully separable state obeys

$$\xi \geq 1. \tag{1.3.18}$$

Conversely, if $\xi < 1$, the state is spin-squeezed and entangled. This allows us to detect metrologically useful multipartite entanglement, beating the shot-noise limit. Other spin-squeezing parameters were also considered, for details see [161, 170, 313, 314].

Generalized spin-squeezing inequalities: Motivated by the above criterion, one can ask: Can we find the most powerful entanglement criteria using the first and second moments of collective angular momenta? Here the first and second moments mean $\langle J_l\rangle$ and $\langle J_l^2\rangle$ for $l = x, y, z$. In Refs. [160, 276], such generalized spin-squeezing inequalities were proposed. Any N-qubit fully separable state

obeys

$$\langle J_x^2\rangle + \langle J_y^2\rangle + \langle J_z^2\rangle \leq \frac{N(N+2)}{4}, \tag{1.3.19}$$

$$(\Delta J_x)^2 + (\Delta J_y)^2 + (\Delta J_z)^2 \geq \frac{N}{2}, \tag{1.3.20}$$

$$\langle J_l^2\rangle + \langle J_m^2\rangle - \frac{N}{2} \leq (N-1)(\Delta J_n)^2, \tag{1.3.21}$$

$$(N-1)\left[(\Delta J_l)^2 + (\Delta J_m)^2\right] \geq \langle J_n^2\rangle + \frac{N(N-2)}{4}, \tag{1.3.22}$$

for l, m, n take all the possible permutations of x, y, z. These were shown to be optimal inequalities for detecting spin-squeezing entanglement in the sense that if the inequality holds for $\langle J_x^2\rangle, \langle J_y^2\rangle$, and $\langle J_z^2\rangle$, then there is a fully separable state compatible with these values [160, 276].

Eq. (1.3.19) is valid for all quantum states. For instance, the fully polarized state can saturate the bound. On the other hand, violation of any of the inequalities in Eqs. (1.3.20, 1.3.21, 1.3.22) implies the presence of multipartite entanglement. In fact, combining all the optimal inequalities can characterize spin-squeezing entanglement very efficiently. In the following, we will discuss what types of entanglement can be detected by these criteria.

Singlet states: The inequalities in Eqs. (1.3.20, 1.3.22) can be maximally violated by the so-called many-body spin singlet states ϱ_{singlet} [160, 275, 276, 315–317]. A pure singlet state is defined as a state invariant under any collective unitary:

$$U^{\otimes N} |\Psi_{\text{singlet}}\rangle = e^{i\theta} |\Psi_{\text{singlet}}\rangle . \tag{1.3.23}$$

That is, it has simultaneous eigenstates of J_l for $l = x, y, z$ with zero eigenvalues. Many-body spin singlet states ϱ_{singlet} are mixtures of pure singlet states and are also invariant under any collective local unitary: $U^{\otimes N} \varrho_{\text{singlet}} (U^\dagger)^{\otimes N} = \varrho_{\text{singlet}}$. Since the state ϱ_{singlet} has $\langle J_l^k\rangle = 0$ for and any integer k, it is at the center of the collective Bloch sphere (Red in Fig. 1.2). Note that other quantum states can also be at the center. Such states can be changed under $U^{\otimes N}$, but their expectations of J_l cannot be changed. Examples are the thermal states of several spin-chain models.

Moreover, their violations are known to detect entanglement very strongly. In fact, it can verify the so-called multiparticle bound entangled states, which cannot be distilled into pure entangled states and can be PPT for all bipartitions [160, 276]. Also, Refs. [318, 319] showed that the inequality in Eq. (1.3.20) can detect many-body Bell nonlocality. Also, Refs. [170, 176, 320] discussed the improvement of the average sensitivity of phase estimation in quantum metrology. In Refs. [321, 322], the high-dimensional generalizations were considered, which can characterize bound entanglement and k-particle entanglement in spin-squeezed states.

Dicke states: The inequality in Eq. (1.3.21) is maximally violated by the symmetric Dicke state $|D_{N,m}\rangle$ with $m = N/2$ in Eq. (1.2.32). Note that the Dicke states are simultaneous eigenstates of the collective angular momentum J_z and the so-called Casimir invariant $J^2 = J_x^2 + J_y^2 + J_z^2$ with $[J_l, J^2] = 0$ for $l = x, y, z$. For the Dicke state $|D_{N,m}\rangle$, the first and second moments are given by

$$\langle J_x \rangle = \langle J_y \rangle = 0, \qquad \langle J_z \rangle = m - \frac{N}{2}, \tag{1.3.24}$$

$$\langle J_x^2 \rangle = \langle J_y^2 \rangle = \frac{N}{4} + \frac{m(N-m)}{2}, \qquad \langle J_z^2 \rangle = \left(m - \frac{N}{2} \right)^2. \tag{1.3.25}$$

In the case of $m = N/2$, since $\langle J_x^2 \rangle, \langle J_y^2 \rangle$ become large at the order of $\mathcal{O}(N^2)$, it can be shown as the Blue circle in Fig. 1.2. This state corresponds to the eigenstate with maximal eigenvalue of J^2, leading to that $\langle J^2 \rangle = N(N+2)/4$. For details, see [323–326].

Heisenberg limit: Consider a metrological scheme where one considers the Dicke state $|D_{N,N/2}\rangle$ as an initial state and measures the observable $M = J_z^2$ after the unitary dynamics $U_\theta = e^{-i\theta J_y}$. In a similar manner to the calculation in the shot-noise limit in Eq. (1.3.5), the precision in the limit of $\theta \to 0$ can be given by

$$(\Delta\theta)^2 \to \frac{1}{N(N+2)}, \qquad \text{for } \theta \to 0. \tag{1.3.26}$$

where we used the results in Ref. [170]. This result is known as the Heisenberg limit, which shows the usefulness of the Dicke state in quantum metrology.

It is important to notice that we used the quadratic collective observable, which contains two-body correlations unlike collective angular momenta J_l. Further extensions to higher-order cases were considered in Ref. [327]. When we measure observables with N-body correlations such as $M = \sigma_x^{\otimes N}$, the GHZ state can also reach the Heisenberg limit.

Symmetric states: A N-particle state ϱ is called permutationally (bosonic) symmetric if it satisfies

$$P_{ab}\varrho = \varrho P_{ab} = \varrho, \tag{1.3.27}$$

for all $a, b \in \{1, 2, \ldots, N\}$. Here P_{ab} is an orthogonal projector onto the so-called symmetric subspace that remains invariant under all the permutations. Note that P_{ab} can be written as $P_{ab} = (\mathbb{1} + \mathbb{S}_{ab})/2$ with the SWAP (flip) operator $\mathbb{S}_{ab} = \sum_{i,j} |ij\rangle\langle ji|$ that can exchange particles a, b. By definition, it holds that

$$\mathbb{S}_{ab}\varrho = \varrho \mathbb{S}_{ab} = \varrho. \tag{1.3.28}$$

The entanglement of permutationally symmetric states has been studied in [89, 187, 198, 323, 328–330]. A permutationally symmetric state ϱ is said to possess

bipartite entanglement or often called spin-squeezed if a two-particle reduced state $\varrho_{ab} = \mathrm{tr}_{(a,b)^c}(\varrho)$ is entangled for all pairs (a,b) with the complement $(a,b)^c$. In previous works [135, 331, 332], such spin-squeezing entanglement has been completely characterized in a necessary and sufficient manner.

We remark that any N-qubit permutationally symmetric state can be written by mixing Dicke states. Then mixed states of Dicke, W, and GHZ states are permutationally symmetric. Also, it is worthwhile to note that any N-particle permutationally symmetric state can be either fully separable or genuinely multipartite entangled (GME) [328, 330].

As a more general concept, a state is called permutationally invariant if

$$\mathbb{S}_{ab}\varrho\mathbb{S}_{ab} = \varrho, \tag{1.3.29}$$

which implies the invariance under the exchange of the particles [198]. The method of state tomography of permutationally invariant states has been discussed [333–335].

Importantly, all permutationally symmetric states are permutationally invariant, but there exist permutationally invariant states that are not permutationally symmetric. Examples of such states are called antisymmetric states that live in an antisymmetric subspace. It was shown that any N-partite antisymmetric state is genuine N-partite entangled, see Lemma 9 in Ref. [187]. An example is the N-particle d-dimensional totally antisymmetric quantum state given by

$$|A_N\rangle = \frac{1}{N!}\sum_{\pi\in \mathrm{Sym}_N} (-1)^{\mathrm{sgn}(\pi)} |\pi_1\rangle \otimes \cdots \otimes |\pi_N\rangle\,, \tag{1.3.30}$$

where π is a permutation in Sym_N and $\mathrm{sgn}(\pi) = 1$ for even permutation and $\mathrm{sgn}(\pi) = -1$ for odd permutation. Note that this state is a singlet state, that is, $U^{\otimes} |A_N\rangle\langle A_N| (U^{\dagger})^{\otimes} = |A_N\rangle\langle A_N|$. For details, see [336–342].

1.3.3 Quantum Fisher information

Classical Cramér–Rao bound: In Sec. 1.1, we discussed classical statistics and explained the estimation of a parameter θ from measurement data. For this purpose, we can create the estimator $\widetilde{\theta} = \widetilde{\theta}(\boldsymbol{x})$ using the measurement outcome $\boldsymbol{x} = \{x_1, x_2, \ldots, x_n\}$. Here the estimator is a function that maps from the data to the parameter. This is a random variable with fluctuating errors: $\widetilde{\theta} = \theta \pm (\text{error})$. It is common to require that the estimator is unbiased, that is,

$$\mathbb{E}[\widetilde{\theta}] = \sum_{\boldsymbol{x}} p_{\boldsymbol{x}}(\theta)\, \widetilde{\theta}(\boldsymbol{x}) = \theta, \tag{1.3.31}$$

where the outcome $\boldsymbol{x}$ occurs with probability $p_{\boldsymbol{x}}(\theta)$ with $\sum_{\boldsymbol{x}} p_{\boldsymbol{x}}(\theta) = 1$. In the estimation theory, the main concern is to reduce the variance denoted as

$$\mathrm{Var}[\widetilde{\theta}] = \sum_{\boldsymbol{x}} p_{\boldsymbol{x}}(\theta)\, [\widetilde{\theta}(\boldsymbol{x}) - \theta]^2. \tag{1.3.32}$$

The classical Cramér–Rao bound tells us that the lower bound of the variance is associated with the classical Fisher information:

$$\mathrm{Var}[\widetilde{\theta}] \geq \frac{1}{\mathcal{F}_C[p_{\boldsymbol{x}}(\theta)]}, \qquad \mathcal{F}_C[p_{\boldsymbol{x}}(\theta)] = \sum_{\boldsymbol{x}} \frac{1}{p_{\boldsymbol{x}}(\theta)} \left(\frac{\partial p_{\boldsymbol{x}}(\theta)}{\partial \theta} \right)^2. \tag{1.3.33}$$

This means that large Fisher information leads to higher precision. The classical Cramér–Rao bound can be shown as follows: We begin by noting that $\partial \mathbb{E}[\widetilde{\theta}]/\partial\theta = 1$. This leads to

$$\begin{aligned} 1^2 &= \left\{ \sum_{\boldsymbol{x}} \frac{\partial p_{\boldsymbol{x}}(\theta)}{\partial \theta} [\widetilde{\theta}(\boldsymbol{x}) - \theta] \right\}^2 \\ &= \left\{ \sum_{\boldsymbol{x}} \frac{\partial \log p_{\boldsymbol{x}}(\theta)}{\partial \theta} \sqrt{p_{\boldsymbol{x}}(\theta)} \sqrt{p_{\boldsymbol{x}}(\theta)} [\widetilde{\theta}(\boldsymbol{x}) - \theta] \right\}^2 \\ &\leq \mathcal{F}_C[p_{\boldsymbol{x}}(\theta)] \cdot \mathrm{Var}[\widetilde{\theta}], \end{aligned} \tag{1.3.34}$$

where we used the Cauchy–Schwarz inequality: $(\sum_x f_x g_x)^2 \leq (\sum_x f_x^2) \cdot (\sum_x g_x^2)$, for $f_x = [\partial \log p_{\boldsymbol{x}}(\theta)/\partial\theta]\sqrt{p_{\boldsymbol{x}}(\theta)}$ and $g_x = \sqrt{p_{\boldsymbol{x}}(\theta)}[\widetilde{\theta}(\boldsymbol{x}) - \theta]$.

Finally, we note that the Fisher information has an additive property for n independent single observations: $\mathcal{F}_C[p_{\boldsymbol{x}}(\theta)] = n\mathcal{F}_C[p_x(\theta)]$. Letting $\mathrm{Var}[\widetilde{\theta}] = (1/n)(\Delta\theta)^2$, this implies that

$$(\Delta\theta)^2 \geq \frac{1}{\mathcal{F}_C[p_x(\theta)]}. \tag{1.3.35}$$

Often this form is also referred as to the classical Cramér–Rao bound.

Quantum Cramér–Rao bound: In quantum mechanics, the probability $p_x(\theta)$ can be obtained from measurements on the state:

$$p_x(\theta) = \mathrm{tr}[\varrho(\theta) M_x], \tag{1.3.36}$$

for POVM measurements $\{M_x\}$ with $M_x \geq 0$ and $\sum_x M_x = \mathbb{1}$. In quantum metrology, it is common to consider that an initial state ϱ is transformed by a unitary transformation U_θ to encode a parameter θ: $\varrho \to \varrho(\theta) = U_\theta \varrho U_\theta^\dagger$ with $U_\theta = e^{-i\theta A}$ with a Hermitian A as the generator of the dynamics.

The quantum Fisher information (QFI) $\mathcal{F}_Q(\varrho, A)$ in Eq. (1.1.201) can be recognized as the maximal quantity of $\mathcal{F}_C[p_x(\theta)]$ over measurements M_x:

$$\max_{M_x} \mathcal{F}_C[p_x(\theta)] = \mathcal{F}_Q(\varrho, A). \tag{1.3.37}$$

This immediately results in the quantum Cramér–Rao bound in Eq. (1.3.2).

Proof. Here we explain this derivation, following the description of Ref. [92]. We begin by rewriting the classical Fisher information as $\mathcal{F}_C[p_x(\theta)] = \sum_x p_x(\theta) L_c^2$

with $L_c = [1/p_x(\theta)][dp_x(\theta)/d\theta]$. This expression leads to $dp_x(\theta)/d\theta = p_x(\theta)L_c$. As the derivative of the quantum state, consider the symmetric form:

$$\frac{\partial \varrho(\theta)}{\partial \theta} = \frac{1}{2}L(\theta)\varrho(\theta) + \frac{1}{2}\varrho(\theta)L(\theta), \tag{1.3.38}$$

with a Hermitian $L(\theta) = L(\theta)^\dagger$. According to Eq. (1.3.36), we can thus immediately obtain

$$\begin{aligned}\frac{dp_x(\theta)}{d\theta} &= \frac{1}{2}\mathrm{tr}\left[L(\theta)\varrho(\theta)M_x\right] + \frac{1}{2}\mathrm{tr}\left[\varrho(\theta)L(\theta)M_x\right] \\ &= \mathrm{Re}\left\{\mathrm{tr}\left[L(\theta)\varrho(\theta)M_x\right]\right\} \\ &\leq \left|\mathrm{tr}\left[L(\theta)\varrho(\theta)M_x\right]\right| = \left|\mathrm{tr}\left[\sqrt{\varrho(\theta)}\sqrt{M_x}\sqrt{M_x}L(\theta)\sqrt{\varrho(\theta)}\right]\right|,\end{aligned}$$

where we used $\mathrm{tr}(A^\dagger) = [\mathrm{tr}(A^\top)]^* = [\mathrm{tr}(A)]^*$ for an operator A and $\mathrm{Re}[z] = (z+z^*)/2 \leq \sqrt{zz^*} = |z|$ for a complex z. Let us apply the Cauchy–Schwarz inequality: $|\mathrm{tr}(X^\dagger Y)|^2 \leq \mathrm{tr}(X^\dagger X)\cdot\mathrm{tr}(Y^\dagger Y)$. Taking $X^\dagger = \sqrt{\varrho(\theta)}\sqrt{M_x}$ and $Y = \sqrt{M_x}L(\theta)\sqrt{\varrho(\theta)}$ leads to

$$\left(\frac{dp_x(\theta)}{d\theta}\right)^2 \leq p_x(\theta)\cdot\mathrm{tr}\left[L(\theta)M_xL(\theta)\varrho(\theta)\right]. \tag{1.3.39}$$

Substituting this result to the classical Fisher information $\mathcal{F}_C[p_x(\theta)]$, we have

$$\mathcal{F}_C[p_x(\theta)] \leq \mathrm{tr}[\varrho(\theta)L^2(\theta)] \equiv \mathcal{F}_Q(\varrho, A), \tag{1.3.40}$$

where we used that $\sum_x M_x = \mathbb{1}$. By definition, the element of $L(\theta)$ can be expressed using the eigenvalue decomposition $\varrho(\theta) = \sum_i p_i |\psi_i\rangle\langle\psi_i|$: $L_{ij} = [2/(p_i + p_j)][\partial_\theta\varrho(\theta)]_{ij}$. A similar calculation with the paragraph of "Quantum Fisher metric" in Sec. 1.1.6 yields the same form with Eq. (1.1.201):

$$\mathcal{F}_Q(\varrho, A) = \sum_{i,j} p_i L_{ij}L_{ji} = 2\sum_{i,j}\frac{(p_i - p_j)^2}{p_i + p_j}|\langle\psi_i|A|\psi_j\rangle|^2. \tag{1.3.41}$$

□

Optimality: Let us discuss the optimal measurements, which can achieve the equality $\mathcal{F}_C[p_x(\theta)] = \mathcal{F}_Q(\varrho, A)$. This equality holds if and only if (i) the term $\mathrm{tr}\left[L(\theta)\varrho(\theta)M_x\right]$ is real and (ii) the Cauchy–Schwarz inequality is saturated, that is, $Y = cX$, equivalently, $\sqrt{M_x}L(\theta)\sqrt{\varrho(\theta)} = c\sqrt{M_x}\sqrt{\varrho(\theta)}$. Thus, the measurements $\{M_x\}$ must be a set of projectors onto the eigenvectors of $L(\theta)$, which depends on an unknown parameter. This is the main reason why finding optimal measurement schemes in quantum metrology is challenging. For details, see [343].

Properties of quantum Fisher information: Here we summarize several properties of the QFI.

- Convexity: The QFI is convex for a quantum state:

$$\mathcal{F}_Q\left(\sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|, A\right) \leq \sum_i p_i \mathcal{F}_Q\left(\left|\psi_i\right\rangle\left\langle\psi_i\right|, A\right). \tag{1.3.42}$$

  This implies that the QFI is always maximized by pure states.

- Commutativity: If ϱ and A commute each other, that is, $[\varrho, A] = 0$, then one has that $\mathcal{F}_Q(\varrho, A) = 0$ (Also, $\mathcal{F}_Q = 0$ leads to $[\varrho, A] = 0$). That is, the state with the same eigenvectors as the generator A in the unitary parameter encoding is not sensitive and therefore not useful. For details, see [170].

- Variance: For any quantum state ϱ the upper bound of the QFI is given by the variance:

$$\mathcal{F}_Q(\varrho, A) \leq 4(\Delta A)^2_\varrho, \tag{1.3.43}$$

  where equality can be saturated by pure states. This allows us to know the best achievable precision by calculating the variance. For details, see [344–346].

- Variance's upper bound: For any state ϱ and Hermitian operator A, the upper bound of the variance $(\Delta A)^2$ is given by

$$(\Delta A)^2 \leq \frac{1}{4}\left(a_{\max} - a_{\min}\right)^2, \tag{1.3.44}$$

  where $a_{\max}, a_{\min}$ are respectively the maximal and minimal eigenvalues of A.

  Proof. This can be shown as follows: Since $a_{\min}\mathbb{1} \leq A \leq a_{\max}\mathbb{1}$, we have

$$0 \leq \langle (a_{\max}\mathbb{1} - A)(A - a_{\min}\mathbb{1})\rangle. \tag{1.3.45}$$

  This leads to $\langle A^2\rangle \leq \langle A\rangle(a_{\max} + a_{\min}) - a_{\max}a_{\min}$. Substituting this inequality to the variance $(\Delta A)^2 = \langle A^2\rangle - \langle A\rangle^2$ yields

$$(\Delta A)^2 \leq (a_{\max} - \langle A\rangle)(\langle A\rangle - a_{\min}). \tag{1.3.46}$$

  Applying the inequality of arithmetic and geometric means $xy \leq [(x + y)/2]^2$ can complete the proof. Note that this proof is similar to the derivation of the so-called Popoviciu inequality [347], as well as the Bhatia–Davis inequality [348, 349]. □

- Optimal state: The inequality in Eq. (1.3.44) can be achieved by the state

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|a_{\max}\right\rangle + \left|a_{\min}\right\rangle\right), \tag{1.3.47}$$

  where $\left|a_{\max}\right\rangle$ and $\left|a_{\min}\right\rangle$ are the normalized eigenvectors with the eigenvalues $a_{\max}$ and $a_{\min}$.

Heisenberg limit: Consider a metrological scenario where a parameter encoding is given by a local unitary

$$U_L = e^{-i\theta A_L}, \qquad A_L = \sum_{i=1}^{N} A_i \otimes \mathbb{1}_{\bar{i}}, \tag{1.3.48}$$

where A_i are the generator acting on i-th subsystem and assumed to be the same for any i. Note that the eigenvalues $a_{\max}$ and $a_{\min}$ of the operator A_L and the corresponding eigenvectors are given by

$$a_{\max} = N\lambda_{\max}, \qquad |a_{\max}\rangle = |\lambda_{\max}\rangle^{\otimes N}, \tag{1.3.49}$$

$$a_{\min} = N\lambda_{\min}, \qquad |a_{\min}\rangle = |\lambda_{\min}\rangle^{\otimes N}, \tag{1.3.50}$$

where $\lambda_{\max}$ and $\lambda_{\min}$ are the eigenvalues of the operator A_i with the eigenvalues $|\lambda_{\max}\rangle$ and $|\lambda_{\min}\rangle$. With the help of the above properties of the QFI, it holds that

$$\mathcal{F}_Q(\varrho, A) \leq \max_{|\phi\rangle} \mathcal{F}_Q(|\phi\rangle, A) \tag{1.3.51}$$

$$= \max_{|\phi\rangle} 4(\Delta A)^2_\phi \tag{1.3.52}$$

$$\leq (a_{\max} - a_{\min})^2 = N^2(\lambda_{\max} - \lambda_{\min})^2, \tag{1.3.53}$$

which can be achieved by the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_{\max}\rangle^{\otimes N} + |\lambda_{\min}\rangle^{\otimes N}\right). \tag{1.3.54}$$

As an example, take the collective angular momentum $A = J_l$ for $l = x, y, z$, where $\lambda_{\max} = 1/2$ and $\lambda_{\min} = -1/2$. Then the minimal precision in this case coincides with the Heisenberg limit:

$$(\Delta\theta)^2 \geq \frac{1}{N^2}. \tag{1.3.55}$$

This is the fundamental ultimate bound in quantum mechanics in the case of the local Hamiltonian dynamics with J_l. For the case with J_z, since $|\lambda_{\max}\rangle = |0\rangle$ and $|\lambda_{\min}\rangle = |1\rangle$, the Heisenberg limit is achieved by the GHZ state.

Separability criteria: A large value of the QFI signals the presence of multiparticle entanglement. Now one may ask: Can we find the separability bound on the QFI? This question has been addressed in Ref. [169] (also see [286]) and later extended to more general concepts of separability, known as k-producibility [176, 320].

Let us recall the form of a fully separable state: $\varrho_{\text{fs}} = \sum_i p_i \varrho_i^{(1)} \otimes \varrho_i^{(2)} \otimes \cdots \otimes \varrho_i^{(N)}$ in Eq. (1.2.22). Any N-qubit fully separable state obeys

$$\mathcal{F}_Q(\varrho_{\text{fs}}, J_l) \leq N. \tag{1.3.56}$$

Violation of this inequality implies that the state is multiparticle entangled. Similarly to Eq. (1.3.53), this criterion can be shown as follows:

$$\mathcal{F}_Q\left(\varrho_{\rm fs}, J_l\right) \leq \max_{|\psi_{\rm fs}\rangle} \mathcal{F}_Q\left(|\psi_{\rm fs}\rangle, J_l\right) = 4(\Delta J_l)^2_{\psi_{\rm fs}} = \sum_{i=1}^{N} (\Delta \sigma_l^{(i)})^2_{\psi_i} \leq N, \tag{1.3.57}$$

which is based on the description of Ref. [169, 288].

Super-Heisenberg limit: In order to reach the Heisenberg limit in the case of a local unitary parameter encoding, initial entanglement is necessary. On the other hand, if a parameter encoding is given by a unitary for a nonlinear k-body interaction coupling, even initial product states can achieve and go beyond the quadratic scaling. In general, it is possible to achieve the following scaling:

$$(\Delta\theta)^2 \sim \frac{1}{N^{2k}}. \tag{1.3.58}$$

This is known as the super-Heisenberg limit, which can suggest that entangling transformations are also metrologically relevant. Roughly speaking, this scaling can be proportional to the number of terms in the corresponding generator in the dynamics.

Let us explain the super-Heisenberg limit in more detail, following the description of Refs. [290, 292]. For other references, see [291, 293, 294]. Consider an unitary $U_k = \exp[-i\theta A^{(k)}]$ with

$$A^{(k)} = \left(\sum_{i=1}^{N} A_i\right)^k = \sum_{\rm wt=k} A_{i_1} A_{i_2} \cdots A_{i_k} + \mathcal{O}(N^{k-1}), \tag{1.3.59}$$

where the summation is taken over all subsets of k systems, weight, wt is the number of non-zero indices. With the help of Eq. (1.3.44, it is sufficient to show that the upper bound of the variance scales with order $\mathcal{O}(N^{2k})$. To proceed, let us denote the operator semi-norm of a Hermitian X as

$$\|X\|_{\rm sn} = x_{\max} - x_{\min}, \tag{1.3.60}$$

where $x_{\max}, x_{\min}$ are the maximal and minimal eigenvalues of X. This norm has the triangle inequality, that is, $\|X+Y\|_{\rm sn} \leq \|X\|_{\rm sn} + \|Y\|_{\rm sn}$. This may lead to

$$\left\|A^{(k)}\right\|_{\rm sn} \sim \| \sum_{\rm wt=k} A_{i_1} A_{i_2} \cdots A_{i_k} \|_{\rm sn} \sim \binom{N}{k} \left\|A_{i_1} A_{i_2} \cdots A_{i_k}\right\|_{\rm sn} \sim \frac{N^k a_k}{k!} \sim \mathcal{O}(N^k), \tag{1.3.61}$$

where we used the well-known Stirling approximation for large N and small k/N and denoted $a_k = \lambda_{\max}^k - \lambda_{\min}^k$ for $\lambda_{\max}$ and $\lambda_{\min}$ the maximal and minimal eigenvalues of the operator A_i. Finally, we note that the terminology of the super-Heisenberg limit has been discussed in Refs. [296, 297].

1.4 Randomized measurements

In this section, we will give a brief introduction to randomized measurements. Roughly and informally speaking, randomized measurements are methods to implement SWAP operators indirectly in an experimentally-friendly manner. More precisely, the scheme of randomized measurements allows us to generate the SWAP operator $\mathbb{S}$, or more generally the permutation operator W_π in Sec 1.1, via Haar random unitary integrals, and the resulting quantities are invariants under local unitaries, which can give advantages for the analysis of quantum systems. This section is based on the description of Ref. [7].

1.4.1 General schemes

Motivations: Quantum technology has advanced rapidly, enabling the manipulation of complex quantum systems. However, as the number of particles increases, the analysis of quantum states becomes increasingly challenging, due to the exponentially increasing dimension of Hilbert space. To address this challenge, methods using random unitary rotations in the measurement direction have been discussed. By studying the moments of the resulting probability distribution, valuable information about the state can be obtained for the analysis of quantum systems. This method, called randomized measurement, offers several advantages:

- Unnecessity of state tomography: Randomized measurements do not require precise knowledge of the elements of the density matrix as a complete mathematical description of the system. This eliminates the need for tomographic reconstruction of the quantum state and significantly reduces the required measurement resources. This point is crucial for the efficient and reliable characterization of multipartite systems.

- Valuable in the absence of prior information: Random measurements are useful in situations where prior information about the state is not available. This is advantageous when one does not know the type of entangled state produced or when dealing with larger and noisier quantum systems. Random measurements can overcome situations where standard methods of entanglement witnesses or Bell inequalities are inadequate.

- Independence of common reference frame: Randomized measurements are effective when control over quantum systems is limited. They do not require careful calibration and alignment of measurement directions or the sharing of a common frame of reference between spatially separated parties. This feature can save operational resources, as establishing a common frame of reference can be resource-intensive in practice [100] and Sec. 1.1.

- Adaptability to noisy environments: Randomized measurements are insensitive to unknown local unitary noise, such as magnetic field fluctuations or rotational polarizations of optical fibers along communication channels

for the transmission of states. This insensitivity can even be achieved by deliberately applying uniformly random rotations, which can wash away unexpected, distorted noise effects that occur in actual experiments.

General formalism: Here we explain the general formalism of randomized measurements in terms of t-th moments in N-particle d-dimensional quantum systems. Let us begin by considering a situation where N parties share a N-qudit quantum state $\varrho \in \mathcal{H}_d^{\otimes N}$ but no common reference frame. To analyze the state in this situation, they first perform a measurement with an observable $\mathcal{M}$ and rotate each party's measurement direction in an arbitrary manner. The expectation can be expressed in the form

$$E(\mathcal{M}, U_1 \otimes \cdots \otimes U_N) = \mathrm{tr}\left[\varrho (U_1 \otimes \cdots \otimes U_N)^\dagger \mathcal{M} (U_1 \otimes \cdots \otimes U_N)\right]. \tag{1.4.1}$$

This expectation function depends not only on ϱ and $\mathcal{M}$ but also on the choice of local unitaries $U_1 \otimes \cdots \otimes U_N$. Here the unitary matrix U_i is defined in the d-dimensional unitary group acting on the i-th subsystem for $i = 1, \ldots, N$. The key idea to proceed is to take a sample over random unitaries and consider the resulting probability distribution of $E(\mathcal{M}, U_1 \otimes \cdots \otimes U_N)$. This probability distribution can contain valuable information about the state and be characterized by its moments

$$\mathcal{R}_{\mathcal{M}}^{(t)}(\varrho) = \mathcal{N}_{N,d,t} \int dU_1 \cdots \int dU_N \, [E(\mathcal{M}, U_1 \otimes \cdots \otimes U_N)]^t, \tag{1.4.2}$$

where the integral is taken according to the Haar measure dU, for details see the paragraph of "Twirling operations" in Sec. 1.1.4. Here, we denote $\mathcal{N}_{N,d,t}$ as a suitable normalization constant, which is defined differently across the literature. In the following, we will summarize several remarks.

- Local unitary invariance: By definition, the moments are invariant under any local unitary transformation. More precisely, since the Haar measure is invariant under left and right translation, it holds that

  $$\mathcal{R}_{\mathcal{M}}^{(t)}(\varrho) = \mathcal{R}_{\mathcal{M}}^{(t)}(V_1 \otimes \cdots \otimes V_N \, \varrho \, V_1^\dagger \otimes \cdots \otimes V_N^\dagger), \tag{1.4.3}$$

  for any local unitary $V_1 \otimes \cdots \otimes V_N$. Thus, we can characterize the state ϱ with the moments $\mathcal{R}^{(t)}(\varrho)$ in a local-basis-independent manner, that is, independent of reference frames between parties or unknown local unitary noise. This invariance is one of the most important properties of randomized measurements and suggests that the moments of the measured distributions contain essential information about the entanglement of the corresponding quantum states.

- Choice of observables: In general, there are two ways to choose the observable $\mathcal{M}$: One is to take a product observable of the form

  $$\mathcal{M}_{\mathrm{P}} = M_1 \otimes M_2 \otimes \cdots \otimes M_N, \tag{1.4.4}$$

where this is a simple choice and has been used in many works. On the other hand, the observable can be of the more general (non-product) form

$$\mathcal{M}_{\mathrm{NP}} = \sum_i m_i M_1^{(i)} \otimes M_2^{(i)} \otimes \cdots \otimes M_N^{(i)}, \tag{1.4.5}$$

with real coefficients m_i [6, 80]. In several cases, the measurement of non-product observables can be advantageous to extract further information about the state.

- Marginal moments: By discarding the measurements of some parties, one can obtain the marginal moments of the reduced states of ϱ. To illustrate this, let us consider a three-particle state ϱ_{ABC} and discard the measurements of the parties B and C, that is, $M_B = M_C = \mathbb{1}$. This yields the corresponding one-body marginal moments $\mathcal{R}_A^{(t)}(\varrho_A)$ of the party A. On the other hand, the case of $M_C = \mathbb{1}$ yields the two-body marginal moments $\mathcal{R}_{AB}^{(t)}(\varrho_{AB})$ of the parties A and B. Here, ϱ_A, ϱ_{AB} are the one and two-body reduced states of ϱ_{ABC}, respectively. Clearly, in the case with $M_X \neq \mathbb{1}$ for $X = A, B, C$, the full three-body moments $\mathcal{R}_{ABC}^{(t)}(\varrho_{ABC})$ are available. Similarly, all the k-body moments for $k \in [1, N]$ can be accessed by discarding the corresponding measurements of $(N-k)$ parties. In particular, the averaging over all second-order k-body moments with product observables yields the k-body sector length S_k, which will be explained later.

- Challenging issues: If higher-order moments are further taken into account, detailed information can be extracted allowing for more powerful entanglement detection methods. However, on a more technical level, this requires at least two additional steps. First, since the moments generally depend on the choice of observables, the definition of the moments relies on finding suitable families of observables with the same spectra, i.e., local unitary equivalent observables. In the case of $t = 2$, the moments are indeed independent of the choice of measurement observables, as long as the observables are traceless [1, 350], while this is not the case in general [1, 258].

  The next step is to search for entanglement criteria using the evaluated higher-order moments. Intuitively, one can power up entanglement detection by combining, for example, $\mathcal{R}^{(2)}$ and $\mathcal{R}^{(4)}$ instead of using only $\mathcal{R}^{(2)}$. To this end, one should systematically search for the most effective combination of such nonlinear functions. Addressing the above issues is not trivial and will be considered in more detail later.

- Qubits: For the qubit case, $d = 2$, the Haar unitary integrals can be replaced by integrals with respect to the uniform measure on the Bloch sphere:

$$\int dU \to \frac{1}{4\pi} \int d\mathbf{u} \tag{1.4.6}$$

with $d\mathbf{u} = \sin(\theta)d\theta d\phi$. With the help of quantum designs, one may simplify the integrals as sums over certain directions on the Bloch sphere.

1.4.2 Sector lengths

Definition: Recall the generalized Bloch decomposition of a N-qudit state in Eqs. (1.1.101, 1.1.103), where $a_{i_1\cdots i_N}$ is defined as the k-fold tensor, that is, the entries for which k indices are non-zero, for $1 \leq k \leq N$. Sector lengths are defined as follows [351]:

$$S_k(\varrho) = \sum_{k \text{ non-zero indices}} a^2_{i_1\cdots i_N} = \frac{1}{d^N}\mathrm{tr}(P_k^2), \tag{1.4.7}$$

where $S_0 = 1$ due to the normalization condition $\mathrm{tr}(\varrho) = 1$. The sector lengths S_k quantify the amount of k-body quantum correlations in the state ϱ.

In the simplest case, if we consider a single-qudit state, then we know that $S_1 = |\boldsymbol{a}|^2$, see Eq. (1.1.24). As mentioned, this length quantifies the degree of mixing of the state, which encodes information about the state obtained in a basis-independent way. The sector lengths are its direct extension to multipartite quantum systems.

For example, consider the two-qubit Bell state $|\mathrm{Bell}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and the three-qubit GHZ state $|\mathrm{GHZ}_3\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. Since their Bloch decompositions are given by

$$\varrho_{\mathrm{Bell}} = \frac{1}{4}(\mathbb{1} + X_1X_2 - Y_1Y_2 + Z_1Z_2)\,, \tag{1.4.8}$$

$$\varrho_{\mathrm{GHZ}_3} = \frac{1}{8}(\mathbb{1} + Z_1Z_2 + Z_1Z_3 + Z_2Z_3 + X_1X_2X_3 - X_1Y_2Y_3 - Y_1X_2Y_3 - Y_1Y_2X_3)\,, \tag{1.4.9}$$

where we abbreviate the notation of the tensor product and denote X_i, Y_i, Z_i as Pauli matrices acting on i-th subsystem. Then the Bell state has $(S_1, S_2) = (0, 2)$ and the GHZ state has $(S_1, S_2, S_3) = (0, 3, 4)$.

Properties of sector lengths: Here we summarize several useful properties of sector lengths.

- Local unitary invariance: The sector lengths are invariant under any local unitary transformation. That is, for a local unitary $V_1 \otimes \cdots \otimes V_N$, it holds that
$$S_k(\varrho) = S_k\big(V_1 \otimes \cdots \otimes V_N \varrho V_1^\dagger \otimes \cdots \otimes V_N^\dagger\big). \tag{1.4.10}$$
- Convexity: The sector lengths are convex on quantum states. That is, for the mixed quantum state $\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, it holds that
$$S_k\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) \leq \sum_i p_i S_k(|\psi_i\rangle). \tag{1.4.11}$$

- Convolution: The sector lengths have a convolution property [352]: For a N-particle product state $\varrho_P \otimes \varrho_Q$, where ϱ_P and ϱ_Q are, respectively, j-particle and $(N-j)$-particle states, we have

$$S_k(\varrho_P \otimes \varrho_Q) = \sum_{i=0}^{k} S_i(\varrho_P) S_{k-i}(\varrho_Q). \tag{1.4.12}$$

- Purity: The sector lengths are directly associated with the purity of ϱ, namely

$$\mathrm{tr}(\varrho^2) = \frac{1}{d^N} \sum_{k=0}^{N} S_k(\varrho). \tag{1.4.13}$$

  That is, the purity can be decomposed into the sector lengths of different orders. Using this relation, the sector lengths can be always represented as the purities of reduced states of ϱ, and vice versa.

- Maximal value: The N-body (often called full-body) sector length S_N for all N-qubit states has been shown to be always maximized by the N-qubit GHZ state, denoted by $|\mathrm{GHZ}_N\rangle = (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$. Its maximal value is given by

$$S_n(\mathrm{GHZ}_N) = 2^{N-1} + \delta_{N,\mathrm{even}}, \tag{1.4.14}$$

  see [350, 353, 354]. However, this is not always true in higher dimensions, that is, quantum states that are not of the GHZ form can attain the maximal S_N value [353]. Even more interestingly, it has been demonstrated that there exist multipartite entangled states with zero S_N for an odd number of qubits [355–359].

- Randomized measurements: The sector lengths can be directly obtained from the randomized measurement scheme. In fact, the k-body sector lengths S_k can be represented as averages over all second-order moments of random correlations in k-particle subsystems. The entanglement criteria using the sector lengths are therefore accessible with randomized measurements.

- Demonstration: Consider the scheme of randomized measurements on N-qubit systems with the product observable $\mathcal{M}_\mathrm{P} = \sigma_z \otimes \cdots \otimes \sigma_z$. Let $\boldsymbol{u} \cdot \boldsymbol{\sigma} = U\sigma_z U^\dagger$ be the randomized Pauli matrix with a unit real vector $\boldsymbol{u} = (u_x, u_y, u_z)$ for $|\boldsymbol{u}|^2 = 1$ and the vector of Pauli matrices $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Then the second moment in Eq. (1.4.2) can be written as

$$\mathcal{R}^{(2)} = \left(\frac{3}{4\pi}\right)^N \int d\boldsymbol{u}_1 \cdots \int d\boldsymbol{u}_N \, E^2(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N), \tag{1.4.15}$$

  where we chose the normalization constant $\mathcal{N}_{N,2,2} = 3^N$ and

$$E(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N) = \mathrm{tr}(\varrho \, \boldsymbol{u}_1 \cdot \boldsymbol{\sigma} \otimes \cdots \otimes \boldsymbol{u}_N \cdot \boldsymbol{\sigma}). \tag{1.4.16}$$

This integral can be simply evaluated as

$$\mathcal{R}^{(2)} = \sum_{i_1,\ldots,i_N=x,y,z} \mathrm{tr}[\varrho(\sigma_{i_1} \otimes \cdots \otimes \sigma_{i_N})]^2 = S_N, \tag{1.4.17}$$

which coincides with the full-body sector length S_N.

Positivity constraints: In Refs. [352, 353, 360], it has been discussed that there are several relations that can limit the allowable ranges of sector lengths in N-qubit systems. Here we explain several positivity constraints, following the description of Ref. [352]:

- Purity identities: For pure states, it holds that

$$M_m \equiv 2^m \sum_{j=0}^{N-m} \binom{N-j}{m} S_j - 2^{N-m} \sum_{j=0}^{m} \binom{N-j}{N-m} S_j = 0, \tag{1.4.18}$$

  with integer $m = 0, \ldots, \lfloor (N-1)/2 \rfloor$. These identities can be derived using the Schmidt decomposition and taking summations over all subsets. In particular, the case $M_m = 0$.

- Upper bounds: For some N-qubit states, it holds that

$$S_1 \leq N, \qquad \text{for } N \geq 1, \tag{1.4.19}$$

$$S_2 \leq \binom{N}{2}, \qquad \text{for } N \geq 3, \tag{1.4.20}$$

$$S_3 \leq \binom{N}{3}, \qquad \text{for } N \geq 5. \tag{1.4.21}$$

  These inequalities can be saturated by any N-qubit pure product state since $(|0\rangle\langle 0|)^{\otimes N} = (\mathbb{1} + \sigma_z/2)$ leads to respectively N, $\binom{N}{2}$, and $\binom{N}{3}$ terms.

- Universal state inversion: For N-qubit states, it holds that

$$B_0 \equiv \frac{1}{2^N} \sum_{r=0}^{N} (-1)^r S_r \geq 0. \tag{1.4.22}$$

  This can be derived using the generalized universal state inversion discussed in Eq. (1.1.134), $\varrho_{B_0} \equiv \bigotimes_{i=1}^{N} \mathcal{S}_d^{(i)}(\varrho)$, and by calculating $\mathrm{tr}[\varrho\varrho_{B_0}] \geq 0$ due to $\varrho_{B_0} \geq 0$.

- Shadow inequalities: For $k = 0, \ldots, N$, it holds that

$$B_k \equiv \frac{1}{2^N} \sum_{r=0}^{N} (-1)^r K_k(r; N) S_r \geq 0, \tag{1.4.23}$$

where $K_k(r;N)$ are called the Kravchuk polynomials given by

$$K_k(r;N) = \sum_{j=0}^{k} (-1)^j 3^{k-j} \binom{r}{j} \binom{N-r}{k-j}. \tag{1.4.24}$$

These inequalities can be derived using the so-called shadow inequalities, which allow us to create positive maps in a symmetric manner as extensions of universal state inversions. For details, see [361–365].

- Wyderka and Gühne bound [352]: for $N \geq 3$, it holds that

$$\binom{N}{3} - \frac{1}{3}\binom{N-1}{2} S_1 - \frac{1}{3}\binom{N-2}{1} S_2 + S_3 \geq 0. \tag{1.4.25}$$

- Tight bounds: For three-qubit states, it holds that

$$0 \leq S_1 \leq 3, \quad 0 \leq S_2 \leq 3, \quad 0 \leq S_3 \leq 4, \tag{1.4.26}$$
$$S_1 + S_2 + S_3 \leq 7, \quad S_1 - S_2 + S_3 \leq 1, \tag{1.4.27}$$
$$S_1 + S_2 \leq 3 + 3S_3. \tag{1.4.28}$$

The most of inequalities can come from the above inequalities, while the last inequality $S_1 + S_2 \leq 3 + 3S_3$ was nontrivially founded by a semidefinite program [352]. These inequalities enable us to consider the geometry of the three-qubit state space in terms of the sector lengths (S_1, S_2, S_3). In the total polytope, the set of all states can be characterized by tight bounds.

1.4.3 Local unitary invariants

Definition: Let $f(\varrho)$ be a function of a N-qudit state ϱ. The state's function $f(\varrho)$ is called local unitary (LU) invariant if

$$f\left(V_1 \otimes \cdots \otimes V_N \varrho V_1^\dagger \otimes \cdots \otimes V_N^\dagger\right) = f(\varrho), \tag{1.4.29}$$

for any local unitary $V_1 \otimes \cdots \otimes V_N$. For instance, the sector lengths are special examples of LU invariants. Since the purity of the global state $\mathrm{tr}(\varrho^2)$ is invariant under any global unitary, one can interpret the relation in Eq. (1.4.13) as a decomposition of a global unitary invariant into LU invariants.

The second-order Rényi entropy in Eq. (1.2.54) is another example of LU invariants. More generally, the Rényi entropy of order α is defined as (see [206]):

$$H_\alpha(\varrho) = \frac{1}{1-\alpha} \log\left[\mathrm{tr}(\varrho^\alpha)\right]. \tag{1.4.30}$$

Makhlin invariants: Let us begin by recalling that two quantum states ϱ and σ are called LU equivalent if and only if there exists local unitary operation $U_A \otimes U_B$ such that

$$\varrho = (U_A \otimes U_B)\sigma(U_A^\dagger \otimes U_B^\dagger). \tag{1.4.31}$$

Clearly, two LU equivalent states have the same values of LU invariants. Conversely, one may ask whether there is a (finite) set of LU invariants, such that two states are LU equivalent if they have the same values for these invariants. In two-qubit systems, this question was answered by Makhlin [366].

It has been shown that two two-qubit states ϱ and σ are LU equivalent if and only if they have equal values of all LU invariants $I_1, \ldots, I_{18}$, nowadays called the Makhlin invariants. To express them, we recall the Bloch decomposition of a two-qubit state in Eq. (1.1.100) with $d = 2$:

$$\varrho_{AB} = \frac{1}{4}\left(\mathbb{1}_2^{\otimes 2} + \sum_{i=1}^{3} a_i\lambda_i \otimes \mathbb{1}_2 + \sum_{i=1}^{3} b_i \mathbb{1}_2 \otimes \lambda_i + \sum_{i,j=1}^{3} t_{ij}\lambda_i \otimes \lambda_j\right), \tag{1.4.32}$$

where we denote the local Bloch vectors as $\boldsymbol{a}, \boldsymbol{b}$ and the correlation matrix as T. The Makhlin invariants are written as

$$I_4 = a^2, \qquad I_7 = b^2, \qquad I_2 = \mathrm{tr}(TT^\top), \tag{1.4.33}$$

$$I_{12} = \boldsymbol{a}^\top T\boldsymbol{b}, \qquad I_1 = \det(T), \tag{1.4.34}$$

$$I_5 = [\boldsymbol{a}T]^2, \qquad I_8 = [T\boldsymbol{b}]^2, \qquad I_3 = \mathrm{tr}(TT^\top TT^\top), \tag{1.4.35}$$

$$I_{14} = \mathrm{tr}(H_a T H_b^\top T^\top), \tag{1.4.36}$$

$$I_{13} = \boldsymbol{a}^\top TT^\top T\boldsymbol{b}, \qquad I_6 = [\boldsymbol{a}TT^\top]^2, \qquad I_9 = [T^\top T\boldsymbol{b}]^2, \tag{1.4.37}$$

where $a^2 = |\boldsymbol{a}|^2$, $b^2 = |\boldsymbol{b}|^2$, and $(H_x)_{ij} = \sum_{k=x,y,z} \varepsilon_{ijk}x_k$ with the Levi-Civita symbol ε_{ijk} for $x = a, b$. Here, the first row includes all LU invariants of degree two, the second row includes those of degree three, the third and fourth rows include those of degree four, and the last row contains those of degrees five and six.

Quantification of negativity: A typical entanglement measure in two-qubit systems is the negativity [279], which is defined as

$$N(\varrho) = -2\min\{0, \mu(\varrho^{\top_B})\}, \tag{1.4.38}$$

where $\mu(\varrho^{\top_B})$ is the minimal eigenvalue of the partial transpose state $\varrho^{\top_B}$. With the help of Newton's identities, this eigenvalue can be calculated by the k-th moments given by $p_k = \mathrm{tr}[(\varrho^{\top_B})^k]$.

It has been shown that the negativity can be obtained by solving the following fourth-degree polynomial for N [367]:

$$48\det(\varrho^{\top_B}) + 3N^4 + 6N^3 - 6N^2(p_2 - 1) - 4N(3p_2 - 2p_3 - 1) = 0. \tag{1.4.39}$$

We remark that the determinant $\det(\varrho^{\top_B})$ can be rewritten in terms of the moments p_k via [197]

$$\det(\varrho^{\top_B}) = \frac{1}{24}(1 - 6p_4 + 8p_3 + 3p_2^2 - 6p_2). \tag{1.4.40}$$

Note that $\det(\varrho^{\top_B}) < 0$ is a necessary and sufficient condition for two-qubit entangled states, see Eq. (1.2.46). Therefore, to quantify the negativity, it is sufficient to use known relations between the p_k and the Makhlin invariants [368]:

$$p_2 = \frac{1}{4}(1 + x_1), \tag{1.4.41}$$

$$p_3 = \frac{1}{16}(1 + 3x_1 + 6x_2), \tag{1.4.42}$$

$$p_4 = \frac{1}{64}(1 + 6x_1 + 24x_2 + x_1^2 + 2x_3 + 4x_4), \tag{1.4.43}$$

where

$$x_1 = I_2 + I_4 + I_7, \qquad x_2 = I_1 + I_{12}, \tag{1.4.44}$$

$$x_3 = I_2^2 - I_3, \qquad x_4 = I_5 + I_8 + I_{14} + I_4 I_7. \tag{1.4.45}$$

Kampe invariant: An interesting LU invariant in three-qubit systems is the so-called Kempe invariant. It was originally introduced to distinguish three-qubit pure states [369]. Its intention to mix states was discussed in Ref. [370] and reads:

$$I_{\text{Kempe}} = \text{tr}[(\varrho_{AB} \otimes \mathbb{1}_C)(\varrho_{AC} \otimes \mathbb{1}_B)(\varrho_{BC} \otimes \mathbb{1}_A)], \tag{1.4.46}$$

where $\varrho_{XY} = \text{tr}_Z(\varrho_{ABC})$ are the two-qubit reduced state for $X, Y, Z = A, B, C$.

1.4.4 Previously known entanglement criteria

***N*-qubit entanglement with second moments:** In Refs. [350, 371–373], it has been shown that any N-qubit fully separable state obeys

$$S_N \leq 1. \tag{1.4.47}$$

The violation of this inequality implies the presence of multipartite entanglement. This proof is straightforwardly obtained as follows:

$$S_N(\varrho_{\text{fs}}) \leq S_N(|\psi_{\text{fs}}\rangle) = S_N(|0\rangle^{\otimes N}) = [S_1(|0\rangle)]^N = 1, \tag{1.4.48}$$

where we denote ϱ_{fs} as a fully separable state defined in Eq. (1.2.22), used the properties of convexity, convolution, and LU invariance.

N-qudit entanglement with second moments: High-dimensional multipartite entanglement can be detected by the k-body sector length S_k. In Refs. [351, 373–376], it has been shown that any N-qudit fully separable state obeys

$$S_k \leq \binom{N}{k}(d-1)^k, \tag{1.4.49}$$

where S_k is the k-body sector length. Violation of this bound implies that the state is entangled as can be easily demonstrated, for instance, in graph states. Note that this criterion can be seen as a generalization of Eq. (1.4.47) to sector lengths between a number of observers smaller than N and any dimension.

In Ref. [377], it was shown that linear combinations of various sector lengths can be useful to detect entanglement. In fact, any N-qudit fully separable state obeys

$$\sum_{k=0}^{N}[(d-1)N - dk]S_k \geq 0. \tag{1.4.50}$$

This criterion is strictly stronger (detects more entangled states) than the criterion in Eq. (1.4.49).

Two-qubit entanglement with higher moments: Recall the Bell-diagonal state ϱ_{BD} in Eq. (1.1.137), which is parameterized by the three parameters (τ_1, τ_2, τ_3). This allows for a much simpler analytical treatment than general states. As mentioned in Eq. (1.2.47), the positive partial transpose (PPT) criterion can be rewritten as $\sum_{i=1}^{3}|\tau_i| \leq 1$.

For a Bell-diagonal state ϱ_{BD}, the second and fourth moments of the product observable $\mathcal{M}_{\mathrm{P}} = \sigma_z \otimes \sigma_z$ are given by [378]:

$$\mathcal{R}^{(2)} = \frac{1}{9}\sum_{i=x,y,z}\tau_i^2, \qquad \mathcal{R}^{(4)} = \frac{2}{75}\sum_{i=x,y,z}\tau_i^4 + \frac{27}{25}[\mathcal{R}^{(2)}]^2. \tag{1.4.51}$$

Bsed on the separability constraint $\sum_{i=1}^{3}|\tau_i| \leq 1$, for a given value of $\mathcal{R}^{(2)}$, one can analytically maximize and minimize the value of $\mathcal{R}^{(4)}$ for separable states. This leads to a separability region in the parameter space spanned by $\mathcal{R}^{(2)}$ and $\mathcal{R}^{(4)}$. This approach allows us to detect entanglement that cannot be detected by the second moment itself. Moreover, by additionally using the sixth moment, a necessary and sufficient condition for entanglement of two-qubit Bell diagonal states can be found, see the Appendix in Ref. [378].

W-class entanglement with higher moments: In addition to entanglement detection, another interesting and important issue is to determine the class to which a given multipartite state belongs. The discrimination of W-class entanglement has been studied with two criteria based on the second and fourth moments of randomized measurements [379].

The first criterion provides an analytical upper bound for the second moment of an N-qubit W-class state:

$$S_N \leq 5 - \frac{4}{N}, \tag{1.4.52}$$

where S_N is denoted as the second moment $\mathcal{R}^{(2)}$, and the inequality is saturated by a pure W state: $|\mathrm{W}\rangle = (|10\cdots0\rangle + |01\cdots0\rangle + \cdots + |0\cdots01\rangle)/\sqrt{N}$. If this condition is violated, it implies that a multiqubit state is detected to be outside of the W class, i.e., it cannot be obtained from the W state by stochastic local operations and classical communication (SLOCC).

The second criterion involves a linear combination of the second and fourth moments, with weights optimized based on the N-qubit W state $|\mathrm{W}_N\rangle$ and the biseparable state $|\mathrm{W}_{N-1}\rangle|\psi\rangle$. Furthermore, Ref. [379] has provided the characterization of three-qubit and four-qubit states using the second and fourth moments through an extensive numerical approach.

1.5 Quantum designs

In this section, we will give a brief introduction to quantum designs. Historically, quantum t-designs were discussed by analogy with classical t-designs in combinatorial mathematics. The idea of designs is helpful to evaluate the Haar integral in Eq. (1.4.2). This section is based on the description of Ref. [7].

1.5.1 Classical designs

Simpson's rule: Let us consider a real quadratic function $f(x)$ for a variable x and take an integral in the interval from a to b. According to the rule found by Thomas Simpson in the 18th century, it holds that the integral for the quadratic function can be exactly evaluated as a simple expression using only three points, namely

$$\int_a^b dx\, f(x) = \frac{b-a}{6}\left[f(a) + 4f\left(\frac{a+b}{2}\right) + f(b)\right]. \tag{1.5.1}$$

An extension of Simpson's rule to a greater number of points is possible, which is called the Gauss-Christoffel quadrature rule.

Spherical designs: A spherical t-design can be seen as a generalization of Simpson's rule for the efficient computation of integrals of certain polynomials over some spheres [380, 381]. Let $\mathcal{S}_{n-1}$ be the n-dimensional real unit sphere and let $X = \{\boldsymbol{x}_i \in \mathcal{S}_{n-1}\}_{i=1,\ldots,K}$ be a finite set of points on it with the number of elements $K = |X|$. We call this set a spherical t-design if

$$\frac{1}{K}\sum_{\boldsymbol{x}_i \in X} f_t(\boldsymbol{x}_i) = \int d\boldsymbol{x}\, f_t(\boldsymbol{x}), \tag{1.5.2}$$

for any homogeneous polynomial function $f_t(\boldsymbol{x})$ in n variables with degree t, where $d\boldsymbol{x}$ is the spherical measure on the n-dimensional unit sphere with $\int d\boldsymbol{x} = 1$ [380, 382]. The spherical design property ensures that the integral for any polynomial of at most degree t over the entire sphere can be efficiently computed by taking the average over the spherical t-design set of only K discrete different points. In the following, we summarize several remarks:

- Hierarchical structure: Clearly, any spherical t-design is also a spherical $(t-1)$-design.
- Construction: It can be shown spherical t-designs exist for any positive integer t and n [383], although they may be difficult to construct explicitly [384]. Furthermore, as expected, if the allowed degree t or the dimension n increases, then a larger set X is required.
- Invariance: By definition, the integral at the right-hand side in Eq. (1.5.2) is invariant under any rotation on the sphere, so the evaluated expression on the left-hand side is also invariant.

Application to randomized measurements: To give a concrete example, let us evaluate the second moment $\mathcal{R}^{(2)}$ in Eq. (1.4.17) using the idea of spherical designs. For the sake of simplicity, let us consider the case $N = 2$.

It is well known that a set of $K = 6$ unit vectors on orthogonal antipodals, $\{\boldsymbol{x}_i = \pm \boldsymbol{e}_i : i = x, y, z\}$, where $\boldsymbol{e}_i$ are the Cartesian axes, is a spherical two-design (and also three-design) [360, 378, 383]. Using this spherical design, we rewrite each of the two integrals in $\mathcal{R}^{(2)}$ over a two-dimensional unit sphere as the average over the set of six points on the sphere:

$$\mathcal{R}^{(2)}(\varrho) = 3^2 \frac{1}{6^2} \sum_{i,j=1}^{6} [E(\boldsymbol{e}_i, \boldsymbol{e}_j)]^2 = \sum_{i,j=x,y,z} [\mathrm{tr}(\varrho\, \sigma_i \otimes \sigma_j)]^2, \tag{1.5.3}$$

where we choose the normalisation $\mathcal{N} = (3/4\pi)^2$ and use the fact that the even function $[E(\boldsymbol{u}_1, \boldsymbol{u}_2)]^2$ does not change under the sign flip. As a result, the integral over the entire spheres $\boldsymbol{u}_1, \boldsymbol{u}_2$ is replaced by a sum of nine (squared) correlation functions computed along orthogonal directions on local Bloch spheres. Note that the second moment in N-qubit systems can be found in a similar manner.

1.5.2 Complex projective designs

Complex projective t-designs (or quantum spherical t-designs) are a generalization of spherical designs to a complex vector space [385, 386]. They allow for example to evaluate expressions based on a random sampling of quantum states. A finite set of unit vectors $D = \{|\psi_i\rangle : |\psi_i\rangle \in \mathcal{CS}_{d-1}\}_{i=1}^{K}$ defined on a d-dimensional sphere $\mathcal{CS}_{d-1}$ in the complex vector space, forms a complex projective t-design if

$$\frac{1}{K} \sum_{|\psi_i\rangle \in D} P_t(\psi_i) = \int d\psi\, P_t(\psi), \tag{1.5.4}$$

for any homogeneous polynomial function P_t in $2d$ variables with degree t (that is, d variables with degree t and their complex conjugates with degree t), where $d\psi$ is the spherical measure on the complex unit sphere $\mathcal{CS}_{d-1}$. In the following, we will summarize several remarks:

- Projective Hilbert space: It is here important to note that $\mathcal{CS}_{d-1}$ is isomorphic to the d-dimensional projective Hilbert space denoted as $P(\mathcal{H}_d)$, where complex unit vectors $|x\rangle, |y\rangle \in P(\mathcal{H}_d)$ are identified iff $|x\rangle = e^{i\phi} |y\rangle$ with a real ϕ [23]. For example, the Bloch sphere is known as $P(\mathcal{H}_2)$, in which a point on the surface of the sphere corresponds to a pure single-qubit state, up to a phase. In this state space, any two states can be distinguished by the so-called Fubini-Study measure, which is invariant under the action of $U(1)$, for details see Refs. [23, 387].

- Quantum state designs: Since polynomials of degree t can be written as linear functions on t copies of a state, the definition of complex projective

t-designs is equivalent to requiring

$$\frac{1}{K}\sum_{|\psi_i\rangle\in D}\left(|\psi_i\rangle\langle\psi_i|\right)^{\otimes t}=\int d\psi\ \left(|\psi\rangle\langle\psi|\right)^{\otimes t}. \tag{1.5.5}$$

In this form, this is also called the quantum state t-design and can be considered as an ensemble of states that is indistinguishable from a uniform random ensemble over all states, if one considers t-fold copies of states selected from that ensemble.

- Projector onto the symmetric subspace: Since the integral on the right-hand side of Eq. (1.5.5) is proportional to the projector onto the symmetric subspace [388–390] (or see Lemma 2.2.2. in Ref. [391]), one can simplify this to

$$\int d\psi\ \left(|\psi\rangle\langle\psi|\right)^{\otimes t}=\frac{P_{\text{sym}}^{(t)}}{d_{\text{sym}}^{(t)}}, \tag{1.5.6}$$

where $P_{\text{sym}}^{(t)}$ is the projector onto the permutation symmetric subspace and $d_{\text{sym}}^{(t)}=\binom{d+t-1}{t}$ is its dimension.

- Qubits: For multi-qubit systems ($d=2$), the symmetric subspace is spanned by the Dicke states $\{|D_{t,m}\rangle\}_{m=0}^{t}$ given in Eq. (1.2.32). Since the dimension of this subspace is $t+1$, the projector can be written as

$$P_{\text{sym}}^{(t)}=\frac{1}{t+1}\sum_{m=0}^{t}|D_{t,m}\rangle\langle D_{t,m}|. \tag{1.5.7}$$

- Qudits: In general, one can write

$$P_{\text{sym}}^{(t)}=\frac{1}{t!}\sum_{\pi\in\text{Sym}(t)}W_\pi, \tag{1.5.8}$$

where the permutation operator W_π defined in Eq. (1.1.123) for a permutation $\pi=\pi(1)\dots\pi(t)\in\text{Sym}(t)$. Examples for $t=1$ and $t=2$ are

$$\int d\psi\ |\psi\rangle\langle\psi|=\frac{\mathbb{1}_d}{d}, \tag{1.5.9}$$

$$\int d\psi\ \left(|\psi\rangle\langle\psi|\right)^{\otimes 2}=\frac{1}{d(d+1)}(\mathbb{1}_d^{\otimes 2}+\mathbb{S}), \tag{1.5.10}$$

where $\mathbb{S}$ denotes the SWAP operator defined in Eq. (1.1.119).

- State moments: Note that Eq. (1.5.6) implies relations between the moments $\text{tr}(\varrho^m)$ for any single-qudit state ϱ [392].

- Frame potentials: Another equivalent definition of complex projective t-designs is given by the condition

$$\frac{1}{K^2}\sum_{|\psi_i\rangle,|\psi_j\rangle\in D}|\langle\psi_i|\psi_j\rangle|^{2t}=\frac{1}{d_{\mathrm{sym}}^{(t)}}. \tag{1.5.11}$$

  The left-hand side is called t-th frame potential. According to the so-called Welch bound [393, 394], it is always greater than or equal to the right-hand side, where the equality is saturated if and only if the set D forms the complex projective t-designs.

- Examples: A trivial example of a complex projective 1-design is a set of orthonormal basis vectors $\{|i\rangle\}_{i=1}^{d}$, which leads to $(1/d)\sum_{i=1}^{d}|i\rangle\langle i|=\mathbb{1}_d/d$. A typical example of complex projective 2-designs are so-called mutually unbiased bases (MUBs).

- MUBs: A collection $\{M_k\}$ of orthonormal bases $M_k=\{|i_k\rangle\}_{i=1}^{d}$ for a d-dimensional Hilbert space is called mutually unbiased if $|\langle i_k|j_l\rangle|^2=1/d$, for any i,j with $k\neq l$, i.e. the overlap of any pair of vectors from different bases is equal [395]. For the case of $d=2$, a set of MUBs is given by $\{M_1,M_2,M_3\}$ with

$$M_1=\{|0\rangle,|1\rangle\},\quad M_2=\{|+\rangle,|-\rangle\},\quad M_3=\{|+i\rangle,|-i\rangle\}. \tag{1.5.12}$$

  Here, the computational bases $\{|0\rangle,|1\rangle\}$, $\{|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}\}$, and $\{|\pm i\rangle=(|0\rangle\pm i\,|1\rangle)/\sqrt{2}\}$ are the normalized eigenvectors of σ_z, σ_x, and $\sigma_x\sigma_z$.

- Details about MUBs: The size of maximal sets of MUBs for a given dimension d is an open problem and only partial answers are known. In fact, this has been recognized as one of the five most important open problems in quantum information theory [224]. It is known that in any dimension d the maximum number of MUBs cannot be more than $d+1$ [396]. In fact, for prime-power dimensions $d=p^r$, sets of $d+1$ MUBs can be constructed [397, 398]. Furthermore, for the dimensions $d=p^2$ or $d=2^r$, an experimental implementation of MUBs is possible [399, 400]. The smallest dimension which is not a power of a prime and where the maximal number of MUBs is unknown is $d=6$ [401]. Finally and importantly, any collection of $(d+1)$ MUBs saturates the Welch bound and therefore forms a complex projective 2-design [394].

1.5.3 Unitary designs

In the case of qubits, spherical designs are suited to evaluate integrals over random unitaries of measurement settings as those can be mapped to rotations on the Bloch sphere. For higher dimensional systems, however, such a mapping no

longer exists and the randomized scenario can be addressed by general unitary designs. A set of unitaries $G = \{U_i : U_i \in \mathcal{U}(d)\}_{i=1}^{K}$ forms a unitary t-design if

$$\frac{1}{K}\sum_{U_i \in G} P_t(U_i) = \int dU\, P_t(U), \tag{1.5.13}$$

for any homogeneous polynomial function P_t in $2d^2$ variables with degree t (that is, on the elements of unitary matrices in $\mathcal{U}(d)$ with degree t and on their complex conjugates with degree t), where dU is the Haar unitary measure on $\mathcal{U}(d)$. For details about unitary t-design, see Refs. [391, 402–404]. In the following, we will summarize several remarks:

- Difference from state designs: Similarly to complex projective designs, there are several equivalent definitions of unitary t-designs. One is given by

$$\frac{1}{K}\sum_{U_i \in G} U_i^{\otimes t} X (U_i^{\dagger})^{\otimes t} = \int dU\, U^{\otimes t} X (U^{\dagger})^{\otimes t}, \tag{1.5.14}$$

  for any operator $X \in \mathcal{H}_d^{\otimes t}$. An important observation here is that if we set $\{|\psi_i\rangle\} = \{U_i|0\rangle\}$, then Eq. (1.5.14) leads to Eq. (1.5.5), i.e. any unitary t-design gives rise to a quantum state t-design. The converse is not necessarily true, even if a set of unitaries creates a state design via $\{|\psi_i\rangle\} = \{U_i|0\rangle\}$, it does not constitute a unitary design. This simply follows from the fact that a relation like $\{|\psi_i\rangle\} = \{U_i|0\rangle\}$ does not determine the U_i in a unique way.

- Simplifications: In order to determine the evaluated expression in an analogy with Eq. (1.5.6), note that the right-hand side in Eq. (1.5.14) commutes with all unitaries $V^{\otimes t}$ for $V \in \mathcal{U}(d)$, due to the left and right invariance of the Haar measure. Then, according to the Schur-Weyl duality, if an operator $A \in \mathcal{H}_d^{\otimes t}$ obeys $\left[A, V^{\otimes t}\right] = 0$ for any $V \in \mathcal{U}(d)$, then A can be written in a linear combination of subsystem permutation operators W_π (while the converse statement is also true) [109]. Thus, one has

$$\Phi_t(X) \equiv \int dU\, U^{\otimes t} X (U^{\dagger})^{\otimes t} = \sum_{\pi \in \mathrm{Sym}(t)} x_\pi W_\pi, \tag{1.5.15}$$

  where each of x_π can be found with the help of the so-called Weingarten calculus [69, 405]. As an example, we have

$$\Phi_1(X) = \frac{\mathrm{tr}(X)}{d}\mathbb{1}_d, \tag{1.5.16}$$

$$\Phi_2(X) = \frac{1}{d^2-1}\left\{\left[\mathrm{tr}(X) - \frac{\mathrm{tr}(X\mathbb{S})}{d}\right]\mathbb{1}_d^{\otimes 2} - \left[\frac{\mathrm{tr}(X)}{d} - \mathrm{tr}(X\mathbb{S})\right]\mathbb{S}\right\}, \tag{1.5.17}$$

  where $\mathbb{S}$ is the SWAP operator. Cases with $t = 3, 4$ are explicitly described in Example 3.27, and Example 3.28 in Ref. [68]. For more details, see [406, 407] and Sec. 1.1.4.

- Frame potentials: Moreover, yet another equivalent definition of unitary t-designs is given in Ref. [402]

$$\frac{1}{K^2}\sum_{U_i,U_j\in G}\left|\mathrm{tr}(U_iU_j^\dagger)\right|^{2t}=\begin{cases}t! & \text{for } d\geq t,\\ \frac{(2t)!}{t!(t+1)!} & \text{for } d=2,\end{cases} \tag{1.5.18}$$

  where the left-hand side is called t-th frame potential and the right-hand side gives its minimal value similar to the Welch bound in complex spherical designs. The frame potential is often employed as a useful measure to quantify the randomness of an ensemble of unitaries in terms of out-of-time-order correlation functions in quantum chaos [109, 408].

- Constructions: For the scenario of N-qubit systems, an example of a unitary 1-design is the Pauli group $\mathcal{P}_N$, the group of all N-fold tensor products of single-qubit Pauli matrices $\{\mathbb{1}_2,\sigma_x,\sigma_y,\sigma_z\}$. This group does not form a unitary 2-design [409], but note that we used Pauli measurements as a form of a spherical design. In contrast, the Clifford group $\mathcal{C}_N$, a group of unitaries with the property $C\in\mathcal{C}_N$ if $CPC^\dagger\in\mathcal{P}_N$ for any $P\in\mathcal{P}_N$, is known to be a unitary 2-design in this scenario. Furthermore, it has been shown that the Clifford group also forms a unitary 3-design, but not a unitary 4-design [410, 411].

Applications to randomized measurements: Finally, we show the usefulness of unitary designs in the scheme of randomized measurements. For the sake of simplicity, we focus on a three-qudit state ϱ_{ABC} and consider how to obtain its full-body sector length S_3 from the unitary two-design. Note that one can straightforwardly generalize this approach to the sector lengths S_k of a N-qudit state for any $1\leq k\leq N$.

Let us consider the product observable $\mathcal{M}=\lambda_a\otimes\lambda_b\otimes\lambda_c$ in the second-order moment in Eq. (1.4.2), for any choice of Gell-Mann matrices with $a,b,c=1,\ldots,d^2-1$. Substituting the generalized Bloch decomposition of ϱ_{ABC} discussed in Eq. (1.1.101) into the second-order moment, one can find

$$\mathcal{R}^{(2)}_{\mathcal{M}}(\varrho_{ABC})=\frac{\mathcal{N}_{3,d,2}}{d^6}\sum_{\boldsymbol{i},\boldsymbol{j}=1}^{d^2-1}\alpha_{i_Ai_Bi_C}\alpha_{j_Aj_Bj_C}\mathrm{tr}\left[\Phi_2^A\otimes\Phi_2^B\otimes\Phi_2^C(\lambda_a\otimes\lambda_b\otimes\lambda_c)^{\otimes 2}\right], \tag{1.5.19}$$

where we employed that $[\mathrm{tr}(M)]^2=\mathrm{tr}(M^{\otimes 2})$ for any matrix M and we denoted that $\boldsymbol{i}=i_A,i_B,i_C$ and $\boldsymbol{j}=j_A,j_B,j_C$. Also, we define the twirling result as

$$\Phi_2^X=\int dU_X\,U_X^{\otimes 2}(\lambda_{i_X}\otimes\lambda_{j_X})(U_X^\dagger)^{\otimes 2}, \tag{1.5.20}$$

for $X=A,B,C$. Now Φ_2^X can be simply evaluated using the formula in Eq. (1.5.17) and be expressed as:

$$\Phi_2^X=\frac{1}{d^2-1}\delta_{i_Xj_X}(d\$-\mathbb{1}_d^{\otimes 2}), \tag{1.5.21}$$

where we employed the SWAP trick mentioned in Sec. 1.1.7 and the properties of the Gell-Mann matrices $\mathrm{tr}(\lambda_i) = 0$ and $\mathrm{tr}(\lambda_i\lambda_j) = d\delta_{ij}$. As the last step, by inserting this form into the second moment in Eq. (1.5.19) and choosing the normalization constant as $\mathcal{N}_{3,d,2} = (d^2-1)^3$, one can have that $\mathcal{R}^{(2)}_{\mathcal{M}} = S_3$.

An important lesson from this result is that randomized measurements of second order are an indirect implication of the SWAP operator. In higher-order cases, the permutation operators W_π will emerge according to the Schur-Weyl duality in Eq. (1.5.15). This will play an important role in estimating the purity of a state, the overlap between two states, and the moments of partially transposes states and extensions, for details see [105, 112, 255, 412–416] and Review paper [417].

Part I

Abstract theory of randomized measurements

Chapter 2

Tripartite entanglement and bound entanglement

As mentioned in Sec. 1.4, several works in randomized measurements have advanced entanglement detection. This Chapter addresses the question of whether one can find optimal or powerful criteria to detect entanglement. In particular, this Chapter deals with tripartite systems with second moments and high-dimensional bipartite systems with fourth moments. This Chapter is based on Refs. [1, 8].

2.1 Introduction

Let us begin by recalling the moments in Eq. (1.4.2) in the scheme of randomized measurements in Sec. 1.4. In the case of a bipartite state ϱ_{AB} and a product observable $\mathcal{M} = M_A \otimes M_B$, the moment is given by

$$\mathcal{R}^{(t)}_{AB}(\varrho_{AB}) = \int dU_A \int dU_B \left[\mathrm{tr}(\varrho_{AB} U_A^\dagger \otimes U_B^\dagger M_A \otimes M_B U_A \otimes U_B)\right]^t. \quad (2.1.1)$$

Clearly, similar moments can be defined for multiparticle systems.

In the scheme of randomized measurements, there are at least two research lines on entanglement detection. One line has been started from the estimation of the state's purity [418], and then protocols for measuring entanglement via Rényi entropies have been presented [412] and experimentally implemented [413]. Also, ideas to estimate the PPT criterion in Eq. (1.2.44) have been introduced [105, 112].

Another research line characterized the relation of the second moments [350, 373] defined as $\mathcal{R}^{(2)}_{AB}$ in Eq. (2.1.1) and those of the marginals [419] to entanglement. Higher moments have been used to characterize multiparticle entanglement [378, 379], and quantum designs have been shown to allow for a simplified implementation, as the integral in Eq. (2.1.1) can be replaced by finite sums [2, 378].

Still, the previous results of the above research directions are incomplete in several respects. First, although many entanglement criteria have been presented, their optimality is not clear. It would be desirable to use the information obtained from random measurements as efficiently as possible. Second, the known results from random measurements can only detect highly entangled states, e.g., states that are close to pure states. However, it is crucial for the long-term impact of the research program that weakly entangled states, e.g., states that cannot be detected with the PPT criterion, can also be analyzed.

The goal of this Chapter is to generalize the existing approaches in two directions: First, we will systematically consider the moments of the measurement results when only some of the parties measure. That is, we evaluate the expressions of the moment $\mathcal{R}^{(r)}_{AB}$ for the special case $M_A = \mathbb{1}$ or $M_B = \mathbb{1}$ and call these quantities the reduced moments $\mathcal{R}^{(r)}_{B}$ and $\mathcal{R}^{(r)}_{A}$. As we will show, these reduced moments can be used to design improved entanglement criteria that are optimal in the sense that if a quantum state is not detected by them, then there is also a separable state compatible with the data.

Second, we present a systematic approach to characterize high-dimensional systems with higher moments $\mathcal{R}^{(r)}_{AB}$. We show how previously known entanglement criteria [241, 242, 244] can be formulated in terms of moments. Thus we show that bound entanglement, a weak form of entanglement that cannot be used for entanglement distillation and is not detectable by the PPT criterion, can also be characterized in a reference-frame-independent way. This shows that the randomized measurement approach is powerful enough to characterize the rich plethora of entanglement phenomena.

Finally, we explain the experimental demonstration of our results in a photonic setup. Then we conclude with a discussion.

2.2 Detection of tripartite entanglement

2.2.1 Second moments

Consider a three-qubit state ϱ_{ABC} and take the product observable $\mathcal{M} = M_A \otimes M_B \otimes M_C$ in the second moment $\mathcal{R}^{(2)}_{ABC}$ in Eq. (1.4.2), where, with out loss of generality, M_A, M_B, M_C can be taken as the Pauli-z matrix σ_z. As mentioned in Sec. 1.5, the full and reduced second moment can be simplified by the fact that each unitary integral can be replaced by sums over the Pauli matrices $\sigma_0, \sigma_1, \sigma_2$, and σ_3.

Recall the Bloch decomposition of a three-qubit state in Eq. (1.1.101):

$$\varrho_{ABC} = \frac{1}{8} \sum_{i,j,k=0}^{3} \alpha_{ijk} \sigma_i \otimes \sigma_j \otimes \sigma_k. \tag{2.2.1}$$

Then the full and reduced second moments can simply be expressed in terms of

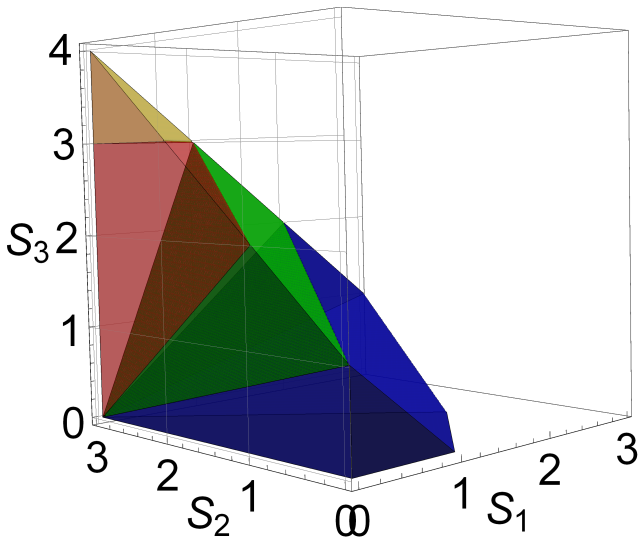

Figure 2.1: Geometry of the three-qubit state space in terms of the second moments of random measurements or sector lengths. The total polytope is the set of all states, characterized by the inequalities $S_k \geq 0$, $S_1 - S_2 + S_3 \leq 1$, $S_2 \leq 3$, and $S_1 + S_2 \leq 3(1 + S_3)$ [352]. The fully separable states are contained in the blue polytope, obeying the additional constraint in Eq. (2.2.5). States that are biseparable for some partitions are contained in the union of the green and blue polytopes, characterized by the additional constraint in Eq. (2.2.11). In fact, for any point in the green and blue areas, there is a biseparable state with the corresponding second moments. The yellow area corresponds to the states violating the best previously known criterion for biseparable states, $S_3 \leq 3$ [351–353, 420]. Thus, the red area marks the improvement of the criterion in Eq. (2.2.11) compared with previous results. This figure is a modified version of a figure from Ref. [1].

the coefficients α_{ijk}:

$$\mathcal{R}^{(2)}_{ABC} = \frac{1}{27}\sum_{i,j,k=1}^{3}\alpha^2_{ijk}, \quad \mathcal{R}^{(2)}_{AB} = \frac{1}{9}\sum_{i,j=1}^{3}\alpha^2_{ij0}, \quad \mathcal{R}^{(2)}_{A} = \frac{1}{3}\sum_{i=1}^{3}\alpha^2_{i00}, \tag{2.2.2}$$

where we take $\mathcal{N}_{3,3,2} = 1$ in Eq. (1.4.2). Similarly for the reduced moments on other parts of the three-particle system.

Sums of this form have already been considered under the concept of sector lengths in Eq. (1.4.7):

$$S_1 = 3(\mathcal{R}^{(2)}_A + \mathcal{R}^{(2)}_B + \mathcal{R}^{(2)}_C), \quad S_2 = 9(\mathcal{R}^{(2)}_{AB} + \mathcal{R}^{(2)}_{AC} + \mathcal{R}^{(2)}_{BC}), \quad S_3 = 27\mathcal{R}^{(2)}_{ABC}. \tag{2.2.3}$$

As mentioned in Sec. 1.4, the set of all three-qubit states forms a polytope in the space of the sector lengths, which has been fully characterized [352], see also Fig. 2.1.

2.2.2 Fully separability

To proceed, recall that a state is fully separable if it can be written as

$$\varrho_{\mathrm{fs}} = \sum_k p_k \varrho_k^A \otimes \varrho_k^B \otimes \varrho_k^C, \tag{2.2.4}$$

where the p_k form a probability distribution. Now, we can formulate the first main result of this Chapter:

Result 1. *Any fully separable three-qubit state obeys*

$$S_2 + 3S_3 \leq 3 + S_1. \tag{2.2.5}$$

This is the optimal linear criterion in the sense that any other linear criterion for the S_i detects strictly fewer states.

Remark 1. The proof of this result, including generalizations to higher-dimensional systems, is given below. The geometrical interpretation is displayed in Fig. 2.1. Since one can easily construct fully separable states on two of the three sides of the resulting triangle (i.e., the surface where equality holds), this criterion is optimal in the sense that any other linear criterion for the S_k detects strictly fewer states. However, there may be points on the plane of the triangle surface that cannot originate from a separable state. This may indicate that there exist stronger, non-linear criteria for full separability using sector lengths.

Also, we present the three-qudit generalization of Eq. (2.2.5):

Result 2. *Any fully separable three-qudit state obeys*

$$S_3 \leq d - 1 + \frac{2d-3}{3} S_1 + \frac{d-3}{3} S_2. \tag{2.2.6}$$

Proof. Let us consider the reduced density matrix of the fully separable state on the subsystem AB: $\varrho_{AB} = \mathrm{tr}_C(\varrho_{\mathrm{fs}}) = \sum_k p_k \varrho_k^A \otimes \varrho_k^B$. Then we have

$$\begin{aligned} \mathrm{tr}(\varrho_{\mathrm{fs}}^2) &= \sum_{k,l} p_k p_l \, \mathrm{tr}(\varrho_k^A \varrho_l^A) \, \mathrm{tr}(\varrho_k^B \varrho_l^B) \, \mathrm{tr}(\varrho_k^C \varrho_l^C) \\ &\leq \sum_{k,l} p_k p_l \, \mathrm{tr}(\varrho_k^A \varrho_l^A) \, \mathrm{tr}(\varrho_k^B \varrho_l^B) = \mathrm{tr}(\varrho_{AB}^2), \end{aligned} \tag{2.2.7}$$

where the Cauchy-Schwarz inequality leads to

$$\mathrm{tr}(\varrho_k^C \varrho_l^C) \leq \sqrt{\mathrm{tr}[(\varrho_k^C)^2]} \sqrt{\mathrm{tr}[(\varrho_l^C)^2]} \leq 1. \tag{2.2.8}$$

Similarly, we obtain that $\mathrm{tr}(\varrho_{\mathrm{fs}}^2) \leq \mathrm{tr}(\varrho_{AC}^2)$ and $\mathrm{tr}(\varrho_{\mathrm{fs}}^2) \leq \mathrm{tr}(\varrho_{BC}^2)$. Summarizing these three purity inequalities gives

$$3\mathrm{tr}(\varrho_{\mathrm{fs}}^2) \leq \mathrm{tr}(\varrho_{AB}^2) + \mathrm{tr}(\varrho_{AC}^2) + \mathrm{tr}(\varrho_{BC}^2). \tag{2.2.9}$$

Then, with the help of the relation (1.4.13), translating this inequality to the form with sector lengths yields Eq. (2.2.6). □

2.2.3 Biseparability

Violation of Eq. (2.2.5) implies that the state contains some entanglement, but it does not mean that all three particles are entangled. Indeed, an entangled state may still be separable with respect to some bipartition, for details see Sec. 1.2. For instance, if we consider the bipartition $A|BC$, a state separable with respect to this bipartition can be written as

$$\varrho_{A|BC} = \sum_k q_k^A \varrho_k^A \otimes \varrho_k^{BC}, \tag{2.2.10}$$

where the q_k^A form a probability distribution and ϱ_k^{BC} may be entangled. Similarly, one can define biseparable states with respect to the two other bipartitions as $\varrho_{B|AC}$ and $\varrho_{C|AB}$. For these states, we can formulate:

Result 3. *Any three-qubit state which is separable with respect to some bipartition obeys*

$$S_2 + S_3 \leq 3(1 + S_1). \tag{2.2.11}$$

This is the optimal criterion in the sense that if the three S_i obey the inequality, then for any bipartition there is a separable state compatible with them.

Remark 2. The proof of this result, including generalizations to higher-dimensional systems, is given below. The geometrical interpretation is displayed in Fig. 2.1. We add that we have strong numerical evidence that Eq. (2.2.11) also holds for mixtures of biseparable states with respect to different partitions, i.e., states of the form $\varrho_{\text{bs}} = p_A \varrho_{A|BC} + p_B \varrho_{B|AC} + p_C \varrho_{C|AB}$, where the p_A, p_B, and p_C form convex weights. Nevertheless, we leave this as a conjecture for further study.

Now we propose the three-qudit generalization of Eq. (2.2.11):

Result 4. *Any three-qudit state which is separable with respect to some bipartition obeys*

$$S_2 + S_3 \leq \frac{d^3 - 2}{2}(1 + S_1). \tag{2.2.12}$$

Proof. Let ϱ_{bs} be a separable three-qudit state with respect to a bipartition, and let ϱ_X be its reduced density matrices on the subsystems X for $X \in \{A, B, C\}$. With the help of the relation (1.4.13), we notice that Eq. (2.2.12) is equivalent to

$$1 + \operatorname{tr}(\varrho_{\text{bs}}^2) \leq \frac{d}{2}\left[\operatorname{tr}(\varrho_A^2) + \operatorname{tr}(\varrho_B^2) + \operatorname{tr}(\varrho_C^2)\right]. \tag{2.2.13}$$

In the following, without loss of generality, we consider a separable state with respect to a fixed bipartition $A|BC$: $\varrho_{A|BC} = \sum_k q_k \varrho_k^A \otimes \varrho_k^{BC}$. Since its reduced density matrix on the subsystem A is given by $\varrho_A = \sum_k q_k \varrho_k^A$, we have

$$\operatorname{tr}(\varrho_{A|BC}^2) = \sum_{k,l} q_k q_l \operatorname{tr}(\varrho_k^A \varrho_l^A) \operatorname{tr}(\varrho_k^{BC} \varrho_l^{BC}) \leq \sum_{k,l} q_k q_l \operatorname{tr}(\varrho_k^A \varrho_l^A) = \operatorname{tr}(\varrho_A^2), \tag{2.2.14}$$

where $\mathrm{tr}(\varrho_k^{BC}\varrho_l^{BC}) \leq 1$. In addition, it follows from the relation (1.4.13) for single particles

$$\mathrm{tr}(\varrho_B^2) + \mathrm{tr}(\varrho_C^2) = \frac{1}{d}(2 + S_1^B + S_1^C), \tag{2.2.15}$$

where we split $S_1 = S_1^A + S_1^B + S_1^C$ corresponding to the contributions from the three particles. Then we have

$$\begin{aligned}
&1 + \mathrm{tr}(\varrho_{A|BC}^2) - \frac{d}{2}\left[\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) + \mathrm{tr}(\varrho_C^2)\right] \\
&\leq 1 + \mathrm{tr}(\varrho_A^2) - \frac{d}{2}\left[\mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) + \mathrm{tr}(\varrho_C^2)\right] \\
&= 1 + \left(1 - \frac{d}{2}\right)\mathrm{tr}(\varrho_A^2) - \frac{1}{2}(2 + S_1^B + S_1^C) \\
&= \left(1 - \frac{d}{2}\right)\mathrm{tr}(\varrho_A^2) - \frac{1}{2}(S_1^B + S_1^C) \leq 0.
\end{aligned} \tag{2.2.16}$$

□

2.2.4 Detailed discussions about Result 3

Here we discuss Eq. (2.2.11) in Result 3 in more details. First, we have a discussion about its optimality: It is the optimal criterion in the sense that if the three S_k obey the inequality, then for any bipartition there is a separable state compatible with them. This can be seen as follows: Consider the family of biseparable three-qubit states

$$\sigma = p\,|0\rangle\langle 0| \otimes |\psi\rangle\langle\psi| + (1-p)\,|1\rangle\langle 1| \otimes |\phi\rangle\langle\phi|\,, \tag{2.2.17}$$

where

$$|\psi\rangle = a\,|00\rangle + b\,|11\rangle\,, \quad |\phi\rangle = c\,|00\rangle + d\,|11\rangle\,, \tag{2.2.18}$$

$$a^2 + b^2 = c^2 + d^2 = 1, \quad \frac{1}{2} \leq p \leq 1, \tag{2.2.19}$$

$$\sqrt{1 - \frac{1}{2p}} \leq a \leq \sqrt{\frac{1}{2p}}, \quad a^2 \leq b^2, \quad c = \sqrt{\frac{2pa^2 - 1}{2(p-1)}}, \quad d = \pm\sqrt{1 - c^2}. \tag{2.2.20}$$

We notice the state σ has the sector lengths

$$S_1 = (2p-1)^2, \tag{2.2.21}$$

$$S_2 = 1 + 2[2pab + 2(1-p)cd]^2 + 2[p(a^2 - b^2) - (1-p)(c^2 - d^2)]^2, \tag{2.2.22}$$

$$S_3 = (2p-1)^2 + 2[2pab - 2(1-p)cd]^2. \tag{2.2.23}$$

Thus this state satisfies the equality $S_2 + S_3 = 3(1 + S_1)$ and lies on the plane displayed as the boundary between the red and green areas in the polytope in Fig. 2.1.

Next, we discuss evidence for the validity of Eq. (2.2.11) for mixtures of different bipartitions. Here we give the analytical evidence:

Result 5. *For three-qubit systems, a rank-2 mixture of two pure biseparable states with respect to different partitions obeys the biseparability criterion in Eq. (2.2.11).*

Proof. Let ϱ be a rank-2 mixture of two pure biseparable states with respect to different partitions, without loss of generality, $A|BC$ and $AB|C$:

$$\varrho = p\,|\Psi\rangle\langle\Psi| + (1-p)\,|\Phi\rangle\langle\Phi|\,, \tag{2.2.24}$$

where $0 \leq p \leq 1$, and without loss of generality, we can write

$$|\Psi\rangle = |0\rangle \otimes (\lambda_0\,|00\rangle + \lambda_1\,|11\rangle)\,, \quad 0 \leq \lambda_0,\, \lambda_1 \leq 1, \quad \lambda_0^2 + \lambda_1^2 = 1,$$
$$|\Phi\rangle = \sum_{i,j=0}^{1} \kappa_{ij}\,|ij\rangle \otimes (c_0\,|0\rangle + c_1\,|1\rangle)\,, \quad \kappa_{ij},\, c_1,\, c_2 \in \mathbb{C}, \quad \sum_{i,j=0}^{1} |\kappa_{ij}|^2 = |c_0|^2 + |c_1|^2 = 1.$$

Now, we define a function

$$f(\varrho_1, \varrho_2) \equiv 1 + \mathrm{tr}(\varrho_1\varrho_2) - \mathrm{tr}(\varrho_{A_1}\varrho_{A_2}) - \mathrm{tr}(\varrho_{B_1}\varrho_{B_2}) - \mathrm{tr}(\varrho_{C_1}\varrho_{C_2}), \tag{2.2.25}$$

where ϱ_i $(i = 1, 2)$ are three-particle quantum states and ϱ_{X_i} for $X \in \{A, B, C\}$ are their reduced density matrices on the subsystems X. Our aim is to prove that the biseparable state ϱ obeys

$$1 + \mathrm{tr}(\varrho^2) \leq \mathrm{tr}(\varrho_A^2) + \mathrm{tr}(\varrho_B^2) + \mathrm{tr}(\varrho_C^2). \tag{2.2.26}$$

This is equivalent to proving that the following function $F(\varrho)$ is non-positive:

$$\begin{aligned} F(\varrho) &\equiv 1 + \mathrm{tr}(\varrho^2) - \mathrm{tr}(\varrho_A^2) - \mathrm{tr}(\varrho_B^2) - \mathrm{tr}(\varrho_C^2) \\ &= p^2 f(\Psi, \Psi) + (1-p)^2 f(\Phi, \Phi) + 2p(1-p) f(\Psi, \Phi). \end{aligned} \tag{2.2.27}$$

Direct calculations yield

$$f(\Psi, \Psi) = 1 - 2(\lambda_0^4 + \lambda_1^4), \tag{2.2.28}$$
$$f(\Phi, \Phi) = 1 - 2\mathrm{tr}(\kappa\kappa^\dagger\kappa\kappa^\dagger), \tag{2.2.29}$$
$$\begin{aligned} f(\Psi, \Phi) = 1 &+ |\lambda_0\kappa_{00}c_0 + \lambda_1\kappa_{01}c_1|^2 - (\kappa_{00}^2 + \kappa_{01}^2) \\ &- \left[\lambda_0^2(\kappa_{00}^2 + \kappa_{10}^2) + \lambda_1^2(\kappa_{01}^2 + \kappa_{11}^2)\right] - \left(\lambda_0^2|c_0|^2 + \lambda_1^2|c_1|^2\right), \end{aligned} \tag{2.2.30}$$

where $\kappa = (\kappa_{ij})$. Here, since κ_{ij} and c_i can be taken as real, we obtain that

$$|\lambda_0\kappa_{00}c_0 + \lambda_1\kappa_{01}c_1|^2 \leq 2\left(\lambda_0^2\kappa_{00}^2c_0^2 + \lambda_1^2\kappa_{01}^2c_1^2\right). \tag{2.2.31}$$

Also, for the 2×2 matrix κ, we know that $1 - 2\mathrm{tr}(\kappa\kappa^\dagger\kappa\kappa^\dagger) = 4(\det\kappa)^2 - 1$. Thus we have

$$\begin{aligned} F(\varrho) \leq\; & p^2\left[1 - 2(\lambda_0^4 + \lambda_1^4)\right] + (1-p)^2\left[4(\det\kappa)^2 - 1\right] \\ & + 2p(1-p)\Big\{1 + \lambda_0^2c_0^2(2\kappa_{00}^2 - 1) + \lambda_1^2c_1^2(2\kappa_{01}^2 - 1) - (\kappa_{00}^2 + \kappa_{01}^2) \\ & - \lambda_0^2(\kappa_{00}^2 + \kappa_{10}^2) - \lambda_1^2(\kappa_{01}^2 + \kappa_{11}^2)\Big\}. \end{aligned} \tag{2.2.32}$$

Now, it is sufficient to show that the maximization of the right-hand side is non-positive. In fact, the best choice is to set

$$c_0^2 = 1, \qquad c_1^2 = 0, \qquad \text{if } (2\kappa_{01}^2 - 1)\lambda_1^2 \leq (2\kappa_{00}^2 - 1)\lambda_0^2, \tag{2.2.33}$$

$$c_1^2 = 1, \qquad c_0^2 = 0, \qquad \text{if } (2\kappa_{00}^2 - 1)\lambda_0^2 \leq (2\kappa_{01}^2 - 1)\lambda_1^2. \tag{2.2.34}$$

Let us consider the former case: $c_0^2 = 1$ and $c_1^2 = 0$. Due to that $\sum_{i,j} \kappa_{ij}^2 = \lambda_0^2 + \lambda_1^2 = 1$, we find

$$\begin{aligned} F(\varrho) \leq p^2 \left\{ 1 - 2\left[\lambda_0^4 + (1-\lambda_0^2)^2\right] \right\} + (1-p)^2 \left[4(\det \kappa)^2 - 1 \right] \\ + 2p(1-p)\left(\kappa_{10}^2 - \kappa_{01}^2 - 2\lambda_0^2 \kappa_{10}^2 \right). \end{aligned} \tag{2.2.35}$$

Maximization of the right-hand side with respect to λ_0^2 can be achieved by three cases: (1) $\lambda_0^2 = 0$, (2) $\lambda_0^2 = 1$, (3) $\lambda_0^2 = [1 - (1-p)\kappa_{10}^2/2p]/2$ if $\kappa_{10} < p/(1-p)$. In all cases, we can immediately show that $F(\varrho) \leq 0$. □

2.2.5 Comparison with existing criteria

Our results show that not only the three-body second moment $\mathcal{R}_{ABC}^{(2)}$, but also the one- and two-body reduced moments such as $\mathcal{R}_{AB}^{(2)}$ and $\mathcal{R}_{A}^{(2)}$ can be useful for entanglement detection. In fact, their linear combinations allow detecting entangled states more efficiently than existing criteria [257, 351, 352, 375].

Here, we focus on the case of qubit systems. The existing criteria are as follows. (i) any fully separable three-qubit state obeys $S_3 \leq 1$ [257, 350]. If this inequality is violated, the state is entangled but it may be still separable for some bipartition. (ii) any biseparable three-qubit state obeys $S_3 \leq 3$ [257, 352]. If this is violated, the state is genuinely tripartite entangled. Note that these existing criteria can straightforwardly be derived from the convexity and convolution of sector lengths. In the following, we will show that our criteria in Eqs. (2.2.5, 2.2.11) significantly improve the existing criteria, introducing some examples.

A good example of three-qubit states is the noisy GHZ-W mixed states [421, 422]:

$$\varrho = g\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + w\,|\mathrm{W}\rangle\langle\mathrm{W}| + \frac{1-g-w}{8}\mathbb{1}^{\otimes 3}, \tag{2.2.36}$$

where $0 \leq g, w \leq 1$, and the GHZ state and the W state are given by $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. The noisy GHZ-W mixed state has

$$(S_1, S_2, S_3) = \left(w^2/3, 3g^2 + 3w^2 - 2gw, 4g^2 + 11w^2/3 \right). \tag{2.2.37}$$

To analyze this state, we will consider three cases: (i) the noisy GHZ state, i.e., $w = 0$ (ii) the noisy W state, i.e., $g = 0$ (iii) the GHZ-W mixed state, i.e., $g + w = 1$. Now we summarize our result as follows:

Criteria for full separability			
Three-qubit states	$S_3 \leq 1$	Eq. (2.2.5)	Optimal values
$w = 0$	$g \leq 0.5$	$g \leq 0.447$	$g \leq 0.2$ [172]
$g = 0$	$w \leq 0.522$	$w \leq 0.469$	$w \leq 0.177$ [423]
$g + w = 1$	Detect all states	Detect all states	

Table 2.1: Results for the fully separable criterion in Eq. (2.2.5), compared with the existing criterion $S_3 \leq 1$ and the optimal values. For $w = 0$ or $g = 0$, the noisy mixed GHZ and W state are known to be fully separable iff $g \leq 0.2$ [172] and $w \leq 0.177$ [423]. Clearly, the bound in Eq. (2.2.5) improves the existing bound $S_3 \leq 1$. This table is a modified version of a table from Ref. [1].

Result 6. *Tables 2.1 and 2.2 list the results of our criteria, comparing them to the existing criteria and the optimal values. Also, the criteria for the state in Eq. (2.2.36) are illustrated on the $g - w$ plane in Fig. 2.2.*

2.3 Detection of high-dimensional entanglement

2.3.1 Optimal entanglement criterion

In many realistic scenarios, it is sufficient to detect entanglement across some fixed bipartition $I|\bar{I}$ of the multiparticle system. For this task, second moments of randomized measurements can be used as well: Performing random measurements at each qubit and considering the second moments allows one to generalize the moments in Eq. (2.2.2) for the given number of qubits. In turn, these moments allow one to determine the quantities $\mathrm{tr}(\varrho_I^2)$, $\mathrm{tr}(\varrho_{\bar{I}}^2)$, and $\mathrm{tr}(\varrho^2)$ for the reduced states of the bipartition and the global state. This approach has been used in an experiment [413], where entanglement criteria with the second-order Rényi entropy $H_2(\varrho_X) = -\log\left[\mathrm{tr}(\varrho_X^2)\right]$ were employed. The entropic criteria for separable states read $H_2(\varrho_X) \leq H_2(\varrho)$ for $X = I, \bar{I}$; if this is violated, then ϱ is entangled [64, 209, 412] and also see Eq. (1.2.54).

Using our methods, we can show that this approach is optimal. To formulate the result, we assume that both sides of the bipartition have the same number of qubits. Then, recall that any bipartite state can be written as

$$\varrho_{AB} = \frac{1}{d^2} \sum_{i,j=0}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j, \tag{2.3.1}$$

where $\lambda_0 = \mathbb{1}$ denotes the identity matrix and λ_i are the Gell-Mann matrices [25, 26]. This is the decomposition of ϱ_{AB} using the basis of Hermitian, orthogonal, and traceless matrices, i.e., $\lambda_i = \lambda_i^\dagger$, $\mathrm{tr}\left[\lambda_i \lambda_j\right] = d\delta_{ij}$, and $\mathrm{tr}\left[\lambda_i\right] = 0$ for $i > 0$. The

Criteria for biseparability			
Three-qubit states	$S_3 \leq 3$	Eq. (2.2.11)	Optimal values
$w = 0$	$g \leq 0.866$	$g \leq 0.655$	$g \leq 0.429$ [274]
$g = 0$	$w \leq 0.905$	$w \leq 0.728$	$w \leq 0.479$ [424]
$g + w = 1$	$g \in [0.102, 0.855]$	$g \in [0.297, 0.612]$	

Table 2.2: Results for the biseparable criterion in Eq. (2.2.11), compared with the existing criterion $S_3 \leq 3$ and the optimal values. For $w = 0$ or $g = 0$, the noisy mixed GHZ and W state are known to be biseparable iff $g \leq 0.429$ [274] and $w \leq 0.479$ [424]. For $g + w = 1$ ($w = 1 - g$), the existing criterion and our criterion in Eq. (2.2.11), respectively, imply that the GHZ-W mixed state can be biseparable only in some interval for g. Interestingly, Ref. [421] has analyzed the GHZ-W mixed states using the three-tangle τ and the squared concurrences C^2_{XY} measuring bipartite entanglement in the reduced states (note that all reduced states are equivalent), for details see Sec. 1.2. It has been shown that in a region $0.292 \leq g \leq 0.627$, the state has zero three-tangle and zero concurrence in the reduced states. This region is larger than the region which is not detected by Eq. (2.2.11). Thus, it can detect multiparticle entanglement even when the three-tangle, as well as tripartite entanglement in reduced states, vanishes. This table is a modified version of a table from Ref. [1].

quantities of interest are

$$S_2 = \sum_{i,j=1}^{d^2-1} t_{ij}^2, \quad S_1^A = \sum_{i=1}^{d^2-1} t_{i0}^2, \quad S_1^B = \sum_{i=1}^{d^2-1} t_{0i}^2. \tag{2.3.2}$$

We also define $S_1 = S_1^A + S_1^B$, which allows to recover the purities via

$$\mathrm{tr}(\varrho_{AB}^2) = \frac{1}{d^2}(1 + S_1 + S_2), \quad \mathrm{tr}(\varrho_A^2) = \frac{1}{d}(1 + S_1^A). \tag{2.3.3}$$

It is interesting that, although the λ_i are not directly linked to a quantum design, the quantities S_1^A, S_1^B, and S_2 are also second moments of measurement of the observables λ_i in random bases. The proof follows from a slight extension of the arguments given in Ref. [350], which will be discussed later. This opens another possibility for an experimental implementation besides making randomized Pauli measurements on all the qubits individually. Now, we can formulate:

Result 7. *Any two-qudit separable state obeys the relation*

$$S_2 \leq d - 1 + \min\{(d-1)S_1^A - S_1^B, (d-1)S_1^B - S_1^A\}. \tag{2.3.4}$$

For $S_1^A \leq S_1^B$, this relation becomes

$$S_2 \leq d - 1 + (d-1)S_1^A - S_1^B, \tag{2.3.5}$$

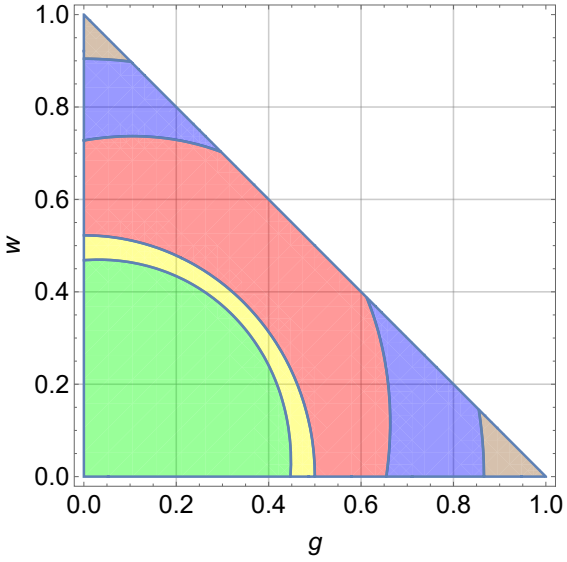

Figure 2.2: Entanglement criteria for the noisy GHZ-W state in Eq. (2.2.36) in the $g - w$ plane. Previously, several works [422, 425] have discussed entanglement criteria in this two-parameter space. The fully separable states are contained in the green area, obeying our criterion (2.2.5). The outside of the green and yellow areas corresponds to the biseparable or genuine entangled states that violate a previously known criterion for fully separable states, $S_3 \leq 1$. Thus, the yellow area marks the improvement of our criterion (2.2.5) compared with previous results. Also, states that are biseparable for some partitions are contained in the union of the green, yellow, and red areas, characterized by our criterion (2.2.11). The brown area corresponds to the genuine entangled states violating a previously known criterion for biseparable states, $S_3 \leq 3$. Thus, the blue area marks the improvement of our criterion (2.2.11) compared with previous results. This figure is taken from Ref. [1].

as well as the analogous one with parties A and B exchanged. This is equivalent to the criterion $H_2(\varrho_X) \leq H_2(\varrho_{AB})$ for $X \in \{A, B\}$, where H_2 denotes the second-order Rényi entropy and ϱ_X denote the reduced density matrices. This criterion is optimal, in the sense that if the inequality holds for S_1^A, S_1^B and S_2, then there is a separable state compatible with these values.

Proof. The criterion itself was established before, so we only have to prove the optimality statement. Let ϱ_{sep} be a two-qudit separable state. Here, the entropic criterion [64, 412] states that any bipartite separable state obeys that $H_2(\varrho_A) \leq H_2(\varrho_{\text{sep}})$ and $H_2(\varrho_B) \leq H_2(\varrho_{\text{sep}})$, where ϱ_X denote the reduced density matrices of ϱ_{sep}. The entropic inequalities can be written as

$$\text{tr}(\varrho_{\text{sep}}^2) \leq \text{tr}(\varrho_A^2), \qquad \text{tr}(\varrho_{\text{sep}}^2) \leq \text{tr}(\varrho_B^2). \tag{2.3.6}$$

Using the relation in Eq. (1.4.13), we can respectively translate these inequalities to

$$S_2 \leq d - 1 + (d-1)S_1^A - S_1^B, \qquad S_2 \leq d - 1 + (d-1)S_1^B - S_1^A. \tag{2.3.7}$$

Thus we have Eq. (2.3.4).

The novel point is proving the optimality. In the following, we show that for $S_1^A \leq S_1^B$, Eq. (2.3.5) is saturated by a family of separable states

$$\varrho(p,\theta) = p\,|00\rangle\langle 00| + q\sum_{j=1}^{d-1} |j\rangle\langle j| \otimes |\theta_{0j}\rangle\langle\theta_{0j}|\,, \tag{2.3.8}$$

$$|\theta_{ij}\rangle = \cos\theta\,|i\rangle + \sin\theta\,|j\rangle\,, \quad q = \frac{1-p}{d-1}, \quad p \in [1/d, 1], \quad \theta \in [0, \pi/2]. \tag{2.3.9}$$

Note that a family for the other case ($S_1^B \leq S_1^A$) can be found if the two parties of $\varrho(p,\theta)$ are interchanged. In fact, from Eqs. (2.3.6, 2.3.7), we immediately notice that Eq. (2.3.5) is saturated iff $\mathrm{tr}(\varrho_{\mathrm{sep}}^2) = \mathrm{tr}(\varrho_A^2)$. For the state (2.3.8), we find

$$\mathrm{tr}(\varrho_A^2) = p^2 + (d-1)q^2 = \mathrm{tr}\left(\varrho(p,\theta)^2\right), \tag{2.3.10}$$

$$\mathrm{tr}(\varrho_B^2) = \mathrm{tr}(\varrho_A^2) + 2(d-1)pq\cos^2(\theta) + 2\binom{d-1}{2}q^2\cos^4(\theta), \tag{2.3.11}$$

which results in

$$S_1^A = dp^2 + d(d-1)q^2 - 1, \tag{2.3.12}$$

$$S_1^B = S_1^A + 2d(d-1)pq\cos^2(\theta) + 2d\binom{d-1}{2}q^2\cos^4(\theta). \tag{2.3.13}$$

We notice that for $p \in [1/d, 1]$, S_1^A varies between 0 and $d-1$. In fact, for fixed p and $\theta \in [0, \pi/2]$, S_1^B ranges from $d-1$ to S_1^A. This covers the whole region of allowed values with $S_1^A \leq S_1^B$. For the other half, one can swap the parties of $\varrho(p,\theta)$. □

Remark 3. The geometrical expression of Eq. (2.3.4) is displayed by Fig. 2.3. Also, for $\theta = \pi/2$, i.e., $S_1^A = S_1^B$, one obtains the relation

$$S_2 \leq d - 1 + \frac{d-2}{2}S_1, \tag{2.3.14}$$

which is also expressed geometrically in Fig. 2.4. In the next subsection, we will discuss how to construct the polytope of all admissible values of S_1^A, S_1^B, and S_2.

Remark 4. The unfortunate consequence of the optimality statement is that any PPT entanglement cannot be detected by the quantities S_1^A, S_1^B and S_2 as the entropic criterion is strictly weaker than the PPT criterion [210]. In Sec. 2.4, we will overcome this obstacle by developing a general criterion for entanglement using higher moments of randomized measurements.

2.3.2 Characterization of two-qudit states

Here we discuss the characterization of two-qudit states based on Result 7. First, we consider the geometrical interpretation using the two-dimensional plane of (S_1, S_2). Second, we demonstrate our entanglement criterion by comparing it with existing criteria.

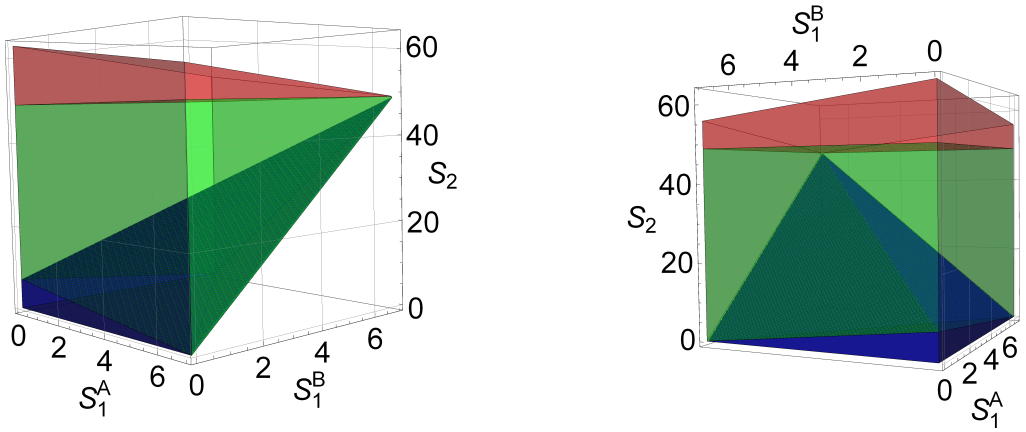

Figure 2.3: Geometry of the state space of $d \otimes d$-dimensional systems in terms of the quantities S_1^A, S_1^B, and S_2, where $d = 8$. The total polytope is the set of all states, characterized by the inequalities $0 \leq S_1^A, S_1^B \leq d-1$, $0 \leq S_2 \leq d^2-1$, $S_1^A + S_1^B + S_2 \leq d^2 - 1$, and $0 \leq (d-1)^2 - (d-1)(S_1^A + S_1^B) + S_2$. The separable states are contained in the blue polytope, obeying the additional constraint in Eq. (2.3.4). The red area corresponds to the states violating a previously known criterion for separable states, $S_2 \leq (d-1)^2$ [350]. Thus, the green area marks the improvement coming from our criterion (2.3.4) compared with the previous result. These figures are modified versions of figures from Ref. [1].

Geometrical interpretation

First, let us characterize two-qudit states using sector lengths. This characterization can be useful for understanding the two-qudit separability criterion geometrically. The previous work [352] has illustrated the set of admissible (S_1, S_2) pairs in two-qubit systems, we will generalize it to two-qudit systems. We begin by recalling that any two-qudit state can be written as

$$\varrho_{AB} = \frac{1}{d^2} \sum_{i,j=0}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j = \frac{1}{d^2} \left(\mathbb{1}^{\otimes 2} + P_1 + P_2 \right), \tag{2.3.15}$$

where the Hermitian operators P_k for $k = 1, 2$ denote the sum of all terms in the basis element weight k. The relation in Eq. (1.4.13) allows us to translate the purity bound $\mathrm{tr}(\varrho_{AB}^2) \leq 1$ to

$$1 + S_1 + S_2 \leq d^2. \tag{2.3.16}$$

Remember that $S_1 = S_1^A + S_1^B$.

As examples of pure states, consider product states $|\mathrm{prod}_j\rangle = |jj\rangle$ with the computational basis for $j = 0, 1, \ldots, (d-1)$. The pure product states have $S_1^A = S_1^B = d-1$, $S_1 = 2(d-1)$, and $S_2 = (d-1)^2$. Also, the maximally entangled state $|\Phi_d^+\rangle = (1/\sqrt{d}) \sum_{i=0}^{d-1} |ii\rangle$ has $S_1^A = S_1^B = S_1 = 0$ and $S_2 = d^2 - 1$.

It is important to note that the pure product states and the maximally entangled state can, respectively, maximize the admissible values of S_1 and S_2 for

all two-qudit states (see Ref. [353]). That is, both values of sector lengths give tight upper bounds for all two-qudit states: $S_1 \leq 2(d-1)$ and $S_2 \leq d^2 - 1$. Due to the purity condition in Eq. (2.3.16), any pure two-qudit state must satisfy $S_1 \in [0, 2(d-1)]$ and $S_2 = d^2 - 1 - S_1$.

To see another constraint on sector lengths, let us recall the state inversion in Sec. 1.1, expressed as

$$\tilde{\varrho}_{AB} = \frac{1}{d^2}\left\{(d-1)^2 \mathbb{1}^{\otimes 2} - (d-1)P_1 + P_2\right\}. \tag{2.3.17}$$

Since $\tilde{\varrho}_{AB}$ is positive, we have

$$0 \leq \mathrm{tr}(\varrho_{AB}\tilde{\varrho}_{AB}). \tag{2.3.18}$$

From the relation (1.4.13) and the expression (2.3.15), the condition (2.3.18) leads to the state inversion bound:

$$0 \leq (d-1)^2 - (d-1)S_1 + S_2. \tag{2.3.19}$$

Here, if $S_2 = 0$, then $S_1 \leq d-1$, where equality holds if a state is given by, for example, $|0\rangle\langle 0| \otimes \mathbb{1}/d$.

In conclusion, we obtained the tight four bounds: $S_1 \leq 2(d-1)$, $S_2 \leq d^2 - 1$, and Eqs. (2.3.16, 2.3.19). These linear constraints on S_1 and S_2 allow us to ensure the positivity of two-qudit states and to find the total set of their admissible values. The geometrical expressions are displayed in Fig. 2.4.

Entanglement detection

Next, let us consider the entanglement detection of two-qudit states. One existing criterion states that any two-qudit separable state obeys $S_2 \leq (d-1)^2$ [350], where an example of states obeying $S_2 = (d-1)^2$ is $|\mathrm{prod}_j\rangle$. In particular, the maximally entangled state $|\Phi_d^+\rangle$ maximally violates this inequality.

Now, we look at the gap between the maximally entangled state and the pure product state

$$\frac{S_2(\Phi_d^+)}{S_2(\mathrm{prod}_j)} = \frac{d^2-1}{(d-1)^2} \to 1, \quad d \gg 2. \tag{2.3.20}$$

This scaling tells us that the simple criterion cannot be useful in very high-dimensional systems. On the other hand, the criteria (2.3.4, 2.3.14) allow us to detect entanglement much more powerfully than the existing criterion since they are expressed as the tilted bounds geometrically, see Figs. 2.3 and 2.4.

To see that, we consider the two-qudit isotropic state:

$$\varrho_{\mathrm{iso}} = p\,|\Phi_d^+\rangle\langle\Phi_d^+| + \frac{1-p}{d^2}\mathbb{1}^{\otimes 2}, \tag{2.3.21}$$

which has $(S_1, S_2) = (0, p^2(d^2-1))$. The existing criterion $S_2 \leq (d-1)^2$ detects this state as entangled for $p > \sqrt{d-1}/\sqrt{d+1}$, while Eq. (2.3.14) detects it already for $p > 1/\sqrt{d+1}$, and the state is known to be entangled iff $p > 1/(d+1)$.

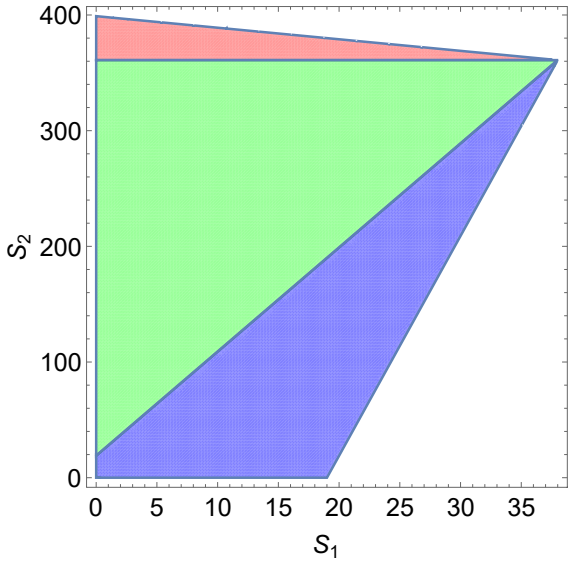

Figure 2.4: Geometry of the state space of $d \otimes d$-dimensional systems in terms of the second moments S_1 and S_2, where $d = 20$. The total figure is the set of all states, characterized by the same inequalities with Fig. 2.3 in the case $S_1^A = S_1^B$. The separable states are contained in the blue area, obeying the additional bound in Eq. (2.3.14). The red area corresponds to the state violating a previously known criterion for separable states, $S_2 \leq (d-1)^2$ [350]. Thus, the green area marks the improvement of our criterion in Eq. (2.3.4) compared with the previous result. This figure is a modified version of a figure from Ref. [1].

2.4 Detection of bound entanglement

2.4.1 Integrals over pseudo-Bloch spheres

In higher-dimensional systems, different forms of entanglement exist e.g., entanglement of different dimensionality [124, 184] or bound entanglement [166, 227, 230, 232]. The previously known criteria for randomized measurements face serious problems in this scenario. First, criteria using purities, such as the criterion in Eq. (2.3.4), can only characterize states that violate the PPT criterion and hence miss the bound entanglement.

Second, while the notion of randomized measurements is independent of the dimension, many results for qubits employ the concept of a Bloch sphere, which is not available for higher dimensions, where not all observables are equivalent under randomized unitaries. Ref. [350] showed that some results for qubits are also valid for higher dimensions as long as only second moments are considered, but these connections are definitely not valid for higher moments. More detailed explanations will be given in the next subsection.

To overcome these problems, we first note that a general observable is characterized by its eigenvectors, determining the probabilities of the outcomes, and the eigenvalues, corresponding to the observed values. For computing the mo-

ments $\mathcal{R}_{AB}^{(r)}$ in Eq. (2.1.1), the eigenvectors do not matter due to the averaging over all unitaries. The eigenvalues are relevant, but they may be altered in classical postprocessing: Once the frequencies of the outcomes are recorded, one can calculate the moments $\mathcal{R}_{AB}^{(r)}$ in Eq. (2.1.1) for different assignments of values to the outcomes.

So the question arises, whether one can choose the eigenvalues of an observable in a way, such that the moments $\mathcal{R}_{AB}^{(r)}$ in Eq. (2.1.1) are easily tractable. For instance, it would be desirable to write them as averages over a high-dimensional sphere (the so-called pseudo-Bloch sphere). The reason is that several entanglement criteria, such as the computable cross norm or realignment criterion [241, 242] and the de Vicente (dV) criterion [244], make also use of a pseudo-Bloch sphere. Surprisingly, the desired eigenvalues can always be found:

Result 8. *Consider an arbitrary observable in a higher-dimensional system. Then, one can change its eigenvalues such that for the resulting observable M_d, the second and fourth moments $\mathcal{R}_{AB}^{(r)}$ in Eq. (2.1.1) equal, up to a factor, a moment $\mathcal{S}_{AB}^{(r)}$ which is taken by an integral over a generalized pseudo-Bloch sphere. That is, $\mathcal{S}_{AB}^{(r)}$ is given by*

$$\mathcal{S}_{AB}^{(r)} = N(r,d) \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 [\mathrm{tr}(\varrho_{AB} \boldsymbol{\alpha}_1 \cdot \boldsymbol{\lambda} \otimes \boldsymbol{\alpha}_2 \cdot \boldsymbol{\lambda})]^r, \tag{2.4.1}$$

where $\boldsymbol{\alpha}_i$ denote (d^2-1)-dimensional unit real vectors uniformly distributed from the pseudo-Bloch sphere, and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_{d^2-1})$ is the vector of Gell-Mann matrices. Furthermore, $N(r,d)$ is a normalization factor.

Remark 5. A more detailed explanation is given in the next subsection, where the detailed form of M_d is given. To give a simple example, for $d = 3$ one may measure the standard spin measurement J_z and assign the values α_+/γ, α_-/γ and $2\beta/\gamma$ instead of the standard values ± 1 and 0 to the three possible outcomes, where $\alpha_\pm = \pm 3 - \beta$, $\beta = -\sqrt{7+2\sqrt{15}}$, and $\gamma = 2\sqrt{5+\sqrt{15}}$. Note that the resulting observable is also traceless.

2.4.2 Detailed explanations about Result 8

Let us elaborate on the relation between the moments $\mathcal{R}_{AB}^{(r)}$ and $\mathcal{S}_{AB}^{(r)}$ more explicitly. In order to explain the difficulties for higher dimensions, let us focus on qubits first. Suppose that Alice and Bob locally perform the measurements M_A and M_B in random bases parameterized by the unitary transformations $U_A, U_B \in \mathcal{U}(d)$, such that

$$\{|u_0\rangle_A = U_A |0\rangle_A, |u_1\rangle_A = U_A |1\rangle_A, \ldots, |u_{d-1}\rangle_A = U_A |d-1\rangle_A\}, \tag{2.4.2}$$
$$\{|u_0\rangle_B = U_B |0\rangle_B, |u_1\rangle_B = U_B |1\rangle_B, \ldots, |u_{d-1}\rangle_B = U_B |d-1\rangle_B\}. \tag{2.4.3}$$

In the case of qubits ($d = 2$), Alice's (Bob's) measurement direction corresponds to a random three-dimensional unit vector $\boldsymbol{u}_A$ ($\boldsymbol{u}_B$) chosen uniformly on the

Bloch sphere $\mathcal{S}^2$. Then, the expectation value is given by $\mathrm{tr}\left[\varrho_{AB}\sigma_{\boldsymbol{u}_A}\otimes\sigma_{\boldsymbol{u}_B}\right]$, where $\sigma_{\boldsymbol{u}}=\boldsymbol{u}\cdot\boldsymbol{\sigma}$ is the rotated Pauli matrix with the vector of the usual Pauli matrices $\boldsymbol{\sigma}=(\sigma_x,\sigma_y,\sigma_z)^\top$. Without loss of generality, one can take the Pauli-Z matrix σ_z as the observables M_A and M_B.

Then we can characterize the obtained distribution via its moments $\mathcal{R}_{AB}^{(r)}$

$$\mathcal{R}_{AB}^{(r)}=\int dU_A\int dU_B\left\{\mathrm{tr}[\varrho_{AB}(U_A\sigma_z U_A^\dagger)\otimes(U_B\sigma_z U_B^\dagger)]\right\}^r \tag{2.4.4}$$

$$=\frac{1}{(4\pi)^2}\int_{\mathcal{S}^2}d\boldsymbol{u}_A\int_{\mathcal{S}^2}d\boldsymbol{u}_B\left[\mathrm{tr}\left(\varrho_{AB}\sigma_{\boldsymbol{u}_A}\otimes\sigma_{\boldsymbol{u}_B}\right)\right]^r, \tag{2.4.5}$$

where the unitaries are typically chosen according to the Haar distribution. For all odd r, the moments $\mathcal{R}_{AB}^{(r)}$ vanish, so the quantities of interest are the moments of even r. Indeed, the second moment $\mathcal{R}_{AB}^{(2)}$ can be evaluated by a unitary two-design, see Sec. 1.5:

$$\mathcal{R}_{AB}^{(2)}=\frac{1}{9}\sum_{\boldsymbol{e}_A,\boldsymbol{e}_B=\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3}\mathrm{tr}\left[\varrho_{AB}\sigma_{\boldsymbol{e}_A}\otimes\sigma_{\boldsymbol{e}_B}\right]^2=\frac{1}{9}\sum_{i,j=1}^{3}t_{ij}^2, \tag{2.4.6}$$

where $\{\pm\boldsymbol{e}_k\mid k=1,2,3\}$ are the orthogonal local directions and the t_{ij} are two-body correlation coefficients with $1\leq i,j\leq 3$ in the Bloch decomposition of ϱ_{AB}, where we call this submatix T_s. It is important that the moments $\mathcal{R}_{AB}^{(r)}$ are by definition invariant under local unitary transformations $U_A\otimes U_B$. This property allows us to find a local unitary such that the matrix T_s can be diagonalized by an orthogonal transformation, due to the isomorphism between $\mathrm{SO}(3)$ and $\mathrm{SU}(2)$.

On the other hand, in the case of higher dimensions ($d>2$), there are several problems. First, the notion of a Bloch sphere is not available. Due to this fact, not all possible observables are equivalent under randomized unitaries. Second, for a odd r, the moments $\mathcal{R}_{AB}^{(r)}$ in Eq. (2.1.1) do not vanish, see Ref. [426]. Third, for $r=2$, the second moments are independent of the choice of observables as long as the observables are traceless (see Theorem 9 in Ref. [350]), while higher moments depend on the choice. To approach these problems, we make use of the quantities from the previous subsection, i.e., the moments $\mathcal{S}_{AB}^{(r)}$ in Eq. (2.4.1). Here, $N(r,d)$ is a normalization factor such that $\mathcal{S}_{AB}^{(r)}=1$ at pure product states:

$$N(r,d)=\frac{[(d^2+r-3)!!]^2}{(d-1)^r[(r-1)!!]^2[(d^2-3)!!]^2}\left(\frac{\Gamma(\frac{d^2-1}{2})}{2\sqrt{\pi}^{d^2-1}}\right)^2, \tag{2.4.7}$$

where, for a positive number n, $n!!$ is the double factorial and $\Gamma(n)$ is the gamma function. The moments $\mathcal{S}_{AB}^{(r)}$ are analytically calculable, so we take $\mathcal{S}_{AB}^{(r)}$ as the starting point for our discussion. Now we can find the following result:

Result 9. *The moments defined in Eq. (2.4.1) are given by*

$$\mathcal{S}_{AB}^{(2)} = V \sum_{i,j} t_{ij}^2, \tag{2.4.8}$$

$$\mathcal{S}_{AB}^{(4)} = W \left\{ 3 \sum_{i,j} t_{ij}^4 + 3 \sum_{i,j,k,i\neq j} t_{ik}^2 t_{jk}^2 + 3 \sum_{i,j,k,i\neq j} t_{ki}^2 t_{kj}^2 + \sum_{i,j,k,l,i\neq k,j\neq l} (t_{ij}^2 t_{kl}^2 + 2 t_{ij} t_{il} t_{kj} t_{kl}) \right\}, \tag{2.4.9}$$

where the t_{ij} are the coefficients from Eq. (2.3.1) and

$$V = \frac{1}{(d-1)^2}, \qquad W = \frac{1}{3\,(d-1)^4}. \tag{2.4.10}$$

Remark 6. The proof of this derivation is given in Sec. 9.1. It is essential that the moments $\mathcal{S}_{AB}^{(r)}$ are invariant not only overall local unitaries but also overall changes of local operator basis $\boldsymbol{\lambda}$, meaning the independence of the specific choice of observable. That is, the moments $\mathcal{S}_{AB}^{(r)}$ are invariant under orthogonal transformations of the submatrix T_{s}, where $T_{\mathrm{s}} = (t_{ij})$ with $1 \leq i, j \leq d^2 - 1$ in Eq. (2.3.1). This orthogonal invariance allows us to consider the diagonalization of the submatrix T_{s}

$$T_{\mathrm{s}}' = O_A T_{\mathrm{s}} O_B^{\top} = \mathrm{diag}(\tau_1, \tau_2, \ldots, \tau_{d^2-1}), \tag{2.4.11}$$

where $O_A, O_B \in \mathrm{SO}(d^2 - 1)$ are non-physical orthogonal matrices and $\tau_i \geq 0$ are singular values of T_{s}. With this, we are able to reduce the number of parameters for the moments $\mathcal{S}_{AB}^{(r)}$. In fact, the evaluated second and fourth moments (2.4.8, 2.4.9) can be simply expressed as

$$\mathcal{S}_{AB}^{(2)} = V \sum_{i=1}^{d^2-1} \tau_i^2, \tag{2.4.12}$$

$$\mathcal{S}_{AB}^{(4)} = W \left[2 \sum_{i=1}^{d^2-1} \tau_i^4 + \left(\sum_{i=1}^{d^2-1} \tau_i^2 \right)^2 \right] = W \left[2 \sum_{i=1}^{d^2-1} \tau_i^4 + \frac{1}{V^2} \left(\mathcal{S}_{AB}^{(2)} \right)^2 \right], \tag{2.4.13}$$

where $V = 1/(d-1)^2$ and $W = 1/3(d-1)^4$.

The question here is whether it is possible to find observables such that $\mathcal{R}_{AB}^{(r)}$ coincides with $\mathcal{S}_{AB}^{(r)}$, up to a constant. While the observables M_A and M_B do not have to be diagonal, they can be assumed to be diagonal in the unitary group averaging. Now let us consider a diagonal observable such that $M_A = M_B = M_d$. Then, we are in a position to present the suitable choice of M_d for the coincidence between $\mathcal{S}_{AB}^{(r)}$ and $\mathcal{R}_{AB}^{(r)}$:

Result 10. *In d-dimensional quantum systems where d is odd, let the diagonal observable M_d be given by*

$$M_d = \mathrm{diag}(\underbrace{\alpha_+, \ldots, \alpha_+}_{(d-1)/2}, \beta_y, \underbrace{\alpha_-, \ldots, \alpha_-}_{(d-1)/2}), \tag{2.4.14}$$

where

$$\alpha_\pm = \frac{\pm d - 2y + 1}{\sqrt{(d-1)[(2y-1)^2 + d)]}}, \tag{2.4.15}$$

$$\beta_y = -\sqrt{\frac{(d-1)(2y-1)^2}{(2y-1)^2 + d}}, \tag{2.4.16}$$

$$y = \frac{1}{2}\left[1 - \sqrt{1 + \frac{d + 3 + \sqrt{d^3 + 3d^2 + d + 3}}{d-2}}\right], \tag{2.4.17}$$

and $\mathrm{tr}(M_d) = 0$ *and* $\mathrm{tr}(M_d^2) = d$*. Then, measuring the observable* M_d *yields*

$$\mathcal{S}_{AB}^{(2)} = (d+1)^2 \mathcal{R}_{AB}^{(2)}, \qquad \mathcal{S}_{AB}^{(4)} = \frac{(d+1)^2(d^2+1)^2}{9(d-1)^2} \mathcal{R}_{AB}^{(4)}. \tag{2.4.18}$$

Remark 7. The proof of this derivation is given in Sec. 9.2. A similar result can be obtained for even dimensions. However, the solution for y is in this case less aesthetic. For details, see Ref. [1].

2.4.3 Entanglement criterion using fourth moments

At last, let us formulate separability criteria in terms of the second and fourth moments $\mathcal{S}_{AB}^{(r)}$. For that, we first recall the dV criterion [244]: Any two-qudit separable state obeys

$$\|T_\mathrm{s}\|_\mathrm{tr} = \|T_\mathrm{s}'\|_\mathrm{tr} = \sum_{i=1}^{d^2-1} \tau_i \leq d - 1, \tag{2.4.19}$$

where T_s' is defined in Eq. (2.4.11). From our results, it also follows that the dV criterion can be evaluated via randomized measurements for all dimensions.

First, it turns out that $\mathcal{S}_{AB}^{(2)}$ and $\mathcal{S}_{AB}^{(4)}$ can, for any dimension, be simply expressed as polynomial functions of the submatrix T_s. Second, the moments $\mathcal{S}_{AB}^{(r)}$ are by definition invariant under orthogonal transformations of the matrix T_s. Also, the dV criterion is also invariant under the named orthogonal transformations. Third, for a fixed value of the second moment $\mathcal{S}_{AB}^{(2)}$, we can maximize and minimize the fourth moment $\mathcal{S}_{AB}^{(4)}$ under the constraint $\|T_\mathrm{s}\|_\mathrm{tr} \leq d - 1$. This task is greatly simplified by orthogonal invariance; in fact, we can assume T_s to be diagonal. This leads to simple, piece-wise algebraic separability conditions for arbitrary dimensions d. Let us make a summary in the following:

Result 11. *The set of admissible values* $(\mathcal{S}_{AB}^{(2)}, \mathcal{S}_{AB}^{(4)})$ *for separable states can be charac-*

terized by maximizing and minimizing the fourth moment as follows:

$$\max_{\tau_i} / \min_{\tau_i} \qquad \mathcal{S}_{AB}^{(4)} = W\left[2\sum_{i=1}^{d^2-1}\tau_i^4 + \frac{1}{V^2}\left(\mathcal{S}_{AB}^{(2)}\right)^2\right], \tag{2.4.20}$$

$$\text{s.t.} \qquad \mathcal{S}_{AB}^{(2)} = V\sum_{i=1}^{d^2-1}\tau_i^2, \tag{2.4.21}$$

$$\sum_{i=1}^{d^2-1}\tau_i \leq d-1, \tag{2.4.22}$$

$$0 \leq \tau_i \leq d-1, \tag{2.4.23}$$

where τ_i is maximal and equal to $d-1$ for a pure product state, due to the positivity of states. If a state lies outside this set, then it must be entangled.

Remark 8. The results for $d = 3$ are shown in Fig. 2.5. The outlined procedure gives an area that contains all values of $\mathcal{S}_{AB}^{(2)}$ and $\mathcal{S}_{AB}^{(4)}$ for separable states. Most importantly, various bound entangled states can be detected [265–268], discussed in Sec. 1.2. Also, the $4 \otimes 4$ bound entangled Piani state from the Ref. [271] can be detected, details are given in Ref. [1].

Remark 9. Let us discuss which states are good candidates for violating our criterion. It is known that in $d \otimes d$-dimensional systems, if the states have maximally mixed subsystems, then the dV criterion is equivalent to the CCNR criterion. If not, the dV criterion is weaker than the CCNR criterion (see Ref. [60]). On the other hand, if an entangled state is very close to a state with maximally mixed subsystems and largely violates the CCNR criterion, then we may detect the entangled state based on the dV criterion. For instance, the so-called cross-hatch 3×3 grid state, one of the bound entangled states detected by our methods, does not have maximally mixed subsystems. Nevertheless, its reduced states are close to maximally mixed, $\varrho_A = \varrho_B = \text{diag}(0.375, 0.25, 0.375)$, and moreover, it violates the CCNR criterion by a large amount.

2.5 Experimental demonstration of theoretical results

In Ref. [8], theoretical results presented in this Chapter have been experimentally demonstrated. Here we explain the experimental implementation of GHZ-W mixed states based on Ref. [8]. For more details and the detection of bound entangled checkerboard states, see Ref. [8]. Concerning details of experimental settings, also see Refs. [427, 428].

In Fig. 2.6, the experimental setup for GHZ-W mixed states is illustrated. The setup is mainly divided into two stages: state preparation and randomized measurements. Let us begin by explaining the state preparation stage:

- State preparation: First, the entangled photon source (EPS) generates two-qubit polarization-entangled photon pairs. Examples are $|\psi_g\rangle$ or $|\psi_w\rangle$,

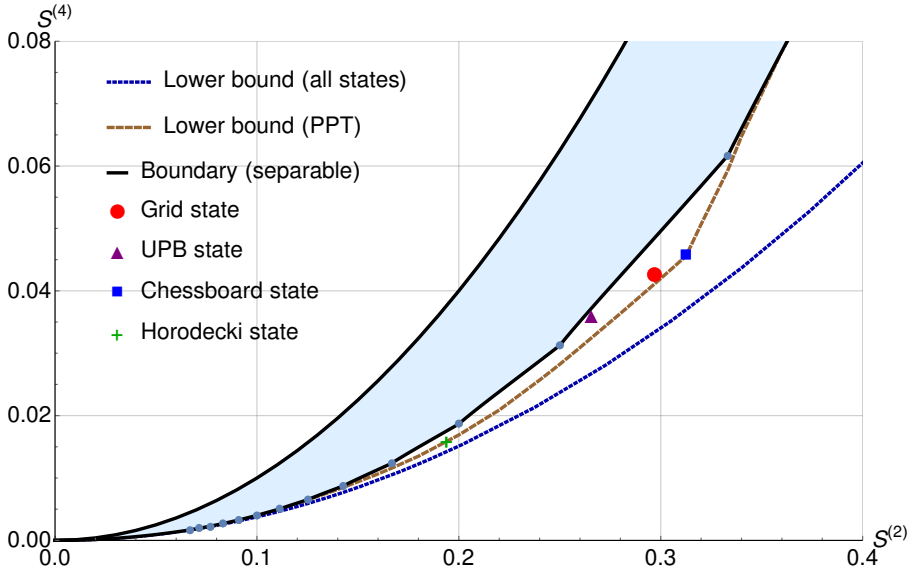

Figure 2.5: Entanglement criterion based on second and fourth moments of randomized measurements for $3 \otimes 3$ systems. Separable states are contained in the light-blue area, according to Result 11. Several bound entangled states (denoted by colored symbols) are outside, meaning that their entanglement can be detected with the methods developed in this Chapter. For comparison, we also indicate a lower bound on the fourth moment for PPT states, obtained by numerical optimization, as well as a bound for general states. Also, the lower bound for general states can be obtained by imposing the constraint $\sum_{i=1}^{d^2-1} \tau_i \leq d^2 - 1$, and the isotropic state ϱ_{iso} in Eq. (2.3.21) satisfies the bound, which proves it is optimal. This figure is taken from Ref. [1].

given by

$$|\psi_g\rangle = \alpha\,|0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle\,, \tag{2.5.1}$$
$$|\psi_w\rangle = \alpha\,|0\rangle \otimes |1\rangle + \beta\,|1\rangle \otimes |0\rangle\,. \tag{2.5.2}$$

Here $|0\rangle$ (or $|1\rangle$) denotes the horizontal (or vertical) polarization of the photon, that is, $|0\rangle = |H\rangle$ (or $|1\rangle = |V\rangle$). The coefficients α and β can be controlled by preparation operation in the EPS.

- Details about the EPS: Here let us explain the inside of the EPS (this is not shown in Fig. 2.6). There are three steps to create the two-qubit entangled state, e.g., $|\psi_g\rangle$ or $|\psi_w\rangle$:

  1. A pump beam state, $|\psi_{\text{beam}}\rangle$, passes through a polarizing beamsplitter (PBS). This projects the pump state $|\psi_{\text{beam}}\rangle$ onto the basis $|0\rangle$ as an initialization.
  2. The new state $|0\rangle$ is rotated by a Half-Wave Plate (HWP) and then becomes $|\psi_s\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. That is, the HWP can act as a Hadamard gate.

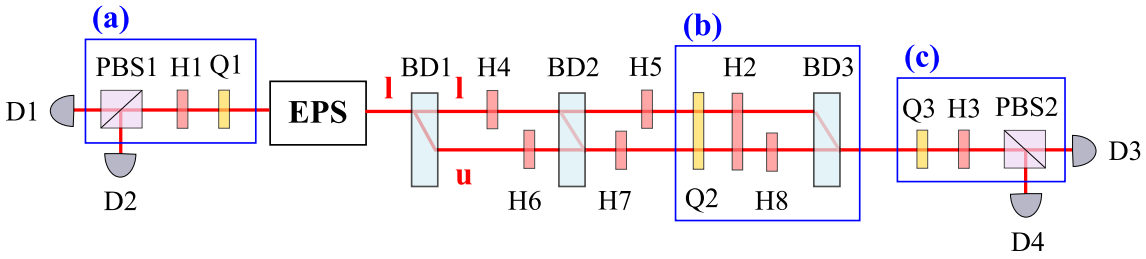

Figure 2.6: Experimental setup for GHZ-W mixed states. This figure is taken from Ref. [8].

3. The rotated state $|\psi_s\rangle$ is directed to the so-called spontaneous parametric down-conversion process through crystals. This is a nonlinear optical process, in which there is a reasonable probability that a higher-energy pump photon will split into a pair of lower-energy photons while conserving energy and momentum. In this experiment, the beam state pumps two crossed-axis type-I β-Barium Borate (BBO) crystals, which create the states $|\psi_g\rangle$ or $|\psi_w\rangle$.

- New registration: After the EPS, a new system $|l\rangle$ is additionally registered and the global state becomes

$$|\psi_g\rangle \to |\psi_{g,l}\rangle = |\psi_g\rangle \otimes |l\rangle\,, \tag{2.5.3}$$
$$|\psi_w\rangle \to |\psi_{w,l}\rangle = |\psi_w\rangle \otimes |l\rangle\,. \tag{2.5.4}$$

  This process is not explicitly illustrated in Fig. 2.6.

- Beam Displacer: After the registration, the state is directed to the Beam Displacer (BD) BD1. This is a unitary process U_{BD1} such that $U_{\text{BD1}}\,|1\rangle \otimes |l\rangle \to |1\rangle \otimes |l\rangle$ and $U_{\text{BD1}}\,|0\rangle \otimes |l\rangle \to |0\rangle \otimes |u\rangle$, where the vertically polarized part passes directly into path l, while the horizontal part passes through while being shifted into path u. This means that the BD1 can act as a CNOT gate. By taking $|l\rangle = |1\rangle$ and $|u\rangle = |0\rangle$ and controlling the four HWPs (H4, H5, H6, H7) and the BD2, each of the three-qubit states becomes

$$|\psi_{g,l}\rangle \to |\text{GHZ}\rangle\,, \tag{2.5.5}$$
$$|\psi_{w,l}\rangle \to |\text{W}\rangle\,. \tag{2.5.6}$$

- Mixing: The GHZ-W mixed state, $\varrho(g) = g\,|\text{GHZ}\rangle\langle\text{GHZ}| + (1-g)\,|\text{W}\rangle\langle\text{W}|$, in Eq.(2.2.36) can be generated by randomly switching the setup settings to produce both states with probability g.

Next, let us explain the stage of randomized measurements. In the measurement stage, the combination of a Quarter-Wave Plate (QWP), an HWP, and a Polarization Beam Splitter (PBS) enables the polarization state measurement on an arbitrary basis:

- In each of the boxed parts (a), (b), and (c) in Fig. 2.6, the created state is then directed to the measurement stages. The measurement stages perform projective measurements on polarization and path degrees of freedom of the down-converted photons. The QWPs (Q1, Q2, Q3) and HWPs (H1, H2, H3) are mounted on Motorized Rotation Mounts (Newport, CONEX-PR50CC). For each randomly drawn local measurement setup, a classical computer inputs the corresponding QWP and HWP settings, and the waveplate is automatically rotated to the target angle for measurement. Note that the BD3 together with Q2 and H2 can act as making projective measurements.

- In this experiment, for each prepared GHZ-W mixed state, $\varrho(g)$, 4000 randomized measurements are taken, with about 5300 copies of the state detected in each measurement.

The quality of the state $\varrho(g)$ can be quantified by the fidelities of the experimentally prepared state and the ideal state. For the GHZ state and W state, their fidelities are 0.9919 and 0.9890, leading to 0.9836 for all fidelities of the GHZ-W mixed states.

The entanglement of the state $\varrho(g)$ can be detected in the second moments from randomized measurements (sector lengths). In fact, the genuinely multipartite entanglement of $\varrho(g)$ can be verified since the previously known $S_3 \leq 3$ is violated. Also, the criterion in Result 3 can be applied to detect the state of $g \leq 0.24$ with no three-tangle and $g \geq 0.67$ with no squared concurrence. For more details, see Ref. [8].

2.6 Discussions

This Chapter developed methods for characterizing quantum correlations using randomized measurements. On the one hand, our approach led to optimal criteria for different forms of entanglement using the second moments of the randomized measurements. On the other hand, we have shown that using fourth moments of randomized measurement detection of bound entanglement as a weak form of entanglement is possible. This opens a new perspective for developing the approach further, as all previous entanglement criteria were only suited for highly entangled states.

There are several directions for further research. First, it would be desirable to prove a conjecture that Result 3 is also true for biseparable states for all bipartitions. In addition, it would be interesting to advance systematic approaches to finding entanglement criteria using non-trivial linear combinations of sector lengths. Moreover, it would be important to formulate entanglement criteria in high-dimensional multipartite systems by utilizing higher-order moments. Finally, we note that our results were extended in terms of the detection of Schmidt number [258, 429] and the systematic discussions about Result 8 in [258].

Chapter 3

Multi-qubit entanglement and statistical significance

This Chapter develops the scheme of randomized measurements in two directions. First, this Chapter presents hierarchical criteria for multiqubit entanglement with second moments. Next, this Chapter analyzes the statistical significance of characterizing quantum correlations using large deviation bounds. This Chapter is based on Ref. [2].

3.1 Introduction

Let us begin by recalling the moments in Eq. (1.4.2) from the randomized measurements discussed in Sec. 1.4. Consider a quantum state ϱ composed of N qubits and a product observable $\mathcal{M} = \sigma_z \otimes \cdots \otimes \sigma_z$. The correlation function is given by

$$E(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N) = \langle \sigma_{\boldsymbol{u}_1} \otimes \ldots \otimes \sigma_{\boldsymbol{u}_N} \rangle_\varrho, \tag{3.1.1}$$

and the corresponding moments are expressed as

$$\mathcal{R}^{(t)} = \frac{1}{(4\pi)^N} \int d\boldsymbol{u}_1 \ldots \int d\boldsymbol{u}_N \left[E(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N) \right]^t. \tag{3.1.2}$$

This Chapter focuses on the analysis of quantum states and the verification of entanglement using the above moments.

In the context of verifying multipartite quantum systems, different approaches have been discussed. On one hand, there are efficient protocols that require fewer measurement resources when the experiment aims to determine specific states, such as entanglement witnessing [17], self-testing [430], or direct fidelity estimation [79, 431]. On the other hand, approaches that rely on few or no assumptions about the underlying quantum state are often resource-intensive and do not scale well with increasing system sizes, such as quantum state tomography [432, 433].

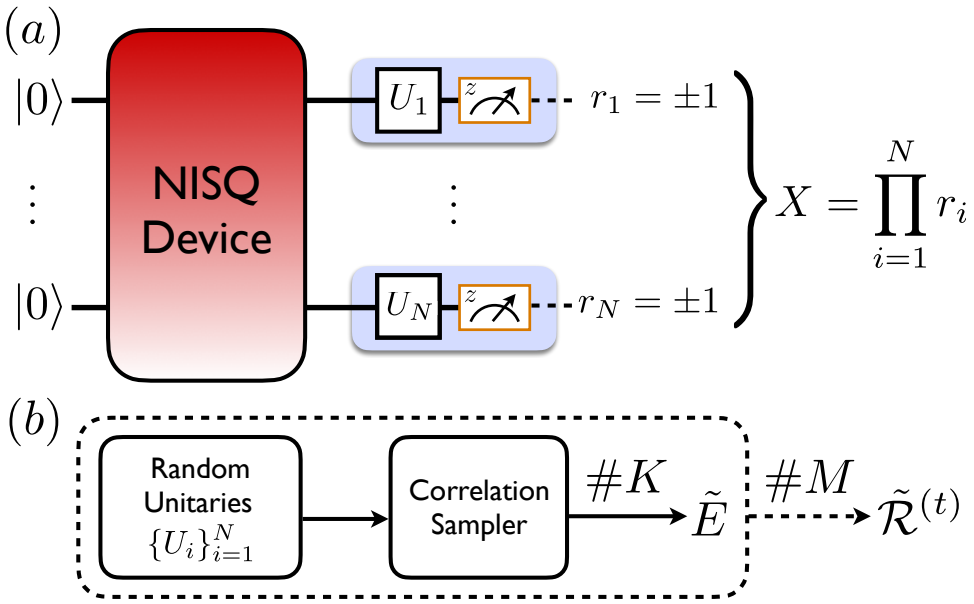

Figure 3.1: Characterization of a Noisy Intermediate-Scale Quantum (NISQ) device using locally randomized measurements. (a) Measurement of N qubits in random local bases defined through the set of local unitary transformations $\{U_i\}_{i=1}^N$ resulting in a correlation sample X. (b) Repetition of the measurement protocol presented in (a) for M sets of randomly sampled measurement bases and K individual projective measurements per fixed measurement bases yields estimates of the moments (3.1.2). For details, see Sec. 3.3.1. This figure is taken from Ref. [2].

Additionally, there are intermediate strategies that focus on specific statistical properties rather than aiming for a complete mathematical description of the system. These strategies significantly reduce the required measurement resources and do not assume any prior information about the state of the system [434–438]. In the scheme of randomized measurements discussed in Sec. 1.4, scaling properties have been derived for the case of bipartite entanglement [105, 439] concerning the resources required for statistically significant tests.

This Chapter presents detailed statistical methods of randomized measurements to certify multiparticle entanglement structures in systems consisting of many qubits. First, we derive criteria based on the second moments for different forms of multiparticle entanglement, enabling us to infer the entanglement depth. Second, we present rigorous approaches for analyzing the underlying statistical errors, based on large deviation bounds. As we will demonstrate, our results are directly applicable in current experiments using Rydberg atom arrays or superconducting qubits [440–442].

3.2 Detection of multiqubit entanglement

3.2.1 Bounds of the second and fourth moments

In general, we can evaluate the integral in Eq. (3.1.2) using spherical designs, as discussed in Sec. 1.5 (also see Ref. [384] and Fig. 2 of Ref. [392]). These spherical designs lead to the expression of the second moment as

$$\mathcal{R}^{(2)} = \frac{1}{3^N} \sum_{i_1,\ldots,i_N=x,y,z} E(\boldsymbol{e}_{i_1},\ldots,\boldsymbol{e}_{i_N})^2, \tag{3.2.1}$$

by summing over the three Pauli observables only. Higher-order moments require higher-order designs. For instance, the fourth moment becomes

$$\mathcal{R}^{(4)} = \frac{1}{6^N} \sum_{i_1,\ldots,i_N=1}^{6} E(\boldsymbol{v}_{i_1},\ldots,\boldsymbol{v}_{i_N})^4, \tag{3.2.2}$$

where $\{\boldsymbol{v}_i\}$ denotes the icosahedron 5-design discussed in Ref. [392]. In the following, we will discuss several bounds of the moments.

First, determining tight upper bounds for the moments is difficult. However, the maximum value of the second moment $\mathcal{R}^{(2)}$ has been found. In Refs. [350, 353], it was shown that the maximum value of the second moment is reached for the N-qubit GHZ state $|\mathrm{GHZ}_N\rangle = (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$:

$$\mathcal{R}^{(2)}_{|\mathrm{GHZ}_N\rangle} = \frac{1}{3^N} \times \begin{cases} 2^{N-1}, & N \text{ odd}, \\ 2^{N-1}+1, & N \text{ even}. \end{cases} \tag{3.2.3}$$

This was derived through the relation of the second moment to the full-body sector lengths, as mentioned in Sec. 1.4.

However, the upper bounds of higher moments are unfortunately not known in general. Numerical evidence from Ref. [443] suggests that the upper bound of the fourth moment $\mathcal{R}^{(4)}$ is also reached for the GHZ state with $N \neq 4$:

$$\mathcal{R}^{(4)}_{|\mathrm{GHZ}_N\rangle} = \frac{1}{15^N} \times \begin{cases} 3\times 8^{N-1}, & N \text{ odd}, \\ 3\times 8^{N-1} + 3^N + 3\times 2^N, & N \text{ even}. \end{cases} \tag{3.2.4}$$

Note that in the exceptional case $N = 4$, the bi-separable state $|\mathrm{Bell}\rangle \otimes |\mathrm{Bell}\rangle$ reaches a larger value than the GHZ state. For an $(N/2)$-fold product of Bell states $|\mathrm{Bell}\rangle^{\otimes(N/2)}$ with N even, the fourth moment reads

$$\mathcal{R}^{(4)}_{|\mathrm{Bell}\rangle^{\otimes\frac{N}{2}}} = \frac{1}{5^{(N/2)}}. \tag{3.2.5}$$

Also, the product state $|\mathrm{GHZ}_{\frac{N}{2}}\rangle \otimes |\mathrm{GHZ}_{\frac{N}{2}}\rangle$ has a smaller fourth moment than Eq. (3.2.4).

Finally, any N-qubit fully separable state, $\varrho_{\text{sep}} = \sum_\alpha p_\alpha \varrho_\alpha^{(1)} \otimes \ldots \otimes \varrho_\alpha^{(N)}$ (also see Sec 1.2), obeys

$$\mathcal{R}^{(2)} \leq \frac{1}{3^N}, \qquad \mathcal{R}^{(4)} \leq \frac{1}{5^N}, \tag{3.2.6}$$

for details, see [378]. This follows from the convexity of the monomials x^t for even t and the fact that for all single-qubit pure states $\mathcal{R}^{(2)}_{N=1} = 1/3$ and $\mathcal{R}^{(4)}_{N=1} = 1/5$.

3.2.2 Hierarchical entanglement criteria

To proceed, let us recall the notion of a k-separable state as defined in Eq. (1.2.26), see Sec 1.2. A state is k-separable if it can be written as

$$|\psi_{k\text{-sep}}\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_k\rangle \,. \tag{3.2.7}$$

A mixed k-separable state can also be defined as the convex mixture of them. In particular, if a state is not 2-separable (biseparable), it is called genuinely multipartite entangled.

Here we formulate the following:

Result 12. *Any N-qubit biseparable state obeys*

$$\mathcal{R}^{(2)} \leq \frac{1}{3^{N-1}} \times \begin{cases} 2^{N-3}, & N \text{ odd}, \\ 2^{N-3}+1, & N \text{ even}. \end{cases} \tag{3.2.8}$$

Remark 10. The proof is given below. The violation of this criterion allows us to detect genuinely multipartite entanglement.

Proof. Since the second moment is convex, it suffices to consider a pure N-qubit biseparable state:

$$\varrho_{\text{bisep}} = \varrho_{N-k} \otimes \varrho_k, \tag{3.2.9}$$

with $k \in \{1, \ldots, N/2\}$. The maximum of its second moment can be calculated as follows:

$$\begin{aligned} \max_{\varrho_{\text{bisep}}} \mathcal{R}^{(2)}_{\varrho_{\text{bisep}}} &= \max_k \mathcal{R}^{(2)}_{\varrho_{N-k}} \times \max_k \mathcal{R}^{(2)}_{\varrho_k} \\ &= \frac{1}{3^N} \left\{ \begin{matrix} 2^{N-k-1}, & N-k \text{ odd} \\ 2^{N-k-1}+1, & N-k \text{ even} \end{matrix} \right\} \times \left\{ \begin{matrix} 2^{k-1}, & k \text{ odd} \\ 2^{k-1}+1, & k \text{ even} \end{matrix} \right\}, \end{aligned} \tag{3.2.10}$$

where we used that the maximum of an m-qubit second moment is attained for the respective m-qubit GHZ state, see Eq. (3.2.3). Next, we consider the cases of even and odd N:

- Case of even N: We find that

$$\begin{aligned}\max_{\varrho_{\text{bisep}}} \mathcal{R}^{(2)}_{\varrho_{\text{bisep}}} &= \frac{1}{3^N} \max_k \begin{Bmatrix} 2^{N-k-1} \times 2^{k-1}, & k \text{ odd} \\ (2^{N-k-1}+1) \times (2^{k-1}+1), & k \text{ even} \end{Bmatrix} \\ &= \frac{1}{3^N} \max_k \begin{Bmatrix} 2^{N-2}, & k \text{ odd} \\ 2^{N-2} + 2^{N-k-1} + 2^{k-1} + 1, & k \text{ even} \end{Bmatrix} \\ &= \frac{1}{3^N} \left[2^{N-2} + 1 + \max_k \left(2^{N-k-1} + 2^{k-1}\right) \right] \\ &= \frac{2^{N-3}+1}{3^{N-1}}, \end{aligned} \tag{3.2.11}$$

  where we used that the function $f(k) = 2^{N-k-1} + 2^{k-1}$ is positive on the interval $[2, N/2]$ and thus takes its maximum at the boundary, i.e., for $k = 2$ or $k = N-2$.

- Case of odd N: We find that

$$\begin{aligned}\max_{\varrho_{\text{bisep}}} \mathcal{R}^{(2)}_{\varrho_{\text{bisep}}} &= \frac{1}{3^N} \max_k \begin{Bmatrix} (2^{N-k-1}+1) \times 2^{k-1}, & k \text{ odd} \\ 2^{N-k-1} \times (2^{k-1}+1), & k \text{ even} \end{Bmatrix} \\ &= \frac{1}{3^N} \max_k \begin{Bmatrix} 2^{N-2} + 2^{k-1}, & k \text{ odd} \\ 2^{N-2} + 2^{N-k-1}, & k \text{ even} \end{Bmatrix} \qquad (3.2.12) \\ &= \frac{1}{3^N} \left[2^{N-2} + \max_k \begin{Bmatrix} 2^{k-1}, & k \text{ odd} \\ 2^{N-k-1}, & k \text{ even} \end{Bmatrix} \right] \qquad (3.2.13) \\ &= \frac{1}{3^N} \left[2^{N-2} + \max_k \left(2^{N-k-1}\right) \right] = \frac{2^{N-3}}{3^{N-1}}, \qquad (3.2.14) \end{aligned}$$

  where we used that $g(k) = 2^{N-k-1}$ is positive in the interval $[2, N/2]$ and its maximum is reached for $k = 2$.

In summary, we obtained the following bound for all biseparable states ϱ_{bisep}:

$$\mathcal{R}^{(2)} \leq \frac{1}{3^{N-1}} \times \begin{cases} 2^{N-3}, & N \text{ odd}, \\ 2^{N-3}+1, & N \text{ even}, \end{cases} \tag{3.2.15}$$

Comparing the bound (3.2.15) with the maximum value of the second moment (3.2.3), we find:

- For an odd number of qubits, it holds that

$$\frac{2^{N-1}}{3^N} > \frac{2^{N-3}}{3^{N-1}}, \tag{3.2.16}$$

  for all N.

- For an even number of qubits, it holds that

$$\frac{2^{N-1}+1}{3^N} \geq \frac{2^{N-3}+1}{3^{N-1}}, \tag{3.2.17}$$

  for all N, with equality if and only if $N = 4$.

Hence, the inequality in Eq. (3.2.15) allows us to detect N-qubit genuine multipartite entanglement for $N > 4$. Note that the bounds in Eq. (3.2.15) are saturated for the states $|\text{Bell}\rangle \otimes |\text{GHZ}_{(N-2)}\rangle$. □

Now we advance the previous Result and present the following:

Result 13. *Any N-qubit k-separable state obeys*

$$\mathcal{R}^{(2)} \leq \frac{1}{3^{N-k+1}} \times \begin{cases} 2^{N-(2k-1)}, & N \text{ odd}, \\ 2^{N-(2k-1)}+1, & N \text{ even}, \end{cases} \tag{3.2.18}$$

with $k = 2, \ldots, \lfloor (N-1)/2 \rfloor$.

Remark 11. This Result provides a hierarchy of entanglement criteria. If this inequality is violated for fixed k, then the state is at most $(k-1)$-separable. This implies that it has an entanglement depth [174, 177] of at least $\lceil N/(k-1) \rceil$.

Proof. The proof of this Result can be carried out through the method of induction. Since we have proven the case $k = 2$, it remains the induction step, i.e., that the case $k+1$ follows from k. First, let us consider the case of even N. Let us assume that for a k-separable state of $N-m$ qubits denoted as ϱ_{N-m}, the following holds

$$\mathcal{R}^{(2)}_{\varrho_{N-m}} \leq \frac{1}{3^{N-m-k+1}} \times \begin{cases} 2^{N-m-(2k-1)}, & N-m \text{ odd}, \\ 2^{N-m-(2k-1)}+1, & N-m \text{ even}. \end{cases} \tag{3.2.19}$$

Now, we consider the maximum of the second moment of an N-qubit $(k+1)$-separable state

$$\max_{\varrho_{(k+1)\text{-sep}}} \mathcal{R}^{(2)}_{\varrho_{(k+1)\text{-sep}}} = \max_m \mathcal{R}^{(2)}_{\varrho_{k\text{-sep},N-m}} \times \max_m \mathcal{R}^{(2)}_{\varrho_m}, \tag{3.2.20}$$

where $\varrho_{k\text{-sep},x}$ denotes a k-separable state of x qubits. The assumption is reformulated as

$$\mathcal{R}^{(2)}_{\varrho_{k\text{-sep},N-m}} \leq \frac{1}{3^{N-m-k+1}} (2^{N-m-(2k-1)} + \delta_{(N-m),\text{even}}). \tag{3.2.21}$$

Also, according to Eq. (3.2.3), we have

$$\mathcal{R}^{(2)}_{\varrho_m} \leq \frac{1}{3^m} (2^{m-1} + \delta_{m,\text{even}}). \tag{3.2.22}$$

Consequently, Eq. (3.2.20) becomes

$$\max_{\varrho_{(k+1)\text{-sep}}} \mathcal{R}^{(2)}_{\varrho_{(k+1)\text{-sep}}} = \max_m \Big\{ \frac{1}{3^{N-m-k+1}} \times (2^{N-m-(2k-1)} + \delta_{(N-m),\text{even}}) \times \frac{1}{3^m}(2^{m-1} + \delta_{m,\text{even}}) \Big\}. \tag{3.2.23}$$

Since N is now even, this is maximized by the case of even m, which thus leads to

$$\begin{aligned} \max_{\varrho_{(k+1)\text{-sep}}} \mathcal{R}^{(2)}_{\varrho_{(k+1)\text{-sep}}} &= \frac{1}{3^{N-k+1}} \times \max_m \{(2^{N-m-(2k-1)} + 1) \times (2^{m-1} + 1)\} \\ &= \frac{1}{3^{N-k+1}} \times \max_m \{2^{N-2k} + 2^{N-m-(2k-1)} + 2^{m-1} + 1\}. \end{aligned} \tag{3.2.24}$$

It thus remains to maximize Eq. (3.2.24) with respect to m. The m-dependent terms of Eq. (3.2.24) can be written as

$$g(M) = \frac{2^{N+1-2k}}{M} + \frac{M}{2}, \tag{3.2.25}$$

with $M := 2^m$. This is a convex function and thus attains its maximum at the boundary $m = 2$. Hence this leads to

$$\mathcal{R}^{(2)} \leq \frac{2^{N-(2k-1)}}{3^{N-k+1}}, \tag{3.2.26}$$

for even N.

Similarly, one can prove the case with odd N. Note that Eq. (3.2.18) is attained by the pure k-separable states $|\text{Bell}\rangle^{\otimes(k-1)} \otimes |\text{GHZ}_{N-2(k-1)}\rangle$. □

Remark 12. Similarly, the k-separable bounds of the fourth moment $\mathcal{R}^{(4)}$ can be formulated. This can play an important role in the determination of the measurement resources required in order to violate Eq. (3.2.18) with a given confidence. Based on the conjecture that for $N > 4$ the N-qubit GHZ state maximizes the fourth moment $\mathcal{R}^{(4)}$ we can show that

$$\mathcal{R}^{(4)} \leq \frac{1}{5^{k-1}} \mathcal{R}^{(4)}_{|\text{GHZ}_{N-2(k-1)}\rangle}, \tag{3.2.27}$$

using similar methods as in the proof of Eq. (3.2.18). As for the second moment $\mathcal{R}^{(2)}$, Eq. (3.2.27) is saturated for the pure states $|\text{Bell}\rangle^{\otimes(k-1)} \otimes |\text{GHZ}_{N-2(k-1)}\rangle$, with $k = 2, \ldots, \lfloor (N-1)/2 \rfloor$.

3.2.3 Example: noisy GHZ state

Let us test our result by considering the following noisy N-qubit GHZ states:

$$\varrho^{(N)}_{\text{GHZ}}(p) = \frac{p}{2^n}\mathbb{1} + (1-p)\,|\text{GHZ}_N\rangle\langle\text{GHZ}_N|\,. \tag{3.2.28}$$

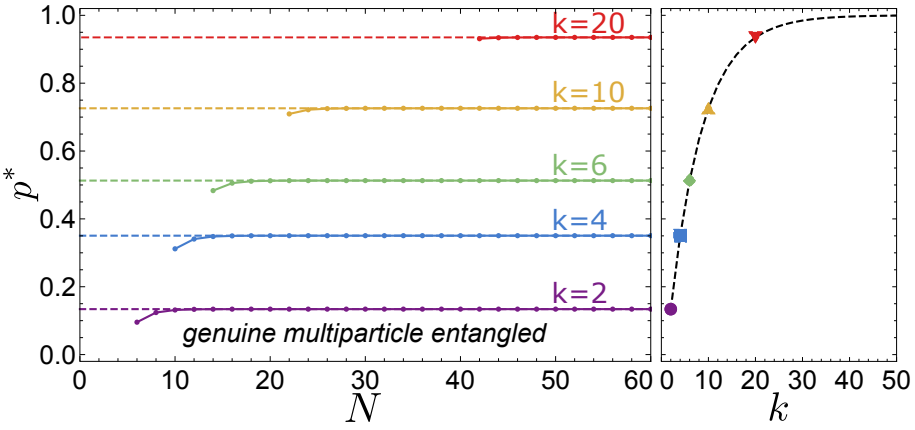

Figure 3.2: Left: Threshold value p^* up to which the noisy GHZ state $\varrho_{\mathrm{GHZ}}^{(N)}(p)$ is detected to be not 2- (violet, bottom), 4- (blue), 6- (green), 10- (yellow), and 20-separable (red, top) as a function of the number of qubits N. Solid lines connecting dots represent values of p^* for even N, and dashed lines correspond to the case of odd N, which also represent the asymptotic values in the limit $N \to \infty$. Right: Plot of the asymptotic values of p^* in the aforementioned limit as a function of the parameter k. The exemplary values of the left plot are highlighted by colored markers, respectively. This figure is taken from Ref. [2].

This yields the second moment of the noisy GHZ state as

$$\mathcal{R}^{(2)}_{\mathrm{GHZ}}(p,N) = (1-p)^2 \mathcal{R}^{(2)}_{|\mathrm{GHZ}_N\rangle}. \tag{3.2.29}$$

For each N, we can now calculate the threshold value of p up to which the criteria (3.2.18) are violated as a function of the parameter k, yielding

$$p^* = 1 - f(N,k)\left(\frac{3}{4}\right)^{\frac{k-1}{2}},\ f(N,k) = \begin{cases} 1, & N \text{ odd}, \\ \sqrt{(4^k + 2^{N+1})/(4 + 2^{N+1})}, & N \text{ even}. \end{cases} \tag{3.2.30}$$

In Fig. 3.2, the behavior of p^* in Eq. (3.2.30) is illustrated. In the case of odd N, the threshold p^* is independent of the number of qubits N and coincides with the asymptotic threshold in the limit $N \to \infty$, where $f(N,k) \to 1$. Hence, the asymptotic thresholds of p^* are strictly smaller than 1.

3.3 Estimation of moments with finite statistics

The purpose of this section is to present methods for estimating the statistical error of moments $\mathcal{R}^{(t)}$ when the number of measurements is limited. In general, when dealing with finite statistics, one uses (unbiased) estimators to estimate the desired quantities. However, these estimators may not match the moments $\mathcal{R}^{(t)}$, unlike for infinite statistics, as mentioned in Sec. 1.1.

Therefore, our goal is to quantify how much the values of our estimator deviate from the actual moment $\mathcal{R}^{(t)}$. In the following, we will derive deviation bounds that provide upper bounds on the probability of the estimator deviating from the mean value by a certain margin.

3.3.1 Unbiased estimators for moments

To be more precise, we aim to provide methods for estimating the statistical error of moments $\mathcal{R}^{(t)}$ when we have a finite sample of M random measurement bases, each undergoing K individual projective measurements. In this context, individual outcomes of a single random measurement on N qubits are represented as $r_1, \ldots, r_N$, with $r_i = \pm 1$. The corresponding correlation sample is denoted as $X = \prod_{i=1}^{N} r_i$, as shown in Fig. 3.1(a).

Then one can write

$$E \equiv E(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N) = P_{\text{even}} - P_{\text{odd}}, \tag{3.3.1}$$

where P_{even} is the probability for obtaining the result $X = +1$, which corresponds to an even number of individual measurement outcomes r_i resulting in -1. Since $P_{\text{even}} + P_{\text{odd}} = 1$, we have

$$E = 2P - 1, \qquad P \equiv P_{\text{even}}. \tag{3.3.2}$$

The probability P can be estimated by an unbiased estimator:

$$\tilde{P}_1 = \frac{\tilde{Y}}{K}. \tag{3.3.3}$$

Here, $\tilde{Y}$ is a random variable distributed following the binomial distribution with probability P and K trials. We find that

$$\mathbb{E}_{\text{bi}}(\tilde{P}_1) = P, \tag{3.3.4}$$

where $\mathbb{E}_{\text{bi}}(\ldots)$ represents the average with respect to the binomial distribution with $\mathbb{E}_{\text{bi}}(\tilde{Y}) = KP$. It is worth mentioning that similar methods have been employed in the context of globally randomized measurement protocols, as discussed in Ref. [439].

Based on that, we summarize our formulation as follows:

Result 14. *The unbiased estimators for the moments $\mathcal{R}^{(t)}$ in Eq. (3.1.2) are given by*

$$\tilde{\mathcal{R}}^{(t)} = \frac{1}{M} \sum_{i=1}^{M} [\tilde{E}_t]_i, \qquad \mathbb{E}_U \mathbb{E}_{bi} \left[\tilde{\mathcal{R}}^{(t)} \right] = \mathcal{R}^{(t)}, \tag{3.3.5}$$

where the subscript i in $[\tilde{E}_t]_i$ refers to estimations of $\tilde{E}_t$ for different randomly sampled local bases, making the $[\tilde{E}_t]_i$ random variables and $\mathbb{E}_U[\ldots]$ represents the average over local random unitaries. Here $\tilde{E}_t$ are the unbiased estimators of E^t given by

$$\tilde{E}_t = (-1)^t \sum_{k=0}^{t} (-2)^k \binom{t}{k} \tilde{P}_k, \qquad \mathbb{E}_{bi}[\tilde{E}_t] = E^t, \tag{3.3.6}$$

where $\tilde{P}_k$ is the estimator for P^k:

$$\tilde{P}_k = \tilde{P}_{k-1} \times \frac{K\tilde{P}_1 - (k-1)}{K-(k-1)} = \frac{\tilde{P}_1(K\tilde{P}_1-1)(K\tilde{P}_1-2)\dots(K\tilde{P}_1-(k-1))}{(K-1)(K-2)\dots(K-(k-1))}. \tag{3.3.7}$$

Proof. Let us begin by defining $\tilde{P}_k$ using the ansatz $\tilde{P}_k = \sum_{r=0}^{k} \alpha_r (\tilde{Y}/K)^r$ and ensuring that the relation $\mathbb{E}(\tilde{P}_k) = P^k$ holds. This way, we can construct unbiased estimators for arbitrary powers of P using only the properties of the binomial distribution. For example, we find:

$$\tilde{P}_2 = \frac{\tilde{P}_1(K\tilde{P}_1-1)}{K-1} = \tilde{P}_1 \times \frac{K\tilde{P}_1-1}{K-1}, \tag{3.3.8}$$

$$\tilde{P}_3 = \frac{\tilde{P}_1(K\tilde{P}_1-1)(K\tilde{P}_1-2)}{(K-1)(K-2)} = \tilde{P}_2 \times \frac{K\tilde{P}_1-2}{K-2}, \tag{3.3.9}$$

$$\tilde{P}_4 = \frac{\tilde{P}_1(K\tilde{P}_1-1)(K\tilde{P}_1-2)(K\tilde{P}_1-3)}{(K-1)(K-2)(K-3)} = \tilde{P}_3 \times \frac{K\tilde{P}_1-3}{K-3}. \tag{3.3.10}$$

which can be recursively used to define the estimator for the t-th moment in Eq. (3.3.7). This can be verified as the unbiased estimator of P^k by considering the factorial moment of the binomial distribution, which reads

$$\mathbb{E}_{\text{bi}}[Y(Y-1)\dots(Y-(k-1))] = \frac{K!P^t}{(k-t)!}, \tag{3.3.11}$$

for details, see [444]. □

3.3.2 General considerations

Now, our goal is to determine the statistical error of estimating $\tilde{\mathcal{R}}^{(t)}$ as a function of the number of qubits N. Specifically, we want lower bounds on the total number of required measurement samples $M_{\text{tot}} = M \times K$ to estimate $\mathcal{R}^{(t)}$ with precision δ and confidence γ, ensuring that

$$\text{Prob}(|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \leq \delta) \geq \gamma, \tag{3.3.12}$$

for $M_{\text{tot}} \geq M(\gamma, t)$.

To achieve this, we can utilize concentration inequalities that provide deviation bounds on the probability $1 - \text{Prob}(|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \leq \delta)$, that is,

$$\text{Prob}(|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \geq \delta) \leq \alpha. \tag{3.3.13}$$

This represents the probability of the estimator deviating from the mean value by a certain margin and $\alpha = 1 - \gamma$ is the statistical significance level, see Sec. 1.1.

In the following subsection 3.3.3, we will treat the entire experiment as a single random variable, that is, $[\tilde{E}_t]_i$ cannot be assumed to be i.i.d. random variables. Then we can find deviation bounds in Eq. (3.3.13) based on the variance of the entire random variable such as the Chebyshev-Cantelli inequality.

Remark 13. There are several ways of deriving deviation bounds: (i) One can consider each unitary as a distinct external parameter, resulting in M repetitions of a random variable with independent, but differently distributed, outcomes due to the different unitary U. For this scenario, we can employ tools like the Bernstein inequality to obtain deviation bounds without additional assumptions. (ii) One can regard the M different terms as independent and identically distributed variables. In each case, we draw a random unitary according to the Haar measure and determine the correlation based on the rules of quantum mechanics. To derive estimation bounds in this scenario, we can use techniques involving Chernoff bounds in a manner similar to the Hoeffding bound. This method typically provides the best bounds, but it relies again on certain assumptions about the maximal values of $\mathcal{R}^{(4)}$. Each method has its advantages and disadvantages, so the choice of which one to use depends on the specifics of the experiment and its data. For more details, see Ref. [2].

3.3.3 Estimating the deviation of the second moment

To proceed, we use the two-sided Chebyshev-Cantelli inequality for the random variable $\tilde{\mathcal{R}}^{(t)}$:

$$\text{Prob}[|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \geq \delta] \leq \frac{2\text{Var}\left(\tilde{\mathcal{R}}^{(t)}\right)}{\text{Var}\left(\tilde{\mathcal{R}}^{(t)}\right) + \delta^2}, \tag{3.3.14}$$

where $\text{Var}(\tilde{\mathcal{R}}^{(t)})$ is the variance of the estimator (3.3.5), and its evaluation involves properties of the binomial distribution. This requires that the confidence $1 - \text{Prob}[|\tilde{\mathcal{R}}^{(t)} - \mathcal{R}^{(t)}| \geq \delta]$ of this estimation is at least γ. For the case of the second moment $\mathcal{R}^{(2)}$ with $t = 2$, we present our results in the following:

Result 15. *The total number of measurements $M_{tot} = M \times K$ required to estimate the second moment $\mathcal{R}^{(2)}$ in a worst-case scenario, considering a fixed relative error and confidence, is illustrated in Fig. 3.3, where $M = M(K)$ is a function of K.*

Proof. We begin by considering the Chebyshev-Cantelli inequality, which provides a minimal two-sided error bar (δ_{err}) of $\tilde{\mathcal{R}}^{(2)}$, ensuring the confidence γ:

$$\delta_{\text{err}} \equiv \sqrt{\frac{1+\gamma}{1-\gamma}\text{Var}(\tilde{\mathcal{R}}^{(t)})}, \qquad \text{Var}\left(\tilde{\mathcal{R}}^{(t)}\right) = \frac{1}{M^2}\sum_{i=1}^{M}\text{Var}\left([\tilde{E}_t]_i\right), \tag{3.3.15}$$

where we used Eq. (3.3.5). Now, to evaluate the variance, we have:

$$\text{Var}\left([\tilde{E}_t]_i\right) = \mathbb{E}_U\mathbb{E}_{\text{bi}}\left[\tilde{E}_t^2\right] - \left(\mathbb{E}_U\left[E^t\right]\right)^2 = \mathbb{E}_U\mathbb{E}_{\text{bi}}\left[\tilde{E}_t^2\right] - \left(\mathcal{R}^{(t)}\right)^2. \tag{3.3.16}$$

Here, $\mathbb{E}_U\mathbb{E}_{\text{bi}}\left[\tilde{E}_t^2\right]$ generally depends on the moments $\mathcal{R}^{(t)}$.

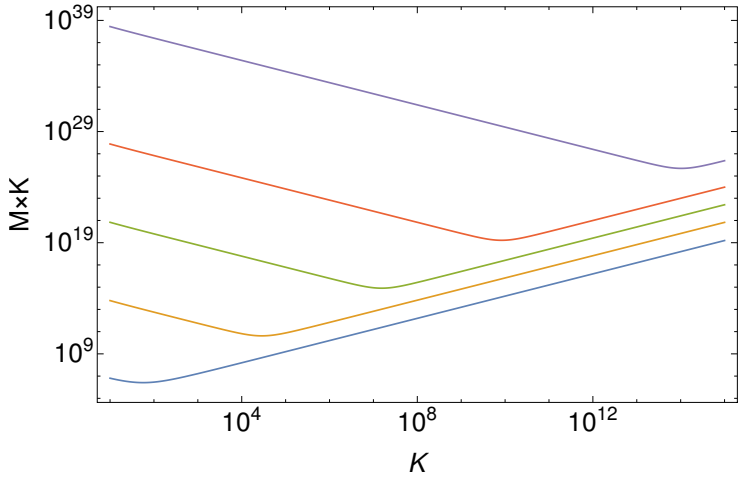

Figure 3.3: Total number of measurements $M_{\text{tot}} = M \times K$ as a function of K for $N = 10$, 30, 50, 70 and 100 qubits (from bottom to top) in order to estimate the second moment with a relative error of 10% and with confidence 90%. Each of the minimal points (valleys) indicates the position of the optimal value $M_{\text{tot}}^{(\text{opt})}$. This figure is a modified version of a figure from Ref. [2].

For the specific case of the second moment $\mathcal{R}^{(2)}$, we find:

$$\text{Var}\left([\tilde{E}_2]_i\right) = A(K)\mathcal{R}^{(4)} + B(K)\mathcal{R}^{(2)} + C(K) - \left(\mathcal{R}^{(2)}\right)^2, \tag{3.3.17}$$

with

$$A(K) = \frac{K-5}{K-1} + \frac{6}{(K-1)K},\ B(K) = \frac{4}{K-1} - \frac{8}{(K-1)K},\ C(K) = \frac{2}{(K-1)K}. \tag{3.3.18}$$

Thus, the variance of $\tilde{\mathcal{R}}^{(2)}$ can be expressed as:

$$\text{Var}(\tilde{\mathcal{R}}^{(2)}) = \frac{1}{M}\left[A(K)\mathcal{R}^{(4)} + B(K)\mathcal{R}^{(2)} + C(K) - \left(\mathcal{R}^{(2)}\right)^2\right]. \tag{3.3.19}$$

To obtain an upper bound on $\text{Var}(\tilde{\mathcal{R}}^{(2)})$, we can omit the last term $(\mathcal{R}^{(2)})^2$ in Eq. (3.3.19) and use Eqs. (3.2.3) and (3.2.4):

$$\text{Var}(\tilde{\mathcal{R}}^{(2)}) \leq \frac{1}{M}\left[A(K)\mathcal{R}^{(4)}_{|\text{GHZ}_N\rangle} + B(K)\mathcal{R}^{(2)}_{|\text{GHZ}_N\rangle} + C(K)\right]. \tag{3.3.20}$$

As a result, the worst-case error in the estimator $\tilde{\mathcal{R}}^{(2)}$ is given by:

$$\delta_{\text{err}} \leq \sqrt{\frac{1+\gamma}{1-\gamma}\frac{1}{M}\left[A(K)\mathcal{R}^{(4)}_{|\text{GHZ}_N\rangle} + B(K)\mathcal{R}^{(2)}_{|\text{GHZ}_N\rangle} + C(K)\right]}. \tag{3.3.21}$$

This upper bound on the error is independent of the state and depends on the number of qubits, denoted by N. Using Eq. (3.3.21), we can derive the necessary

numbers of measurements M and K to achieve a given error δ_{err} and confidence level γ. As the interval size $[0, \mathcal{R}^{(2)}_{|\text{GHZ}_N\rangle}]$ relies on the number of qubits N, we consider a minimum relative error, i.e., a fraction of the entire interval length. By minimizing $M(K) \times K$ with respect to K and keeping the number of parties N fixed, we can determine the optimal number of projective measurements per random measurement setting. □

3.4 Finite statistics entanglement characterization

Here our aim is to determine the measurement resources required for the detection of multiparticle entanglement with a confidence level γ. To enhance our procedure, we utilize the upper bound on the variance in Eq. (3.3.19) specifically tailored for k-separable states, rather than using the general overall upper bound presented in Fig. 3.3. Now, we present the following result:

Result 16. *The optimal total number of measurements $M^{(opt)}_{tot}$ required to certify the violation of k-separability for different values of the noise parameter p and the number of qubits N in the state $\varrho^{(N)}_{GHZ}(p)$ is illustrated in Fig. 3.4.*

Proof. For the remainder of this discussion, we will utilize the method based on the one-sided Chebyshev-Cantelli inequality, similarly with in Sec. 3.3.3.

$$\text{Prob}[\tilde{\mathcal{R}}^{(2)} - \mathcal{R}^{(2)} \geq \delta] \leq \frac{\text{Var}\left(\tilde{\mathcal{R}}^{(2)}\right)}{\text{Var}\left(\tilde{\mathcal{R}}^{(2)}\right) + \delta^2}. \tag{3.4.1}$$

The one-sided version is sufficient for the scenario of entanglement detection since we only need to demonstrate that $\mathcal{R}^{(2)}$ exceeds the bounds of the criteria (3.2.18). To rule out the hypothesis that the state belongs to a specific class of separable states, we invoke the respective upper bounds on the second and fourth moments to obtain an upper bound on the variance $\text{Var}\left(\tilde{\mathcal{R}}^{(2)}\right)$. For detecting non-$k$-separability, we use Eqs. (3.2.18) and (3.2.27) to derive an upper bound on the variance in Eq. (3.4.1). Additionally, we set the confidence $\gamma = 90\%$ and the accuracy as follows:

$$\delta = \mathcal{R}^{(2)}_{\text{GHZ}}(p, N) - \max \mathcal{R}^{(2)}_{\varrho_{k\text{-sep}}} = (1-p)^2 \mathcal{R}^{(2)}_{|\text{GHZ}_N\rangle} - \max \mathcal{R}^{(2)}_{\varrho_{k\text{-sep}}}, \tag{3.4.2}$$

where $\max \mathcal{R}^{(2)}_{\varrho_{k\text{-sep}}}$ denotes the RHS of Eq. (3.2.18), ensuring that the state $\varrho^{(N)}_{\text{GHZ}}(p)$ violates the respective k-separability bound. □

3.5 Discussions

This Chapter explored statistical methods for characterizing multiparticle quantum systems using randomized measurements. First, we introduced novel criteria to detect various types of multiparticle correlations in N-qubit systems,

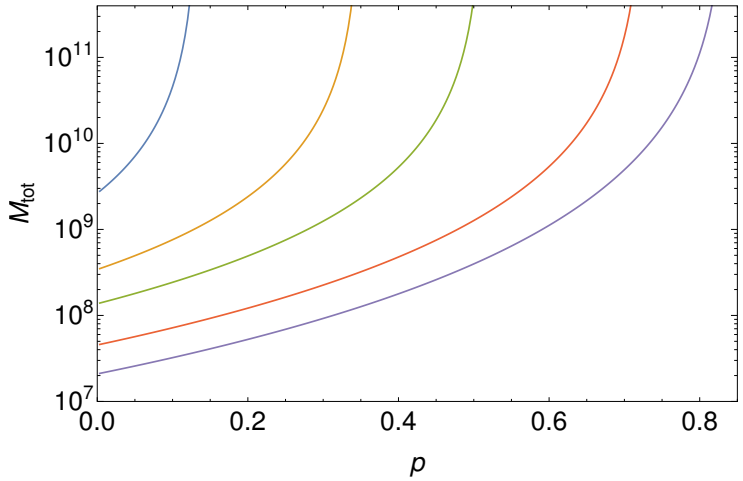

Figure 3.4: Measurement budget $M_{\text{tot}}^{(\text{opt})}$ obtained from Chebyshev-Cantelli inequality required to certify the violation of the k-separability criteria (3.2.18) of $\varrho_{\text{GHZ}}^{(N)}(p)$, with $k = 2$ (blue, left), 4 (yellow), 6 (green), 10 (red) and 14 (purple, right), for $N = 30$ and confidence $\gamma = 90\%$. This figure is a modified version of a figure from Ref. [2].

including genuine multiparticle entanglement, utilizing only the lowest non-vanishing moment. Moreover, we conducted a detailed analysis of the associated statistical errors, enabling us to estimate the statistical significance of our methods. Finally, we applied the developed framework to certify diverse forms of multiparticle entanglement based on finite statistics.

There are several directions for further research. First, Results 12, 13 correspond to the entanglement criteria described by the full-body sector length S_N. It would be interesting to consider whether one can find similar bounds using the marginal sector lengths such as S_{N-1} or S_{N-2}. Second, it would be important to analytically prove the conjecture of whether the upper bounds of higher moments $\mathcal{R}^{(t)}$ with $t > 2$ can be achieved by the GHZ states, except for special cases, such as Eq. (3.2.4). Moreover, in Refs. [445, 446], similar approaches have been discussed in terms of the quantification of multipartite entanglement, also see Refs. [447–449].

Chapter 4

Complete characterization of two-qubit entanglement

This Chapter deepens the understanding of randomized measurement schemes based on non-product observables. This Chapter mainly deals with two-qubit systems and provides the complete characterization of quantum correlations based on non-product observables. This Chapter is based on Ref. [6].

4.1 Introduction

Let us begin by recalling the moments in Eq. (1.4.2) in the scheme of randomized measurements in Sec. 1.4. In the case of a two-qubit state ϱ_{AB} and a general observable $\mathcal{M}$, the moment is given by

$$\mathcal{R}^{(t)}_{\mathcal{M}}(\varrho_{AB}) = \int dU_A \int dU_B \left[\mathrm{tr}(\varrho_{AB} U_A^\dagger \otimes U_B^\dagger \mathcal{M} U_A \otimes U_B)\right]^t. \tag{4.1.1}$$

In the previous Chapters, we have considered the product observable such as $\mathcal{M} = \sigma_z \otimes \sigma_z$. This Chapter addresses the question of whether the choice of non-product observables is useful and advantageous for extracting additional information about ϱ_{AB}.

In this Chapter, we develop a general framework linking the moments of randomized measurements and the set of local unitary invariants. First, we show that the Makhlin invariants in Eq. (1.4) can be accessed by the randomized measurement scheme. They are known to form the complete set of 18 polynomial invariants. Next, we discuss the applications of Makhlin invariants in quantum information processing tasks. In fact, we provide the perfect detection of two-qubit entanglement, the certification of Bell nonlocality, and the usefulness of the prepared states for teleportation schemes.

4.2 Makhlin invariants

Let us begin by recalling the Bloch decomposition of a two-qubit state:

$$\varrho_{AB} = \frac{1}{4}\left(\mathbb{1}^{\otimes 2} + \sum_{i=1}^{3}\alpha_i\lambda_i\otimes\mathbb{1} + \sum_{i=1}^{3}\beta_i\mathbb{1}\otimes\lambda_i + \sum_{i,j=1}^{3}T_{ij}\lambda_i\otimes\lambda_j\right). \tag{4.2.1}$$

with the local Bloch vectors $\boldsymbol{\alpha},\boldsymbol{\beta}$ and the correlation matrix T. As mentioned Sec. 1.3, the Makhlin invariants [366] are written as

$$I_4 = \alpha^2, \qquad I_7 = \beta^2, \qquad I_2 = \mathrm{tr}(TT^\top), \tag{4.2.2}$$

$$I_{12} = \boldsymbol{\alpha}^\top T\boldsymbol{\beta}, \qquad I_1 = \det(T), \tag{4.2.3}$$

$$I_5 = [\boldsymbol{\alpha}T]^2, \qquad I_8 = [T\boldsymbol{\beta}]^2, \qquad I_3 = \mathrm{tr}(TT^\top TT^\top), \tag{4.2.4}$$

$$I_{14} = \mathrm{tr}(H_\alpha T H_\beta^\top T^\top), \tag{4.2.5}$$

$$I_{13} = \boldsymbol{\alpha}^\top TT^\top T\boldsymbol{\beta}, \qquad I_6 = [\boldsymbol{\alpha}TT^\top]^2, \qquad I_9 = [T^\top T\boldsymbol{\beta}]^2, \tag{4.2.6}$$

where $\alpha^2 = |\boldsymbol{\alpha}|^2$, $\beta^2 = |\boldsymbol{\beta}|^2$, and $(H_x)_{ij} = \sum_{k=x,y,z}\varepsilon_{ijk}x_k$ with the Levi-Civita symbol ε_{ijk} for $x = \alpha,\beta$.

It has been proven that two two-qubit states are LU equivalent if and only if they have equal values of all LU invariants. Now the question arises of how randomized measurements can be used to completely characterize the Makhlin invariants. Here we present our results in the following:

Result 17. *All the above Makhlin invariants are accessible from randomized measurements. That is, for the moments $\mathcal{R}^{(t)}_{\mathcal{M}}$ in Eq. (4.1.1) with several observables $\mathcal{M}$, it holds that*

$$\mathcal{R}^{(2)}_{\sigma_z\otimes\mathbb{1}} = \frac{1}{3}I_4, \quad \mathcal{R}^{(2)}_{\mathbb{1}\otimes\sigma_z} = \frac{1}{3}I_7, \quad \mathcal{R}^{(2)}_{\sigma_z\otimes\sigma_z} = \frac{1}{9}I_2, \tag{4.2.7}$$

$$\mathcal{R}^{(3)}_{(\mathbb{1}+\sigma_z)^{\otimes 2}} = \frac{1}{3}(I_2 + 2I_{12}) + \cdots, \quad \mathcal{R}^{(3)}_{\mathcal{M}_{\mathrm{det}}} = I_1, \tag{4.2.8}$$

$$\mathcal{R}^{(4)}_{(\mathbb{1}+\sigma_z)^{\otimes 2}} = \frac{2}{15}[(I_4+I_7)I_2 + 2(I_5+I_8)] + \cdots, \quad \mathcal{R}^{(4)}_{\sigma_z\otimes\sigma_z} = \frac{1}{75}(2I_3 + I_2^2), \tag{4.2.9}$$

$$\mathcal{R}^{(4)}_{\mathcal{M}_{\mathrm{H}}^{\mp}} = \pm\frac{1}{6}I_{14} + \cdots, \tag{4.2.10}$$

$$\mathcal{R}^{(5)}_{(\mathbb{1}+\sigma_z)^{\otimes 2}} = \frac{1}{15}[2I_3 + I_2(I_2 + 4I_{12}) + 8I_{13}] + \cdots, \tag{4.2.11}$$

$$\mathcal{R}^{(6)}_{(\mathbb{1}+\sigma_z)^{\otimes 2}} = \frac{8}{35}(I_6 + I_9) + \cdots, \tag{4.2.12}$$

where we denote

$$\mathcal{M}_{\mathrm{det}} = \sum_{i=x,y,z}\sigma_i\otimes\sigma_i, \tag{4.2.13}$$

$$\mathcal{M}_{\mathrm{H}}^{\mp} = \mathbb{1}\otimes\sigma_x + \sigma_x\otimes\mathbb{1} + \sigma_y\otimes\sigma_z \mp \sigma_z\otimes\sigma_y. \tag{4.2.14}$$

Remark 14. The proof of this derivation is given in Sec. 9.3. It is worthwhile to note that I_1 and I_{14} flip the sign under the partial transposition of the state, while the others are invariant. This is why I_1 and I_{14} can be obtained using the non-product observables $\mathcal{M}_{\rm det}$ and $\mathcal{M}_{\rm H}^{\mp}$, whereas the others come from the product observables. The LU invariants I_1 and I_{14} are sensitive to partial transposition and then allow us to extract vital information about nonlocal properties.

4.3 Applications to quantum information processings

Here we discuss the applications of Result 17 to the analysis of quantum states. The simplest example is to use the second moment $\mathcal{R}^{(2)}_{\sigma_z\otimes\sigma_z}$, i.e., I_2. This coincides with the sector length S_2 up to a factor, so the separability bound can be derived as mentioned in Sec. 1.4: $S_2 \leq 1$ for any two-qubit separable states. Then this violation implies that the state is entangled. Also, as presented in Chapter 2 and Ref. [378, 379], the fourth moment $\mathcal{R}^{(4)}_{\sigma_z\otimes\sigma_z}$ allows us to enhance the entanglement detection. This results from linear combinations between the second and fourth moments.

Another interesting approach to utilizing the Makhlin invariants is to consider their nonlinear combinations. In the following let us elaborate on this in more detail. Now, we can formulate the application to Bell nonlocality:

Result 18. *The presence of Bell nonlocality can be observed from randomized measurements. More precisely, the CHSH quantity* $\max_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}} \langle \mathcal{B} \rangle$ *in Eq. (1.2.43) can be completely computed from the moments* $\mathcal{R}^{(t)}_{\mathcal{M}}$.

Proof. As mentioned in Eq. (1.2.43) in Sec. 1.2, it holds that $\max_{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d}} \langle \mathcal{B} \rangle = 2\sqrt{\lambda_1^2 + \lambda_2^2}$, where λ_1 and λ_2 are the two largest singular values of the correlation matrix $T = (t_{ij})$. Since the squares of the singular values of T (that is, λ_i^2) coincide with the eigenvalues of $TT^\top$, the three invariants I_1, I_2, I_3 are sufficient to calculate a potential violation of the CHSH quantity following its characteristic polynomial:

$$p_T(x) = x^3 - \mathrm{tr}(TT^\top)x^2 - -\frac{1}{2}[\mathrm{tr}(TT^\top TT^\top) - \mathrm{tr}(TT^\top)^2]x - \det(T)^2. \quad (4.3.1)$$

According to Result 17, these LU invariants are accessible to the moments $\mathcal{R}^{(t)}_{\mathcal{M}}$ for $t = 2, 3, 4$. Hence, the scheme of randomized measurements enables us to compute its roots and therefore verify the violation of the CHSH inequality. □

In a similar manner, we can further proceed with the analysis of entangled states. In the following we can give two results:

Result 19. *The usefulness of quantum teleportation can be observed from randomized measurements. More precisely, the lower bound on the teleportation fidelity* $\mathcal{F}_U(\varrho_{AB})$ *in Eq. (1.2.64) can be completely computed from the moments* $\mathcal{R}^{(t)}_{\mathcal{M}}$.

Result 20. *The necessary and sufficient condition for two-qubit entanglement can be observed from randomized measurements. More precisely, the negativity of* $\det(\varrho_{AB}^{\top_B})$ *in Eq. (1.4.40) can be completely computed from the moments* $\mathcal{R}_{\mathcal{M}}^{(t)}$.

Proof. As mentioned in Eq. (1.2.64), $\mathcal{F}_U(\varrho_{AB}) = f(\tau_1, \tau_2, \tau_3)$ is a function of the eigenvalues τ_i of the correlation matrix T. This quantity can be accessible from the invariants I_1, I_2, I_3, that is, from randomized measurements. Concerning $\det(\varrho_{AB}^{\top_B})$, as we can see from Eq. (1.4.40), it is a function of several invariants that can be obtained from randomized measurements. □

4.4 Discussions

This Chapter showed that local unitary invariants in two-qubit systems, i.e., the Makhlin invariants, can be accessed from the moments of randomized measurements. We demonstrated that additional quantum information can be extracted by developing the scheme with non-product observables. Then we provided the complete characterization of two-qubit states via the associated quantities with Bell nonlocality, quantum teleportation, and the PPT criterion.

There are several directions for further research. First, it would be interesting to extend our results into multipartite higher-dimensional quantum systems. This may allow us to develop the characterization of nonlocal quantum channels or multiparticle quantum correlations in a reference-frame-independent way. Next, it would be desirable to deepen the understanding of cases with non-product observables in multipartite systems. Finally, we note that Ref. [6] provides the experimental demonstration of our results and discussed the statistical analysis of the generation of random unitaries in terms of frame potentials.

Part II

Applications of randomized measurements

Chapter 5

Work fluctuations and entanglement in quantum batteries

The previous Chapters have developed several methods of randomized measurements for detecting quantum entanglement. This Chapter focuses on their applications to the analysis of thermodynamic work cost in local random unitary processes. This Chapter characterizes quantum entanglement by monitoring the work fluctuations and develops its estimation in energy measurement protocols with noisy detectors. This Chapter is based on Ref. [4].

5.1 Introduction

At the heart of quantum thermodynamics [450] lies the fundamental question about the emergence of thermodynamic properties in small quantum systems. Quantum thermodynamics has not only established a common playground for statistical mechanics and quantum information theorists, it is now driving experimental efforts to seek and exploit genuine quantum signatures in thermodynamic processes.

In particular, quantum correlations have been investigated in terms of their fundamental energetic footprint [451, 452] and work cost [453–458], and as a resource in quantum thermal machines [459, 460]. Research on quantum batteries [461] highlights the role of correlations for work extraction [462–464] and storage [465–473] in composite quantum systems. Experimental investigations of quantum batteries are already underway [474, 475].

In practice, if work is consumed or generated on the quantum scale, strong fluctuations are often inevitable. Whether they are caused by a lack of experimental control, environmental decoherence, or other unknown sources of noise, the fluctuations are not only detrimental to the performance of thermodynamic tasks, but their precise statistics are often inaccessible. It is a common approach in quantum information theory to circumvent this problem by considering—or even deliberately applying—uniformly random unitary operations on the quantum system [1, 2, 350, 373, 378, 379, 412–415, 418]. This operational "worst-

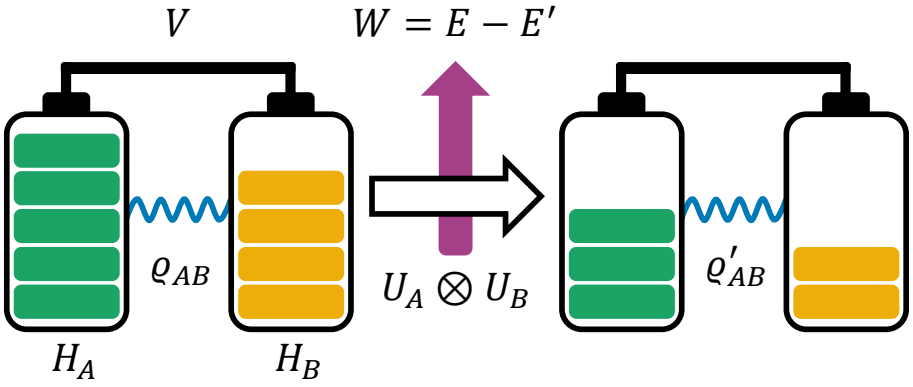

Figure 5.1: Sketch of the interacting quantum battery as a composite working medium that can be entangled in a $d \times d$ system. The quantum battery is described by a state ϱ_{AB} and a Hamiltonian $H_{AB} = H_A + H_B + gV$ with coupling strength g. It is transformed by a local random unitary operation $U_A \otimes U_B$: $\varrho_{AB} \to \varrho'_{AB} = (U_A \otimes U_B)\varrho_{AB}(U_A^\dagger \otimes U_B^\dagger)$. Then the average extractable work in this process $W(U_A, U_B) = E - E'$ becomes random. The essential thermodynamic quantity to characterize high-dimensional entanglement in this Chapter is the work variance $(\Delta\overline{W})^2$ over the random unitaries. This figure is taken from Ref. [4].

case" procedure will override other noise effects by rotating around an arbitrary Hilbert space direction, which results in a maximally mixed system state on average. Nevertheless, measurement data from a large sample of random unitaries can reveal genuine quantum features of the system state.

In the context of quantum thermodynamics, random unitaries and random Hamiltonians that generate them have been used to characterize the work distribution in chaotic quantum systems [476–480]. Other studies analyzed the thermodynamics of quantum batteries under random unitary rotations [481, 482], randomly repeated collisions [483–485], or random interaction Hamiltonians [486–488].

Here, we show that one can detect bipartite entanglement in a composite interacting working medium through work fluctuations under local random unitaries. We derive a hierarchy of bounds on high-dimensional entanglement in terms of the so-called Schmidt number, and we show that stronger work fluctuations can verify the presence of stronger entanglement. Furthermore, we develop noisy two-point energy measurement protocols based on inefficient detectors that can estimate work fluctuations and thereby probe the Schmidt number.

5.2 Work fluctuations under local unitary processes

5.2.1 Quantum battery

Consider an interacting bipartite quantum system with dimension $d \times d$ and Hamiltonian $H_{AB} = H_A \otimes \mathbb{1}_B + \mathbb{1}_A \otimes H_B + gV$, prepared in a (possibly entangled) quantum state ϱ_{AB}. Its energy content $E = \mathrm{tr}[\varrho_{AB} H_{AB}]$ has contributions from the local Hamiltonians H_A, H_B and from the interaction term V at coupling strength g. The system shall act as a quantum battery that receives or delivers energy through a local (non-entangling) unitary control operation, which we describe by $\varrho'_{AB} = (U_A \otimes U_B)\varrho_{AB}(U_A^\dagger \otimes U_B^\dagger)$, see also Fig. 5.1.

We assume a pulsed (or cyclic) operation that leaves the system Hamiltonian unchanged, i.e., $H'_{AB} = H_{AB}$. Indeed, this is based on an operational description of quantum thermodynamics, where the battery is characterized by a bare, time-independent Hamiltonian and unitaries represent pulsed (or cyclic) control operations that always take the system back to this bare Hamiltonian. No further assumptions are made here about how random control operations are realized, whether by controlled cyclic time evolution or by rapid quench (switching on and off the Hamiltonian that generates the operation).

The associated locally extracted work is quantified by the energy difference

$$W(U_A, U_B) = E - E' = \mathrm{tr}[(\varrho_{AB} - \varrho'_{AB})H_{AB}]. \tag{5.2.1}$$

Most studies on quantum battery (dis-)charging focus on the maximum amount of the extractable work, called ergotropy [489], which has recently been linked to quantum correlations [452, 490–492]. In this Chapter, we will not be concerned with the maximization, but rather with the work statistics over a sample of uniformly random local operations and relate it to the entanglement between the parts of the battery. We consider the average work and its variance over a sample of unitaries U_A, U_B drawn from the unitary groups $\mathcal{U}(d)$:

$$\overline{W} = \int dU_A \int dU_B \, W(U_A, U_B), \tag{5.2.2}$$

$$(\Delta\overline{W})^2 = \overline{W^2} - \overline{W}^2, \tag{5.2.3}$$

where the integrals are taken over the Haar measure, see Sec. 1.1 for details. We immediately find that $\overline{W} = E - \mathrm{tr}[H_{AB}]/d^2$, since the averaged final battery state is always maximally mixed. On the other hand, we will see that the variance $(\Delta\overline{W})^2$ of work fluctuations can reveal initial quantum correlations in the battery.

5.2.2 Work fluctuations

By virtue of the Schur-Weyl duality [109, 493, 494], we can carry out the unitary integrals in Eq. (5.2.3) and link the work fluctuations to the generalized Bloch decomposition of ϱ_{AB} and H_{AB}. Recall that any $d \times d$ state ϱ_{AB} can be written as

$$\varrho_{AB} = \frac{1}{d^2}\Big(\mathbb{1}_{AB} + \sum_{i=1}^{d^2-1} r_i^A \lambda_i \otimes \mathbb{1}_B + \sum_{i=1}^{d^2-1} r_i^B \mathbb{1}_A \otimes \lambda_i + \sum_{i,j=1}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j\Big), \tag{5.2.4}$$

with $\lambda_0 = \mathbb{1}_d$ and λ_i the so-called Gell-Mann matrices for $i = 1, \ldots, d^2 - 1$ [25, 26, 495]. These matrices generalize the Pauli matrices to SU(d), satisfying $\lambda_i^\dagger = \lambda_i$, $\mathrm{tr}[\lambda_i] = 0$, and $\mathrm{tr}[\lambda_i \lambda_j] = d\delta_{ij}$. The coefficient vectors $\vec{r}^A$ and $\vec{r}^B$ characterize the two reduced battery states, while the matrix (t_{ij}) represents all correlations. Similarly, we can expand the terms of the Hamiltonian as

$$H_X = \sum_{i=0}^{d^2-1} h_i^X \lambda_i, \qquad V = \sum_{i,j=1}^{d^2-1} v_{ij} \lambda_i \otimes \lambda_j. \tag{5.2.5}$$

This leads to an explicit form for the work fluctuations:

Result 21. *The work variance over local random unitary operations in a $d \times d$ quantum battery described by ϱ_{AB} and H_{AB} can be written in terms of the Bloch representation as*

$$(\Delta \overline{W})^2 = \frac{1}{d^2 - 1} \left(r_A^2 h_A^2 + r_B^2 h_B^2 + \frac{t^2 g^2 v^2}{d^2 - 1} \right), \tag{5.2.6}$$

where

$$r_X^2 = |\vec{r}^X|^2, \quad t^2 = \sum_{i,j} t_{ij}^2, \quad h_X^2 = |\vec{h}^X|^2, \quad v^2 = \sum_{i,j} v_{ij}^2, \tag{5.2.7}$$

for $X = A, B$.

Proof. First, we can immediately find

$$(\Delta \overline{W})^2 = \overline{(E')^2} - \overline{E'}^2. \tag{5.2.8}$$

The first term on this right-hand side can be written as

$$\begin{aligned} \overline{(E')^2} &= \int dU_A \int dU_B \, \left\{ \mathrm{tr}[\varrho'_{AB} H_{AB}] \right\}^2 \\ &= \int dU_A \int dU_B \, \mathrm{tr} \left[\varrho'^{\otimes 2}_{AB} H^{\otimes 2}_{AB} \right] \\ &= \mathrm{tr} \left[\left(\int dU_A \int dU_B \, \varrho'^{\otimes 2}_{AB} \right) H^{\otimes 2}_{AB} \right] \\ &= \mathrm{tr} \left[\Phi(\varrho_{AB}) H^{\otimes 2}_{AB} \right], \end{aligned} \tag{5.2.9}$$

where the map $\Phi(\varrho_{AB})$ is given below, see Eq. (5.2.11). For a two-qudit state ϱ_{AB}, let us consider

$$\Phi(\varrho_{AB}) = \int dU_A dU_B \, (U_A^{\otimes 2} \otimes U_B^{\otimes 2}) \varrho_{AB}^{\otimes 2} (U_A^\dagger)^{\otimes 2} \otimes (U_B^\dagger)^{\otimes 2}. \tag{5.2.10}$$

Using the generalized Bloch representation of ϱ_{AB} and the formulas in Sec. 1.5, we can obtain

$$\Phi(\varrho_{AB}) = \frac{1}{d^4} \left\{ \mathbb{1}_{AB}^{\otimes 2} + \frac{1}{d^2 - 1} \left[r_A^2 \widetilde{A} \otimes \mathbb{1}_B^{\otimes 2} + r_B^2 \mathbb{1}_A^{\otimes 2} \otimes \widetilde{B} + \frac{t^2 \widetilde{A} \otimes \widetilde{B}}{d^2 - 1} \right] \right\}, \tag{5.2.11}$$

where $\widetilde{X} = d\mathbb{S}_X - \mathbb{1}_X^{\otimes 2}$ for $X = A, B$ and $\mathbb{S}_A$ and $\mathbb{S}_B$ respectively are the SWAP operators acting on the two-copy system of $\varrho_{AB}^{\otimes 2}$. Using the expansion of the Hamiltonian terms in Eq. (5.2.5), with the help of the properties of Gell-Mann matrices, a long but straightforward calculation leads to the expression (5.2.6). □

Remark 15. Similar quantities have appeared in the notion of sector lengths in quantum information theory, see Sec. 1.4. Here, the bipartite correlations of the battery state ϱ_{AB} contribute to $(\Delta\overline{W})^2$ via the term t^2, provided there is a finite coupling $g \neq 0$ between the battery parts.

5.2.3 Schmidt number detection

Here we characterize the entanglement in ϱ_{AB} based on Eq. (5.2.6). Let us recall the concept of the Schmidt number in Eq. (1.2.6)

$$\mathrm{SN}(\varrho_{AB}) = \inf_{\mathcal{D}(\varrho_{AB})} \max_{\{\psi_i\}} r(\psi_i). \tag{5.2.12}$$

A higher Schmidt number thus indicates stronger entanglement, augmenting the separability problem [17, 123]. Several methods to witness the Schmidt number are already known [259, 496–499]. We now formulate a criterion based on work fluctuations, which elucidates the role of entanglement in work exchange processes:

Result 22. *Any $d \times d$ composite quantum battery described by ϱ_{AB} and H_{AB} with $\mathrm{SN}(\varrho_{AB}) = k$ obeys*

$$(\Delta\overline{W})^2 \leq \frac{1}{d^2-1}\left(r_A^2 h_A^2 + r_B^2 h_B^2 + \frac{g^2 v^2 s_k}{d^2-1}\right), \tag{5.2.13}$$

with the function

$$s_k = s\left(k, d, r_A^2, r_B^2\right) = kd - 1 + \frac{kd-2}{2}\left(r_A^2 + r_B^2\right) - \frac{kd}{2}\left|r_A^2 - r_B^2\right|. \tag{5.2.14}$$

Proof. Let us begin by considering a map given by

$$M_k(X) = \mathrm{tr}[X]\mathbb{1} - \frac{X}{k}, \tag{5.2.15}$$

for an operator $X \in \mathcal{H}^d$ and an integer k. Ref. [124] showed that, if a two-qudit state ϱ_{AB} has Schmidt number $\mathrm{SN}(\varrho_{AB}) = k$, then $(M_k \otimes \mathbb{1}_B)(\varrho_{AB})$ is positive,

$$(M_k \otimes \mathbb{1}_B)(\varrho_{AB}) = \varrho_A \otimes \mathbb{1}_B - \frac{1}{k}\varrho_{AB} \geq 0, \tag{5.2.16}$$

where $\varrho_A = \mathrm{tr}_B[\varrho_{AB}]$. Noting that $\mathrm{tr}[\varrho_{AB} O] \geq 0$ for any positive operator O, and taking $O = (M_k \otimes \mathbb{1}_B)(\varrho_{AB})$, we have

$$\mathrm{tr}[\varrho_{AB}^2] \leq k\,\mathrm{tr}[\varrho_A^2]. \tag{5.2.17}$$

Similarly, we can show that $\mathrm{tr}[\varrho_{AB}^2] \leq k\,\mathrm{tr}[\varrho_B^2]$. In summary, any $d \times d$ quantum state ϱ_{AB} with Schmidt number k obeys

$$\mathrm{tr}[\varrho_{AB}^2] \leq k \min\left\{\mathrm{tr}[\varrho_A^2],\, \mathrm{tr}[\varrho_B^2]\right\}. \tag{5.2.18}$$

For $k = 1$, this inequality becomes equivalent to the well-known entropic separability criterion [64, 412].

Here we note that

$$\mathrm{tr}[\varrho_{AB}^2] = \frac{1}{d^2}\left(1 + r_A^2 + r_B^2 + t^2\right). \tag{5.2.19}$$

Using Eq. (5.2.19) and $\min(a,b) = (a+b-|a-b|)/2$, we can rewrite the above condition as

$$t^2 \leq kd - 1 + \frac{kd-2}{2}\left(r_A^2 + r_B^2\right) - \frac{kd}{2}\left|r_A^2 - r_B^2\right|. \tag{5.2.20}$$

In the above Result, the right-hand side is subsumed as $s_k \equiv s\left(k, d, r_A^2, r_B^2\right)$. A violation of this inequality implies that the state has a Schmidt number of at least $(k+1)$. Result 22 follows by applying the inequality to the work fluctuations $(\Delta\overline{W})^2$ in Eq. (5.2.6). We remark that a similar proof technique was employed in Ref. [1]. □

A violation of Eq. (5.2.13) implies that the battery state ϱ_{AB} has a Schmidt number of at least $(k+1)$. Hence, observing stronger work fluctuations from local random unitaries on a composite quantum battery allows us to detect high-dimensional entanglement.

Remark 16. Note that the converse argument can be also true in the case of pure states. To see this, we begin by noting that the purity constraint $\mathrm{tr}[\varrho_{AB}^2] = 1$ is equivalent to $r_A^2 + r_B^2 = d^2 - 1 - t^2$. For the sake of simplicity, assuming $h_A^2 = h_B^2 = h^2$, we can then express $(\Delta\overline{W})^2$ as

$$(\Delta\overline{W})^2 = h^2 + \frac{Gt^2}{d^2-1}, \tag{5.2.21}$$

where $G = (g^2v^2)/(d^2-1) - h^2$. Also, we can rewrite the Schmidt number criterion as $t^2 \leq d^2 + 1 - \frac{2d}{k}$. If the interaction is sufficiently strong, that is, $G > 0$, then we get an upper bound on $(\Delta\overline{W})^2$ from the Schmidt number criterion and arrive at the same conclusion as Result 22. On the other hand, if the interaction is weak, $G < 0$, then a *lower* bound on $(\Delta\overline{W})^2$ is obtained, and hence *weaker* work fluctuations would certify higher entanglement.

Remark 17. We remark that our approach to detecting high-dimensional entanglement by observing random fluctuations can be applied not only to energy, but also to other observables measuring bipartite correlations.

5.2.4 Example: entangled thermal state

We shall test our criterion with the family of states

$$\varrho_\alpha = \alpha\,|\phi\rangle\langle\phi| + (1-\alpha)\tau_A \otimes \tau_B. \tag{5.2.22}$$

They are mixtures between the product of local Gibbs states at temperature T, $\tau_X = \exp(-H_X/T)/Z_X$, and the pure entangled state $|\phi\rangle$ that is locally indistinguishable from the Gibbs states, $\mathrm{tr}_A(|\phi\rangle\langle\phi|) = \tau_B$ and $\mathrm{tr}_B(|\phi\rangle\langle\phi|) = \tau_A$. Note that, in the limit $T \to \infty$, the Gibbs states are maximally mixed, and hence the ϱ_α are isotropic states.

As a simple example, consider an interacting four-qubit battery based on the Ising-type Hamiltonian

$$H_I = \sum_{i=1,2,3} J_i Z_i \otimes Z_{i+1} + b\sum_{i=1}^{4} Z_i, \tag{5.2.23}$$

with Z_i being the Pauli-Z matrix acting on the i-th qubit, b the homogeneous field strength, and J_i the nearest-neighbour couplings. Assuming the bipartition $(A|B) = (1,2|3,4)$, we can identify $h_A^2 = J_1^2 + 2b^2$, $h_B^2 = J_3^2 + 2b^2$, and $g^2v^2 = J_2^2$. We illustrate the work fluctuations for an exemplary choice of strong coupling parameters in Fig. 5.2. Panel (a) shows the work variance as a function of (b,α) and the Schmidt-number thresholds for $k = 1,2,3$, while (b) shows two selected histograms of suitably binned work values Eq. (5.2.1) associated with the Haar-random local unitaries.

In practice, these values could be inferred from joint local measurements in the Z-basis on sufficiently many identical copies of each unitary sample, and the statistical significance can be evaluated according to Ref. [2]. In the following, however, we will proceed to introduce two different measurement schemes to estimate the work fluctuations.

5.3 Energy measurement protocols

5.3.1 Noisy two-point measurements

The projective two-point measurement (TPM) protocol [500–502] defines a quantum notion of fluctuating work in analogy to classical stochastic thermodynamics, for trajectories of an arbitrary system state subject to a given isentropic process U. In this protocol, one first performs a projective measurement in the system's energy eigenbasis, lets the post-measurement state evolve under U, and then performs a second projective energy measurement. The difference between both outcomes can be seen as a random realization of work under U, and the so defined work statistics obey the Jarzynski equality [500–502].

However, the protocol has two major downsides. First, it is highly invasive since the first measurement voids all the coherence between energy levels that

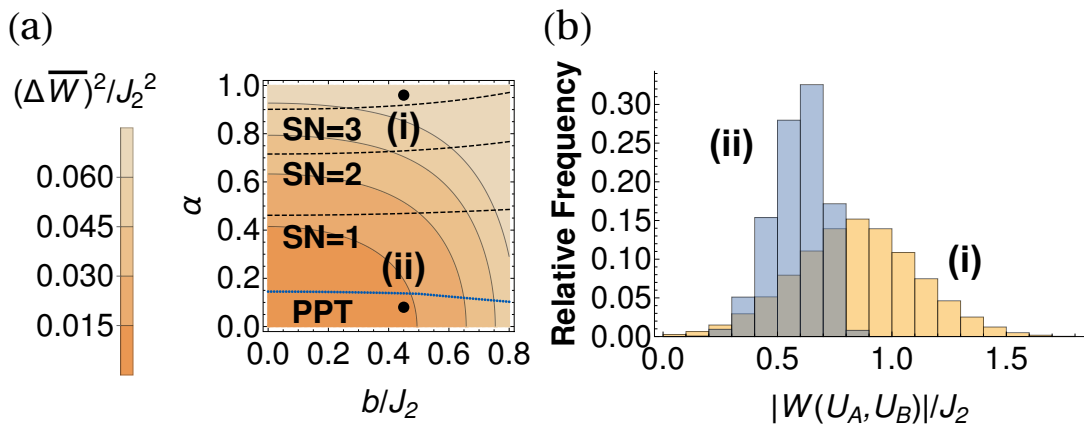

Figure 5.2: Schmidt number detection through local work fluctuations in an Ising-type battery of $2+2$ qubits. (a) Variance of average work extracted by local random unitaries acting on each battery half as a function of the field strength b and the mixing ratio α between a maximally entangled and a product Gibbs state. All energies are in units of the interaction strength J_2, and we fix $J_{1,3} = 0.5J_2$ and $T = 1.5J_2$. Quantum states with SN $= 1, 2, 3$ are contained in the areas below the respective dashed lines, according to Eq. (5.2.13), so above a line allows us to detect SN. For comparison, we also indicate a bottom blue threshold given by the PPT criterion. (b) Exemplary histograms of negative work values from a sample of 10^6 unitaries for the two marked cases (i) and (ii) at $b = 0.45$, corresponding to an entangled state of SN $= 4$ at $\alpha = 0.96$ and a state at $\alpha = 0.08$, compatible with separable states, respectively. Work values are divided into bins of size $0.1J_2$. This figure is taken from Ref. [4].

the initial system state might have. Genuine quantum signatures such as entanglement between different system parts may thus be destroyed. Second, ideal projective measurements may not be achievable due to limited accuracy and unavoidable noise in experiments. These two problems have motivated recent efforts to generalize the TPM protocol [47, 503–512].

We alleviate both problems by employing a TPM protocol with noisy detectors, first introduced in Ref. [47]. We adapt it to our setting of composite quantum batteries and have A, B each apply the protocol for a *local* energy measurement. To this end, we expand

$$H_X = \sum_{i=1}^{d} E_i^X \Pi_i^X, \tag{5.3.1}$$

with the energy eigenvalues E_i and the projectors Π_i^X to the corresponding eigenspaces. Moreover, we write the interaction term as

$$V = \sum_{i,j=1}^{d} D_{ij} \Pi_i^A \otimes \Pi_j^B + V_{od}, \tag{5.3.2}$$

with $\mathrm{tr}[V_{od} \Pi_i^A \otimes \Pi_j^B] = 0$ for all i, j. This separates mere level shifts of the joint diagonal energy spectrum, $E_{ij} = E_i^A + E_j^B + g D_{ij}$, from the actual change of the energy eigenbasis via the off-diagonal part V_{od}. The following results are based on estimating the E_{ij}-spectrum from noisy measurements in the basis of the $\Pi_i^A \otimes \Pi_j^B$. We stress that, for $V_{od} \neq 0$, the E_{ij}-values are not the battery energies and the measurement does not constitute an actual energy measurement (though it approximates one for small V_{od}).

The population of the diagonal spectrum (E_{ij}) can be probed straightforwardly by combining the outcomes of local energy measurements. Suppose these measurements are erroneous in that they detect the correct local energy state only with probability ε, while producing a completely random outcome with probability $1 - \varepsilon$. Assuming the same ε for both sides, the corresponding POVMs are

$$P_i^X = \varepsilon \Pi_i^X + \frac{1 - \varepsilon}{d} \mathbb{1}_X, \quad \sum_{i=1}^{d} P_i^X = \mathbb{1}_X. \tag{5.3.3}$$

Here we assume that the Π_i^X are rank-1 projectors, so that the entire POVM has d outcomes. On average, we can obtain an unbiased estimator for (E_{ij}) from them by assigning to each joint outcome (ij) occuring with probability $m_{ij} = \mathrm{tr}[P_i^A \otimes P_j^B \varrho_{AB}]$ the rescaled and shifted energy value [47]

$$e_{ij} = \frac{E_i^A + E_j^B}{\varepsilon} + \frac{g D_{ij}}{\varepsilon^2} - \frac{1 - \varepsilon}{d\varepsilon} \left(\mathrm{tr}[H_A] + \mathrm{tr}[H_B] \right). \tag{5.3.4}$$

For $\varepsilon = 1$, we have noiseless projective measurements and $e_{ij} = E_{ij}$, whereas small values $\varepsilon \ll 1$ correspond to a weak measurement dominated by errors.

Note that the case of different errors $\varepsilon_A, \varepsilon_B$ is also discussed in the next subsection.

We subject the post-measurement state to local random unitaries $U_A \otimes U_B$,

$$\sigma_{ij} = \frac{U_A \sqrt{P_i^A} \otimes U_B \sqrt{P_j^B} \varrho_{AB} \sqrt{P_i^A} U_A^\dagger \otimes \sqrt{P_j^B} U_B^\dagger}{m_{ij}}, \tag{5.3.5}$$

before applying the same local measurement again. The probability to obtain e'_{kl} if the first outcome was e_{ij} is $m_{kl|ij} = \mathrm{tr}[P_k^A \otimes P_l^B \sigma_{ij}]$, to which we associate a presumed work value $w_{ijkl} = e_{ij} - e'_{kl}$. (It may only approximate the extracted work if $V_{od} \neq 0$, but small.) Averaged over many repetitions at fixed $U_A \otimes U_B$, we define

$$W_{\mathrm{TPM}}(\varepsilon) \equiv W_{\mathrm{TPM}}(\varepsilon, U_A, U_B) = \sum_{i,j,k,l} m_{ij} m_{kl|ij} w_{ijkl}, \tag{5.3.6}$$

which in turn can be averaged over a large sample of unitaries to yield

$$\overline{W_{\mathrm{TPM}}(\varepsilon)} = \int dU_A \int dU_B \, W_{\mathrm{TPM}}(\varepsilon), \tag{5.3.7}$$

$$(\Delta \overline{W_{\mathrm{TPM}}(\varepsilon)})^2 = \overline{W_{\mathrm{TPM}}(\varepsilon)^2} - \overline{W_{\mathrm{TPM}}(\varepsilon)}^2. \tag{5.3.8}$$

In general, these TPM cumulants do not coincide with the previously defined ones in Eqs. (5.2.2) and (5.2.3). However, we can still obtain an explicit relation between the variances:

Result 23. *For any $d \times d$ composite quantum battery described by ϱ_{AB} and H_{AB}, the local noisy TPM protocol results in the presumed work variance*

$$(\Delta \overline{W_{\mathrm{TPM}}(\varepsilon)})^2 = n_0(\varepsilon)(\Delta \overline{W})_D^2 + n_1(\varepsilon)(\Delta \overline{W_{\mathrm{Proj}}})^2 + [1 - n_0(\varepsilon) - n_1(\varepsilon)](\Delta \overline{W_{\mathrm{Noisy}}})^2, \tag{5.3.9}$$

where the functions $n_{0,1}(\varepsilon) \in [0,1]$ for any $\varepsilon \in [0,1]$ are explicitly given. The term $(\Delta \overline{W})_D^2$ is the theoretical work variance in Eq. (5.2.6) evaluated for $V_{od} = 0$. The $(\Delta \overline{W_{\mathrm{Proj}}})^2$ and $(\Delta \overline{W_{\mathrm{Noisy}}})^2$ represent the variance for a noiseless projective TPM and an additional contribution at finite noise $\varepsilon \in (0,1)$, respectively, both also at $V_{od} = 0$.

Remark 18. For detailed descriptions, see Result 25, where the lengthy explicit expressions for $(\Delta \overline{W_{\mathrm{Proj}}})^2$, $(\Delta \overline{W_{\mathrm{Noisy}}})^2$, and $n_{0,1}(\varepsilon)$ are given. There we also show that the noisy TPM variance obeys

$$(\Delta \overline{W_{\mathrm{TPM}}(\varepsilon)})^2 \leq (\Delta \overline{W})_D^2, \tag{5.3.10}$$

which saturates in the limit $\varepsilon \to 0$, where $n_0 \to 1$ and $n_1 \to 0$. In the opposite limit $\varepsilon \to 1$ where $n_1 \to 1$ and $n_0 \to 0$, we have a local projective TPM which does not detect any entanglement. We compare the measured work variance at various noise levels to the theoretical values for our example states Eq. (5.2.22) in Fig. 5.3, demonstrating that the noisy local TPM can detect entanglement.

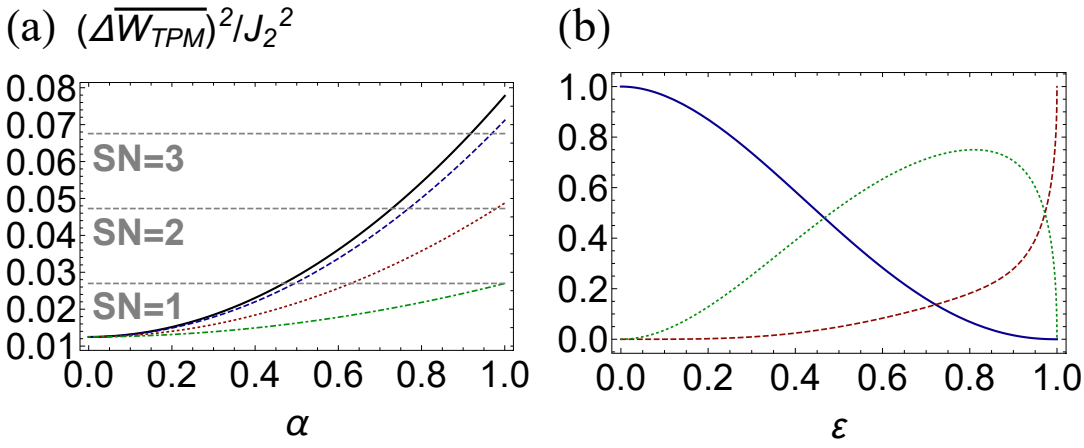

Figure 5.3: (a) Comparison between the theoretical work variance $(\Delta\overline{W})^2_D$ (black solid) and the variance $(\Delta\overline{W_{\rm TPM}(\varepsilon)})^2$ resulting from a local TPM protocol at various noise levels $\varepsilon = 0.2, 0.5$, and 1.0 (respectively, dashed blue, dotted red, and dash-dotted green), for the Ising battery of Fig. 5.2 at fixed $b = 0.45J_2$ and varying mixing ratio α. The dashed horizontal lines show the bounds compatible with Schmidt numbers $1, 2, 3$. (b) Weight functions $n_0(\varepsilon)$ (blue solid), $n_1(\varepsilon)$ (dashed red), and $1 - n_0(\varepsilon) - n_1(\varepsilon)$ (dotted green) versus noise level ε. This figure is taken from Ref. [4].

5.3.2 Detailed discussions about Result 23

More generally, let us begin by considering noisy local energy measurements on A and B with errors ε_A, ε_B,

$$P_i^A = \varepsilon_A \Pi_i^A + \frac{1-\varepsilon_A}{d}\mathbb{1}_A, \qquad P_i^B = \varepsilon_B \Pi_i^B + \frac{1-\varepsilon_B}{d}\mathbb{1}_B. \tag{5.3.11}$$

In the previous subsection, we assumed $\varepsilon_A = \varepsilon_B$. The probability to obtain the local measurement outcomes i, j on ϱ_{AB} is given by $m_{ij} = \mathrm{tr}[P_i^A \otimes P_j^B \varrho_{AB}]$. Following the notion of quantum instruments [20], the normalized post-measurement state can be described by

$$\sigma_{ij} = \frac{1}{\mathrm{tr}[\mathcal{J}_{ij}(\varrho_{AB})]}\mathcal{J}_{ij}(\varrho_{AB}), \tag{5.3.12}$$

where $\mathcal{J}_{ij}$ is a linear completely positive and trace-preserving (CPTP) map satisfying

$$m_{ij} = \mathrm{tr}[\mathcal{J}_{ij}(\varrho_{AB})]. \tag{5.3.13}$$

Like most studies on two-point measurement protocols, we employ the so-called von Neumann-Lüders instrument in the previous subsection,

$$\mathcal{J}_{ij}^{\text{vN-L}}(\varrho_{AB}) = \sqrt{P_i^A} \otimes \sqrt{P_j^B}\varrho_{AB}\sqrt{P_i^A} \otimes \sqrt{P_j^B}. \tag{5.3.14}$$

For the sake of simplicity, let us now define the diagonal Hamiltonian H_D as an effective description:

$$H_D = H_{AB} - gV_{od}, \tag{5.3.15}$$

where

$$V = \sum_{i,j=1}^{d} D_{ij}\Pi_i^A \otimes \Pi_j^B + V_{od} \tag{5.3.16}$$

and V_{od} is the off-diagonal part of the interaction Hamiltonian (with vanishing diagonal elements) in the eigen-energy basis of the local Hamiltonian. On the one hand, the Hamiltonian H_D can be decomposed using the corresponding projectors $\Pi_i^A \otimes \Pi_j^B$,

$$H_D = \sum_{i,j} E_{ij}\Pi_i^A \otimes \Pi_j^B, \tag{5.3.17}$$

with the joint diagonal energy spectrum $E_{ij} = E_i^A + E_j^B + gD_{ij}$, given in the previous subsection. On the other hand, the Hamiltonian H_D can also be decomposed into the measurement operators P_i^A, P_j^B,

$$H_D = \sum_{i,j} e_{ij}P_i^A \otimes P_j^B, \tag{5.3.18}$$

with appropriate energy values e_{ij} assigned to each pair of measurement outcomes (i,j),

$$e_{ij} = e_i^A + e_j^B + gd_{ij}, \tag{5.3.19}$$

$$e_i^A = \frac{1}{\varepsilon_A}E_i^A - \frac{1-\varepsilon_A}{d\varepsilon_A}\mathrm{tr}[H_A], \quad e_j^B = \frac{1}{\varepsilon_B}E_j^B - \frac{1-\varepsilon_B}{d\varepsilon_B}\mathrm{tr}[H_B], \tag{5.3.20}$$

$$d_{ij} = \frac{1}{\varepsilon_A\varepsilon_B}D_{ij}. \tag{5.3.21}$$

The POVM decomposition of the Hamiltonian is motivated by the research in Ref. [47]. For $\varepsilon_A, \varepsilon_B = 1$, we have noiseless projective measurements and $e_{ij} = E_{ij}$, whereas small values $\varepsilon_A, \varepsilon_B \ll 1$ correspond to a weak measurement dominated by errors.

Similarly to the previous subsection, we define the average work over the noisy TPM protocol for independent errors as

$$W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B) \equiv W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B, U_A, U_B) = \sum_{i,j,k,l} m_{ij}m_{kl|ij}w_{ijkl}. \tag{5.3.22}$$

Here we recall that $m_{kl|ij} = \mathrm{tr}[P_k^A \otimes P_l^B \sigma'_{ij}]$ is the conditional probability to obtain the outcomes k,l associated to the energy value e'_{kl} in the second measurement, given that we obtained (i,j) and e_{ij} in the first measurement. The second measurement receives the state $\sigma'_{ij} = (U_A \otimes U_B)\sigma_{ij}(U_A \otimes U_B)^\dagger$, which is the state transformed by a local random unitary operation after the first noisy energy

measurement. We associate the presumed work value $w_{ijkl} = e_{ij} - e'_{kl}$ to the outcomes. Taking an average over a large sample of local unitaries yields

$$\overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)} = \int dU_A \int dU_B \, W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B), \tag{5.3.23}$$

$$(\Delta \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)})^2 = \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)^2} - \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)}^2. \tag{5.3.24}$$

In the following, we evaluate and simplify the unitary integrals:

Result 24. *For any $d \times d$ composite quantum battery described by ϱ_{AB} and H_D, the local noisy TPM protocol with ε_A and ε_B for the von Neumann-Lüders instrument results in the average which can be expressed as*

$$\overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)} = \mathrm{tr}[\varrho_{AB} H_D] - \frac{\mathrm{tr}[H_D]}{d^2}. \tag{5.3.25}$$

Result 25. *For any $d \times d$ composite quantum battery described by ϱ_{AB} and H_D with $\mathrm{tr}[H_D] = 0$, the local noisy TPM protocol with ε_A and ε_B for the von Neumann-Lüders instrument results in the presumed work variance which can be expressed as*

$$(\Delta \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)})^2 = \mathrm{Y}_{\mathrm{Ideal}} + \mathrm{Y}_{\mathrm{Proj}} + \mathrm{Y}_{\mathrm{Noisy}}, \tag{5.3.26}$$

where $\mathrm{Y}_{\mathrm{Ideal}}$, $\mathrm{Y}_{\mathrm{Proj}}$, and $\mathrm{Y}_{\mathrm{Noisy}}$, respectively, represent the effects of the ideal theoretical work variance, the variance from a noiseless projective TPM, and the noisy additional measurements at finite noise. They are given by

$$\mathrm{Y}_{\mathrm{Ideal}} \equiv \kappa_{AB}^2 (\Delta \overline{W})_D^2, \tag{5.3.27}$$

$$\begin{aligned} \mathrm{Y}_{\mathrm{Proj}} \equiv \frac{1}{d^2-1} \Bigg\{ & \left[(f_{\varepsilon_A}^4 f_{\varepsilon_B}^4 + \kappa_A^2) \left(d p_A^2 - 1 \right) + \kappa_B^2 r_A^2 \right] h_A^2 \\ & + \left[(f_{\varepsilon_A}^4 f_{\varepsilon_B}^4 + \kappa_B^2) \left(d p_B^2 - 1 \right) + \kappa_A^2 r_B^2 \right] h_B^2 \\ & + \frac{g^2 v^2}{d^2-1} \Big[f_{\varepsilon_A}^4 f_{\varepsilon_B}^4 \left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1 \right) \\ & + \kappa_A^2 \sum_{a,b,c} t_{ab} t_{cb} \zeta_{ac}^A + \kappa_B^2 \sum_{a,b,c} t_{ab} t_{ac} \zeta_{bc}^B \Big] \Bigg\}, \end{aligned} \tag{5.3.28}$$

$$\begin{aligned} \mathrm{Y}_{\mathrm{Noisy}} \equiv \frac{2}{d^2-1} \Bigg\{ & \left[\gamma_A \left(d p_A^2 - 1 \right) + \kappa_B \kappa_{AB} r_A^2 \right] h_A^2 + \left[\gamma_B \left(d p_B^2 - 1 \right) + \kappa_A \kappa_{AB} r_B^2 \right] h_B^2 \\ & + \frac{g^2 v^2}{d^2-1} \left[\gamma_{AB} \left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1 \right) \right] \\ & + \kappa_A \kappa_{AB} \sum_{a,b,c} t_{ab} t_{cb} \zeta_{ac}^A + \kappa_B \kappa_{AB} \sum_{a,b,c} t_{ab} t_{ac} \zeta_{bc}^B \Bigg\}. \end{aligned} \tag{5.3.29}$$

Here, $(\Delta \overline{W})_D^2$ is the ideal theoretical work variance, Eq. (5.2.6) in the previous subsection, evaluated for the diagonal Hamiltonian H_D, that is, for $V_{od} = 0$ and $v^2 =$

$(1/d^2)\sum_{i,j} D_{ij}^2$. *In the above expressions, we introduce the short-hand notations*

$$\gamma_A \equiv f_{\varepsilon_A}^2 f_{\varepsilon_B}^2(\kappa_A+\kappa_B+\kappa_{AB})+\kappa_A(\kappa_B+\kappa_{AB}), \tag{5.3.30}$$

$$\gamma_B \equiv f_{\varepsilon_A}^2 f_{\varepsilon_B}^2(\kappa_A+\kappa_B+\kappa_{AB})+\kappa_B(\kappa_A+\kappa_{AB}), \tag{5.3.31}$$

$$\gamma_{AB} \equiv f_{\varepsilon_A}^2 f_{\varepsilon_B}^2(\kappa_A+\kappa_B+\kappa_{AB})+\kappa_A\kappa_B, \tag{5.3.32}$$

$$\kappa_{AB} \equiv \kappa_A\kappa_B/(f_{\varepsilon_A}^2 f_{\varepsilon_B}^2), \tag{5.3.33}$$

$$\kappa_A \equiv f_{\varepsilon_A}^2 g_{\varepsilon_B}\left(2f_{\varepsilon_B}+dg_{\varepsilon_B}\right), \tag{5.3.34}$$

$$\kappa_B \equiv f_{\varepsilon_B}^2 g_{\varepsilon_A}\left(2f_{\varepsilon_A}+dg_{\varepsilon_A}\right), \tag{5.3.35}$$

$$f_{\varepsilon_X} \equiv \sqrt{\varepsilon_X+\frac{1-\varepsilon_X}{d}}-\sqrt{\frac{1-\varepsilon_X}{d}}, \tag{5.3.36}$$

$$g_{\varepsilon_X} \equiv \sqrt{\frac{1-\varepsilon_X}{d}}, \tag{5.3.37}$$

$$p_{AB}^2 \equiv \sum_{i,j}(p_{ij}^{AB})^2, \quad p_A^2 \equiv \sum_i (p_i^A)^2, \quad p_B^2 \equiv \sum_j (p_j^B)^2, \tag{5.3.38}$$

$$p_{ij}^{AB} \equiv \mathrm{tr}[\Pi_i^A \otimes \Pi_j^B \varrho_{AB}], \quad p_i^A \equiv \sum_j p_{ij}^{AB}, \quad p_j^B \equiv \sum_i p_{ij}^{AB}, \tag{5.3.39}$$

$$\zeta_{ab}^A \equiv \sum_i \frac{\mathrm{tr}(\Pi_i^A\lambda_a\Pi_i^A\lambda_b)}{d}, \quad \zeta_{ab}^B \equiv \sum_i \frac{\mathrm{tr}(\Pi_i^B\lambda_a\Pi_i^B\lambda_b)}{d}, \tag{5.3.40}$$

with the normalization condition

$$f_{\varepsilon_X}^2+2f_{\varepsilon_X}g_{\varepsilon_X}+dg_{\varepsilon_X}^2=1, \tag{5.3.41}$$

for $X=A,B$. *Let us define*

$$n_0(\varepsilon_A,\varepsilon_B) \equiv \kappa_{AB}^2, \tag{5.3.42}$$

$$n_1(\varepsilon_A,\varepsilon_B) \equiv f_{\varepsilon_A}^4 f_{\varepsilon_B}^4+\kappa_A^2+\kappa_B^2, \tag{5.3.43}$$

$$n_{\mathrm{Noisy}}(\varepsilon_A,\varepsilon_B) \equiv 2\left[f_{\varepsilon_A}^2 f_{\varepsilon_B}^2(\kappa_A+\kappa_B+\kappa_{AB})+\kappa_A\kappa_B+\kappa_A\kappa_{AB}+\kappa_B\kappa_{AB}\right], \tag{5.3.44}$$

where $n_0(\varepsilon_A,\varepsilon_B)$, $n_1(\varepsilon_A,\varepsilon_B)$, *and* $n_{\mathrm{Noisy}}(\varepsilon_A,\varepsilon_B)$ *are explicitly known functions obeying*

$$0 \le n_0(\varepsilon_A,\varepsilon_B),\, n_1(\varepsilon_A,\varepsilon_B),\, n_{\mathrm{Noisy}}(\varepsilon_A,\varepsilon_B) \le 1, \tag{5.3.45}$$

$$n_0(\varepsilon_A,\varepsilon_B)+n_1(\varepsilon_A,\varepsilon_B)+n_{\mathrm{Noisy}}(\varepsilon_A,\varepsilon_B)=1. \tag{5.3.46}$$

Then we also have

$$\begin{aligned}(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)})^2 \equiv\ & n_0(\varepsilon_A,\varepsilon_B)(\Delta\overline{W})_D^2+n_1(\varepsilon_A,\varepsilon_B)(\Delta\overline{W_{\mathrm{Proj}}})^2 \\ & +[1-n_0(\varepsilon_A,\varepsilon_B)-n_1(\varepsilon_A,\varepsilon_B)](\Delta\overline{W_{\mathrm{Noisy}}})^2,\end{aligned} \tag{5.3.47}$$

where

$$(\Delta\overline{W_{\mathrm{Proj}}})^2 \equiv \frac{1}{n_0(\varepsilon_A,\varepsilon_B)}\mathrm{Y}_{\mathrm{Proj}}, \tag{5.3.48}$$

$$(\Delta\overline{W_{\mathrm{Noisy}}})^2 \equiv \frac{1}{1-n_0(\varepsilon_A,\varepsilon_B)-n_1(\varepsilon_A,\varepsilon_B)}\mathrm{Y}_{\mathrm{Noisy}}. \tag{5.3.49}$$

Remark 19. In the case of symmetric errors, $\varepsilon_A = \varepsilon_B = \varepsilon$, we arrive at Result 23 in the previous subsection.

Remark 20. The proofs of Results 24 and 25 are given in Sec. 9.4.

Remark 21. For any $\varepsilon_A, \varepsilon_B$ and any dimension d, we find the inequality

$$(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)})^2 \leq (\Delta\overline{W})_D^2, \tag{5.3.50}$$

which is saturated by the limit $\varepsilon_A, \varepsilon_B \to 0$. To see this, we first show that

$$p_A^2 = \sum_i (p_i^A)^2 = \sum_i \mathrm{tr}[\Pi_i^A \varrho_A]^2 = \sum_i \mathrm{tr}[\Pi_i^A \varrho_A \Pi_i^A \varrho_A] \leq \sum_i \mathrm{tr}[\Pi_i^A \varrho_A^2] = \mathrm{tr}[\varrho_A^2], \tag{5.3.51}$$

where we employ that $\mathrm{tr}[ABAB] \leq \mathrm{tr}[A^2B^2]$, for any Hermitian operators A, B. This result directly yields $dp_A^2 - 1 \leq r_A^2$. Similarly we can have that $dp_B^2 - 1 \leq r_B^2$ and $d^2p_{AB}^2 - dp_A^2 - dp_B^2 + 1 \leq t^2$. Also, we find

$$\begin{aligned}
\sum_{a,b,c} t_{ab}t_{cb}\zeta_{ac}^A &= \frac{1}{d^2}\sum_{a,b,c,d}\sum_i t_{ab}t_{cd}\mathrm{tr}(\Pi_i^A\lambda_a\Pi_i^A\lambda_c)\mathrm{tr}(\lambda_b\lambda_d) \\
&= \frac{1}{d^2}\sum_{a,b,c,d}\sum_i t_{ab}t_{cd}\mathrm{tr}\left[(\Pi_i^A\otimes\mathbb{1}_B)(\lambda_a\otimes\lambda_b)(\Pi_i^A\otimes\mathbb{1}_B)(\lambda_c\otimes\lambda_d)\right] \\
&= \frac{1}{d^2}\sum_i \mathrm{tr}\left[(\Pi_i^A\otimes\mathbb{1}_B)T_2(\Pi_i^A\otimes\mathbb{1}_B)T_2\right] \\
&\leq \frac{1}{d^2}\sum_i \mathrm{tr}\left[(\Pi_i^A\otimes\mathbb{1}_B)T_2^2\right] = \frac{1}{d^2}\mathrm{tr}[T_2^2] = t^2,
\end{aligned} \tag{5.3.52}$$

where we employ that $\mathrm{tr}[ABAB] \leq \mathrm{tr}[A^2B^2]$, for any Hermitian operators A, B. Similarly, we have that $\sum_{a,b,c} t_{ab}t_{ac}\zeta_{bc}^B \leq t^2$. Substituting these results into the expression $(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)})^2$ given in Result 25 and using the condition $f_{\varepsilon_X}^2 + 2f_{\varepsilon_X}g_{\varepsilon_X} + dg_{\varepsilon_X}^2 = 1$ for $X = A, B$, we can straightforwardly complete the proof.

5.3.3 Noisy coincidence measurements

In order to estimate the work variance in Eq. (5.3.8), the noisy TPM scheme still relies on subjecting many copies of the battery state to the same randomly drawn local unitary. We can reduce this overhead by performing local coincidence measurements on merely two state copies $\varrho_{AB} \otimes \varrho_{A'B'}$ subjected to the same local unitary $U_A \otimes U_B$.

Ideally, a joint dichotomic projective measurement $\Pi_{AA'} \otimes \Pi_{BB'}$ would act locally on both A-copies and on both B-copies, with

$$\Pi_{XX'} = \sum_i \Pi_i^X \otimes \Pi_i^{X'}, \tag{5.3.53}$$

which projects onto the subspace spanned by energy product states with the same eigenvalues $E_i^X = E_i^{X'}$. By repeating this measurement with a large sample

of Haar-random unitaries, we could estimate the average probability $\overline{C}$ that the two copies' local energies on the A- and on the B-side both coincide.

More generally, we can define a dichotomic energy coincidence POVM based on noisy local energy measurements according to Eq. (5.3.3),

$$P_{XX'} = \sum_i P_i^X \otimes P_i^{X'} = \varepsilon^2 \Pi_{XX'} + \frac{1-\varepsilon^2}{d} \mathbb{1}_{XX'} \tag{5.3.54}$$

The probability for local energy coincidence between the copies on both sides is then $\mathcal{C}(\varepsilon) = \mathrm{tr}[P_{AA'} \otimes P_{BB'} \varrho'_{AB} \otimes \varrho'_{A'B'}]$. Averaged over the unitaries,

$$\overline{\mathcal{C}(\varepsilon)} = \frac{1}{d^2} \left[1 + \frac{(r_A^2 + r_B^2)\varepsilon^2}{d+1} + \frac{t^2 \varepsilon^4}{(d+1)^2} \right], \tag{5.3.55}$$

which we can directly relate to the entanglement-sensitive work variance $(\Delta \overline{W})^2$ from Eq. (5.2.3). Eq. (5.3.55) can be derived more generally, using different errors $\varepsilon_A, \varepsilon_B$ for measurements on the A, B sides:

Proof. First, we can immediately find

$$\overline{\mathcal{C}(\varepsilon_A, \varepsilon_B)} = \mathrm{tr}\left[\Phi(\varrho_{AB}) P_{AA'} \otimes P_{BB'} \right],$$

where $\Phi(\varrho_{AB})$ is defined in Eq. (5.2.11). Since

$$\mathrm{tr}[P_{XX'}] = \varepsilon_X^2 \mathrm{tr}[\Pi_{XX'}] + \frac{1-\varepsilon_X^2}{d} \mathrm{tr}[\mathbb{1}_{XX'}] = d, \tag{5.3.56}$$

$$\begin{aligned} \mathrm{tr}[S_X P_{XX'}] &= \varepsilon_X^2 \mathrm{tr}[S_X \Pi_{XX'}] + \frac{1-\varepsilon_X^2}{d} \mathrm{tr}[S_X \mathbb{1}_{XX'}] \\ &= (d-1)\varepsilon_X^2 + 1, \end{aligned} \tag{5.3.57}$$

we find

$$\overline{\mathcal{C}(\varepsilon_A, \varepsilon_B)} = \frac{1}{d^2} \left[1 + \frac{r_A^2 \varepsilon_A^2}{d+1} + \frac{r_B^2 \varepsilon_B^2}{d+1} + \frac{t^2 \varepsilon_A^2 \varepsilon_B^2}{(d+1)^2} \right].$$

For $\varepsilon_A = \varepsilon_B = \varepsilon$, we arrive at Eq. (5.3.55). □

Expressing the battery interaction strength as $g^2 v^2 = (d-1)(h^2 \varepsilon^2 + c)$, with $h^2 = \min(h_A^2, h_B^2)$ and a new term c, we find:

Result 26. *In the noisy energy coincidence measurement protocol, we have*

$$\overline{\mathcal{C}(\varepsilon)} \leq \frac{1}{d^2} \left[1 + \frac{(d-1)\varepsilon^2}{h^2} (\Delta \overline{W})^2 + \frac{t^2 \varepsilon^2 (|c| - c)}{2(d+1)^2 h^2} \right]. \tag{5.3.58}$$

Hence, the energy coincidence measurement protocol on two identical copies gives access to nonlinear functions of the battery state such as the work variance, which allows us to detect the Schmidt number by virtue of Result 22.

The proven influence of the Schmidt number on work fluctuations exemplifies the observable thermodynamic implications of high-dimensional bipartite entanglement. Our assessment in terms of the work variance with respect to Haar-random samples of unitaries extends previous studies on the direct estimation of nonlinear functions [107, 113, 513–516], experimental lower bounds on the concurrence [517–520], and protocols for randomized measurements [414, 415, 418].

5.4 Discussions

This Chapter investigated the role of entanglement in local work exchange with a composite quantum battery, as described by an interacting bipartite quantum system. In particular, we found that the variance of the average extracted work over a Haar-random sample of local unitary processes obeys a hierarchy of inequalities that detects the Schmidt number of the battery state. While we have seen that these bounds cannot be probed directly in a standard projective two-point measurement scheme, we have shown that the Schmidt number can be detected in a two-point measurement with noisy detectors as well as in an energy coincidence measurement.

There are several directions for further research. First, it would be interesting to verify our results on experimental platforms for quantum thermal machines and batteries. Second, the randomized two-point measurement approach could be extended to non-unitary, dissipative processes, facilitating the detection of heat leaks and non-unital dynamics in complex open quantum systems [521, 522]. Finally, our approach may encourage the development of temperature estimation [310] and thermodynamic uncertainty relation [523, 524] from randomized measurement schemes.

Chapter 6

Reference-frame-independent quantum metrology

This Chapter addresses the application of random measurements for reference-frame-independent quantum metrology. This Chapter provides systematic approaches using multiple copies of states based on randomized measurement observables. This Chapter shows that our formulation remains invariant under local unitaries and allows us to achieve several scalings in nonlinear Hamiltonian dynamics.

6.1 Introduction

As discussed in Sec. 1.3, the major task in quantum metrology is to enhance the metrological scheme so that it reaches an optimal precision beyond the classical regime. To reach a higher accuracy, precise control of state preparation and optimal measurement strategies should be required. In practice, however, unavoidable noise effects, such as magnetic field fluctuations or rotational polarizations of optical fibers may result in losing calibration of measurement directions or lacking common reference coordinate frames between different particles. This may lead to a loss of the quantum advantage and improved precision may not be achieved. Also, establishing a common frame of reference is known as an expensive process in resource theory [100].

In this Chapter, we address this issue and develop a metrological scheme under such limited quantum control. The key idea is to consider several copies of a quantum state and arbitrarily rotate the measurement direction after an entangling transformation. This procedure can be implemented by applying uniform Haar random local unitary operations on the quantum system, spirited by previous works of randomized measurements [1, 2, 4, 6, 7, 378, 379] and see Sec. 1.4.

Based on this idea, we will first present the estimation precision for the state's copies using the error-propagation formula with the randomized measurements, illustrated in Fig. 6.1. Our formulation can be described by local unitary in-

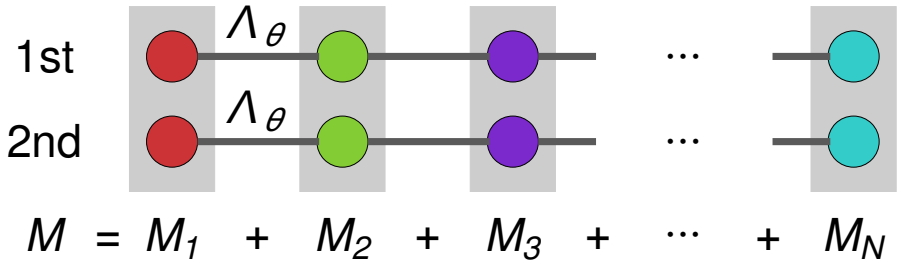

Figure 6.1: Sketch of the quantum metrology scheme from randomized measurements for two copies of N particles, proposed in this Chapter. In this scheme, the parameter θ is first encoded onto the 1st and 2nd copies by $\Lambda_\theta \otimes \Lambda_\theta$ in parallel in different colors. Then the randomized measurement $M = \sum_i M_i$ is performed with each local observable M_i acting on the 1st and 2nd copy, vertically in Gray color. This Chapter shows that the precision $(\Delta\theta)^2$ can be smaller beyond the single-copy regime.

variants and then can allow us to save the overall consumption of operational resources experimentally friendly. Then we will give several examples and demonstrate that quadratic scaling can also be achieved in a reference-frame-independent way. Finally, we will discuss how our scalings can be worsened by the effects of decoherence. Note that our approach differs from the previous parameter estimation tasks with limited control over reference frames [525–530].

6.2 Quantum metrology

Let ϱ be a N-particle d-dimensional quantum (N-qudit) state defined in $\mathcal{H}_d^{\otimes N}$. Suppose that the initial state ϱ can be transformed by a quantum transformation Λ_θ to encode a parameter θ: $\varrho \to \varrho_\theta = \Lambda_\theta(\varrho)$. A typical example is given by a unitary operator $V_\theta = e^{-i\theta H}$ with a Hamiltonian H as the generator of the dynamics.

In general, the parameter θ can be estimated from a measurement observable M. The precision of this estimation can be characterized by the well-known error-propagation formula [170, 171, 289, 298, 299]

$$(\Delta\theta)^2 = \frac{(\Delta M)^2}{|\partial_\theta \langle M \rangle|^2}, \tag{6.2.1}$$

where $(\Delta M)^2 \equiv \langle M^2 \rangle - \langle M \rangle^2$ and $\langle M \rangle$ is the expectation of M.

In many studies of quantum metrology, there are often discussions about the fundamental limit on precision with the help of the Cramer-Rao bound [300], where the notions of quantum Fisher information and Hamiltonian variance are used. There, the optimal measurement scheme is assumed to find the best accuracy and reach the known scalings. In the following, we will start with the error-propagation formula and show that the same scalings are achievable even

in scenarios where quantum control is limited in the sense of lacking a common reference frame.

6.3 Randomized observables

6.3.1 Two copies

We begin by considering k copies of the quantum state and performing a measurement on the system

$$\langle M_k \rangle = \mathrm{tr}(\varrho_\theta^{\otimes k} M_k), \tag{6.3.1}$$

where M_k acts on the k copies of the state defined in $(\mathcal{H}_d^{\otimes N})^{\otimes k}$. Here we suppose that the measurement observable M_k is written in the *local* form

$$M_k = \sum_{i=1}^{N} M_i^{(k)}, \tag{6.3.2}$$

where $M_i^{(k)}$ acts on the k copies of the i-th system.

Let us introduce a *randomized* (twirled) measurement observable

$$\Phi_k(\mathcal{O}) = \int dU \, (U^\dagger \mathcal{O} U)^{\otimes k}, \tag{6.3.3}$$

where $\mathcal{O}$ is an observable operator defined in $\mathcal{H}_d$ and the integral is taken as the Haar random unitaries. By definition, this does not change under any local unitary $V^{\otimes k}$ for $V \in \mathcal{U}(d)$: $\Phi_k(V^\dagger \mathcal{O} V) = \Phi_k(\mathcal{O})$. For the sake of simplicity, by default, we hereafter assume that $\mathrm{tr}(\mathcal{O}) = 0$ and $\mathrm{tr}(\mathcal{O}^2) = d$. Now, we can formulate the first main result of this Chapter:

Result 27. *Consider the case with $k = 2$ and $M_i^{(2)} = \Phi_2(\mathcal{O}_i)$. Then we have*

$$\langle M_2 \rangle = \frac{1}{d^2 - 1} S_1(\theta), \tag{6.3.4}$$

where $S_1(\theta) = \sum_{i=1}^{N} [d\,\mathrm{tr}(\varrho_i^2) - 1]$ for the single-particle reduced state $\varrho_i = \mathrm{tr}_{\bar{i}}(\varrho_\theta)$. Thus the error-propagation formula leads to that

$$(\Delta\theta)_2^2 = \frac{(d^2-1)N - 2S_1(\theta) + 2S_2(\theta) - S_1^2(\theta)}{|\partial_\theta S_1(\theta)|^2}, \tag{6.3.5}$$

where $S_2(\theta) = \sum_{i<j} [d^2 \mathrm{tr}(\varrho_{ij}^2) - 1 - S_1(\theta)]$ for the two-particle reduced state $\varrho_{ij} = \mathrm{tr}_{\overline{ij}}(\varrho_\theta)$.

Proof. To prove this result, we need to evaluate the Haar integral. In fact, one can have

$$\Phi_2(\mathcal{O}_i) = \frac{1}{d^2-1}\left(d\mathbb{S}_i - \mathbb{1}_d^{\otimes 2}\right), \tag{6.3.6}$$

where $\mathbb{S}_i$ is the SWAP operator acting on both the first and second copies of the i-th system: $\mathbb{S}|x\rangle|y\rangle = |y\rangle|x\rangle$, for details, see Refs. [68, 109, 531]. Using the property $\mathbb{S}_i^2 = \mathbb{1}_d$ and the SWAP trick $\mathrm{tr}[(X\otimes Y)\mathbb{S}] = \mathrm{tr}[XY]$ for operators X and Y, we can straightforwardly arrive at the Eqs. (6.3.4) and (6.3.5). □

Remark 22. The metrological scheme of this result is illustrated in Fig. 6.1, which includes the three stages of preparation, encoding, and measurement.

Remark 23. The $S_l(\theta)$ is the so-called l-body sector length, which can capture l-body quantum correlations for the integer $l \in [1, N]$ in general, see Eq. (1.4.7). The l-body sector length can be associated with the purity of the l-particle reduced states, and moreover it holds that $\sum_{l=1}^{N} S_l(\varrho) = d^N \mathrm{tr}(\varrho^2) - 1$ for any N-qudit state ϱ. An important property is that it is invariant under any local unitary: $S_l(V_1\otimes\cdots\otimes V_N \varrho V_1^\dagger \otimes\cdots\otimes V_N^\dagger) = S_l(\varrho)$ for an unitary $V_i \in \mathcal{U}(d)$ for $i = 1, \ldots, N$.

Remark 24. The precision obtained in Eq. (6.3.5) may remind us of the standard spin-squeezing parameter [159–161, 313, 314]. This is because the denominator depends on the reduced single-particle state, while the numerator depends not only on the reduced single-particle state but also on the reduced two-particle state. Note that the denominator and numerator in our result do not change under any local unitary, unlike spin squeezing.

Remark 25. The precision $(\Delta\theta)_2^2$ in Eq. (6.3.5) does not change under any parameter encoding by local unitary $V_L = e^{-i\theta H_L}$ for a local Hamiltonian $H_L = \sum_{i=1}^{N} H_i \otimes \mathbb{1}_{\bar{i}}$. On the other hand, some parameter encoding $V_G = e^{-i\theta H_G}$ for a nonlinear interaction Hamiltonian H_G can change the precision $(\Delta\theta)_2^2$.

Remark 26. One can generalize this method to further multicopy scenarios or nonlocal measurement observables. This may lead to other types of local unitary invariants with high degrees. However, evaluating the Haar integrals and finding the simplified precision would be demanding, and moreover, they cannot necessarily enable us to reach higher precision.

6.3.2 Four copies

In the following, we will consider four copies and derive the precision with higher-order quantities. For the sake of simplicity of computation, let us consider the case with qubits. Without loss of generality, we take $\mathcal{O} = \sigma_z$. Now we can formulate the result:

Result 28. *Consider the case with $k = 4$, $d = 2$, and $M_i^{(4)} = \Phi_4(\sigma_z^{(i)})$ for $i = 1, \ldots, N$. Then we have*

$$\langle M_4 \rangle = \frac{1}{5} F_1(\theta), \tag{6.3.7}$$

where $F_1(\theta) = \sum_{i=1}^{N} r_i^4$ *and* $r_i^2 = 2\mathrm{tr}[\varrho_i^2] - 1$ *for the single-particle reduced state* $\varrho_i = \mathrm{tr}_{\bar{i}}(\varrho_\theta)$. *Thus the error-propagation formula leads to that*

$$(\Delta\theta)_4^2 = \frac{1}{3}\frac{Z(\theta)}{|\partial_\theta F_1(\theta)|^2}, \tag{6.3.8}$$

where

$$Z(\theta) = 15N - 20S_1(\theta) + 8F_1(\theta) + 2F_2(\theta) - 3F_1^2(\theta) \tag{6.3.9}$$

and the sector length S_1. *Here we define that*

$$F_2(\theta) = \sum_{i<j}\left\{[\mathrm{tr}(T_{ij}T_{ij}^\top)]^2 + 2\mathrm{tr}(T_{ij}T_{ij}^\top T_{ij}T_{ij}^\top)\right\}, \tag{6.3.10}$$

with the matrix T_{ij} *with the element* $[T_{ij}]_{ab} = \mathrm{tr}(\varrho_{ij}\sigma_a \otimes \sigma_b)$ *for the two-particle reduced state* $\varrho_{ij} = \mathrm{tr}_{\overline{ij}}(\varrho_\theta)$.

Remark 27. The proof of Result 28 is given in Sec. 9.5. As the proof's main idea, we will first evaluate the expectation and then the variance, with the help of results given in formulas in Ref. [6]. Here we would like to especially mention that naively computing $\langle M_4^2\rangle$ directly requires almost ten thousand terms, exactly $(24+16+12+16+24)^2 = 92^2 = 8464$ terms, according to Example 3.28. in Ref. [68]. Instead, we apply the SWAP trick to obtain $\mathrm{tr}[XY^2] = \mathrm{tr}[(XY\otimes Y)\mathbb{S}]$ mentioned the proof of Result 27, and use the fact that the SWAP in many qubits can be decomposed into the SWAP in individual qubits, see Ref. [107].

6.4 Nonlinear Hamiltonian dynamics

Here it should be essential to notice that $(\Delta\theta)_2^2$ in Eq. (6.3.5) results from the two copies of N particles, while $(\Delta\theta)_4^2$ in Eq. (6.3.8) results from the four copies of N particles. To compare both correctly in terms of metrological usefulness, let us introduce the gain relative to the shot-noise limit

$$G_k = \frac{1}{kN(\Delta\theta)_k^2}. \tag{6.4.1}$$

Note that $G_k > 1$ implies the signature of quantum advantage for higher precision.

Here we show several scalings in the proximity of $\theta = 0$ based on our results. For that, we will consider the estimation precision in the limit of $\theta \to 0$. Now, we present the following result:

Result 29. *Consider that*

$$|\psi_\theta\rangle = e^{-i\theta H}|1\rangle^{\otimes N}, \qquad H = J_x^2, \qquad J_x = \frac{1}{2}\sum_{i=1}^{N}\sigma_x^{(i)}. \tag{6.4.2}$$

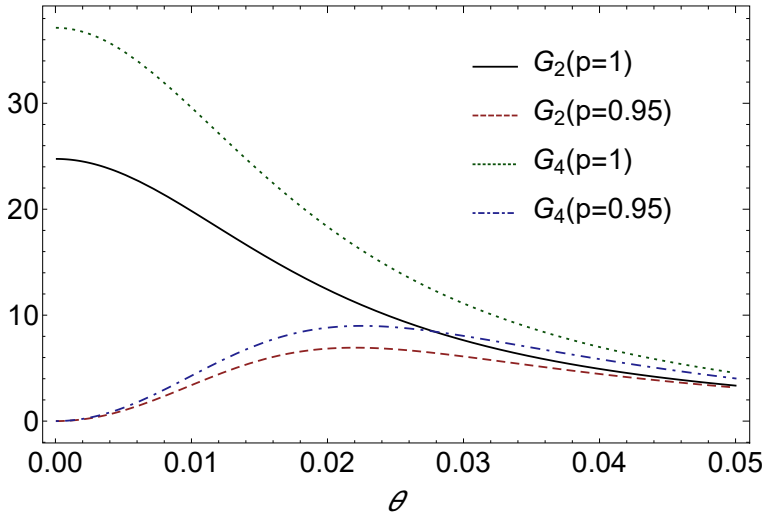

Figure 6.2: Sensitivity of the metrological gain defined in Eq. (6.4.1) to parameter shifts based on Result 29 in $N = 100$, where p denotes the noise parameter in the local depolarizing channel in Eq. (6.5.1).

Then, the gain in Eq. (6.4.1) is obtained as

$$\lim_{\theta\to 0} G_2 = \frac{N-1}{4}, \tag{6.4.3a}$$

$$\lim_{\theta\to 0} G_4 = \frac{3(N-1)}{8}, \tag{6.4.3b}$$

for $k = 2$ and $k = 4$, respectively.

Proof. To prove them, we have to compute all the terms $S_1(\theta), S_2(\theta), F_1(\theta)$, and $F_2(\theta)$. Let us begin by noting that the state $|\psi_\theta\rangle$ is symmetric under exchange for any two qubits. This property enables us to calculate them efficiently. In fact, it is sufficient to focus on one of the marginal reduced two-qubit states and multiply its results by N or $N(N-1)/2$ in the end. With the help of the result in Ref. [532], we can have that

$$S_1(\theta) = N\cos^{2N-2}(\theta), \tag{6.4.4a}$$

$$S_2(\theta) = \frac{N(N-1)}{4}\Big[\cos^{2(N-2)}(2\theta) + 4\sin^2(\theta)\cos^{2N-4}(\theta) + 1\Big]. \tag{6.4.4b}$$

In a similar manner, $F_1(\theta)$ and $F_2(\theta)$ can be calculated. □

Remark 28. The nonlinear Hamiltonian dynamics with $H = J_x^2$ is called the one-axis twisting Hamiltonian. This nonlinear dynamics is known to produce spin squeezing which is metrologically useful entanglement [161, 313] and also many-body Bell correlations [533].

Remark 29. Although the best precision for product states with separable measurements has been shown as $(\Delta\theta)^2 \propto 1/N^3$ [293, 534], our results still have an operational advantage since they are independent of the reference frame independence between separated particles.

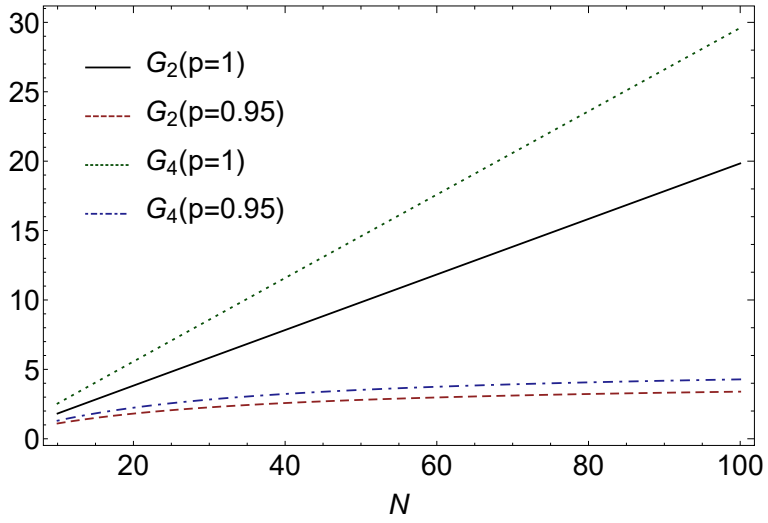

Figure 6.3: Growth in the metrological gains defined in Eq. (6.4.1) for an increasing number of particles based on Result 29 with a fixed $\theta = 1/N$, where p denotes the noise parameter in the local depolarizing channel in Eq. (6.5.1).

Remark 30. Fig. 6.2 compares the sensitivity of both gains to the parameter shift in $N = 100$. Also, Fig. 6.3 illustrates the growth in both gains for increasing particles for fixed $\theta = 1/N$.

6.5 Decoherence

Here we discuss how decoherence can influence metrological gain. As a typical decoherence model, we consider the so-called depolarizing noise channel for a quantum state $\sigma \in \mathcal{H}_d$, see Ref. [19]

$$\mathcal{E}_p(\sigma) = p\sigma + \frac{1-p}{d}\mathbb{1}_d, \tag{6.5.1}$$

where $0 \leq p \leq 1$. In the following, let us discuss a scenario that a pure initial state is transformed by nonlinear unitary dynamics, and then each particle is locally affected by the depolarizing channel with the same local error parameter

$$\Lambda_\theta(\varrho) = \mathcal{E}_p^{\otimes N}(V_\theta \varrho V_\theta^\dagger). \tag{6.5.2}$$

In this scenario, compared to the noiseless case, the S_l and F_l for $l = 1, 2$ in the precision in Eqs. (6.3.5) and (6.3.8) can be changed as

$$S_l(\theta) \to p^{2l} S_l(\theta), \tag{6.5.3a}$$
$$F_l(\theta) \to p^{4l} F_l(\theta). \tag{6.5.3b}$$

In Figs. 6.2 and 6.3, we plot the gains $G_k(p)$ for a noise parameter p of Result 29 and compare the noiseless and a noisy case with $p = 0.95$. In Fig. 6.2,

we can find that the maximal gain in the noisy case cannot be achieved by the limit of $\theta \to 0$ unlike the noiseless case, and the optimal value of θ can be shifted depending on p and N [317, 535].

6.6 Exponential scaling

Here we consider another Hamiltonian dynamics and show that the gain G_k in Eq.(6.4.1) for $k = 2, 4$ scales exponentially, similarly to the example of Roy and Braunstein in Ref. [295]. Here we formulate the exponential scaling:

Result 30. *Consider that* $|\psi_\theta^n\rangle = e^{-i\theta H} |0\rangle^{\otimes N}$ *and* $H = Q_n$ *for* $n = 1, 2$ *such that* $Q_1 + iQ_2 = (\sigma_x + i\sigma_y)^{\otimes N}$. *Then both the gains in Eq. (6.4.1) are given by*

$$\lim_{\theta \to 0} G_2 = \frac{4^N}{N+1}, \tag{6.6.1a}$$

$$\lim_{\theta \to 0} G_4 = \frac{3 \times 2^{2N+1}}{3N+1}. \tag{6.6.1b}$$

We remark that the Hamiltonian Q_1 is the same as the Hermitian operator used in Mermin-type inequalities [116, 536–538]. Our exponential scaling can coincide with the limit proposed by Roy and Braunstein in Ref. [295].

Proof. According to Ref. [295], we have that

$$|\psi_\theta^1\rangle = \cos(\theta') |0\rangle^{\otimes N} - i \sin(\theta') |1\rangle^{\otimes N}, \tag{6.6.2a}$$

$$|\psi_\theta^2\rangle = \cos(\theta') |0\rangle^{\otimes N} + \sin(\theta') |1\rangle^{\otimes N}, \tag{6.6.2b}$$

where $\theta' = 2^{N-1}\theta$. To proceed, we should evaluate all the terms $S_1(\theta), S_2(\theta), F_1(\theta)$, and $F_2(\theta)$. In more general, let us consider the N-qubit asymmetric GHZ state: $|\mathrm{GHZ}_{\alpha,\beta}\rangle = \alpha |0\rangle^{\otimes N} + \beta |1\rangle^{\otimes N}$ for complex coefficients α, β with $|\alpha|^2 + |\beta|^2 = 1$. Since the marginal reduced two-qubit state in any systems $x, y = 1, \ldots, N$ is given by

$$\begin{aligned} \varrho_{xy}^{(2)} &= \mathrm{tr}_{\overline{xy}} \left(|\mathrm{GHZ}_{\alpha,\beta}\rangle \langle \mathrm{GHZ}_{\alpha,\beta}| \right) \\ &= \frac{1}{4} \left\{ \mathbb{1}_2^{\otimes 4} + \Delta[\sigma_z^{(x)} + \sigma_z^{(y)}] + \sigma_z^{(x)} \otimes \sigma_z^{(y)} \right\}, \end{aligned} \tag{6.6.3}$$

with $\Delta = |\alpha|^2 - |\beta|^2$, we can immediately find

$$S_1(\mathrm{GHZ}_{\alpha,\beta}) = N\Delta^2, \tag{6.6.4a}$$

$$S_2(\mathrm{GHZ}_{\alpha,\beta}) = \frac{N(N-1)}{2}, \tag{6.6.4b}$$

$$F_1(\mathrm{GHZ}_{\alpha,\beta}) = N\Delta^4, \tag{6.6.4c}$$

$$F_2(\mathrm{GHZ}_{\alpha,\beta}) = \frac{3N(N-1)}{2}. \tag{6.6.4d}$$

Substituting these into the form in Eq. (6.4.1) and taking the limit $\theta \to 0$, we can complete the proof. □

6.7 Discussions

This Chapter proposed metrological schemes with two and four copies of a quantum state from randomized measurements.We have shown that the quadratic scaling of the estimation precision can be also achieved in our method.

There are several research directions in which our work can be generalized. First, it would be interesting to analytically show several scaling with the nonlinear Hamiltonian $H = J_x^k$ [290, 291, 294]. Second, by the spirit of spin squeezing, finding metrologically-worthwhile uncertainty relations from randomized measurements may give fundamental limitations on precision. Finally, our method may encourage the further development of parameter estimation tasks in terms of multicopy metrology [539, 540], multiparameter scenarios [94, 302–305], or temperature estimation in quantum thermodynamics [310].

Chapter 7

Collective randomized measurements in quantum information processing

This Chapter develops the scheme of randomized measurements in ensembles of particles in the collective rotations. This Chapter presents several criteria for characterizing spin-squeezing entanglement from collective randomized measurements. Also, this Chapter shows that an antisymmetric observable which is invariant under collective rotations is useful to detect the entanglement of phased Dicke states. This Chapter is based on Ref. [10].

7.1 Introduction

The current findings from randomized measurements are not fully comprehensive in several respects. One limitation of the results presented so far is the assumption that local subsystems can be controlled individually. However, this may not be available in an ensemble of quantum particles such as cold atoms [541], trapped ions [542], or Bose-Einstein condensates with spin squeezing [159, 312, 313]. Such quantum systems can be characterized by measuring global quantities such as collective angular momenta [160, 161, 171, 276, 289].

Another practical challenge is that powerful entanglement detection requires many operational resources. For instance, Refs. [1, 255] suggested that at least fourth-order moments are needed to characterize a very weak form of entanglement, known as bound entanglement. Bound entanglement cannot be distilled into pure maximally entangled states [166] and may not be verified by the PPT criterion [194, 195], while it has been shown to be useful for cryptography [232, 233] and metrology [234, 235]. On the other hand, from a practical side, the implementation of higher-order moments may be challenging, because it requires more measurements by Haar random unitaries, which may not be feasible due to the limitations of unitary designs [7, 378, 402, 543].

In this Chapter, we will overcome these issues and propose systematic meth-

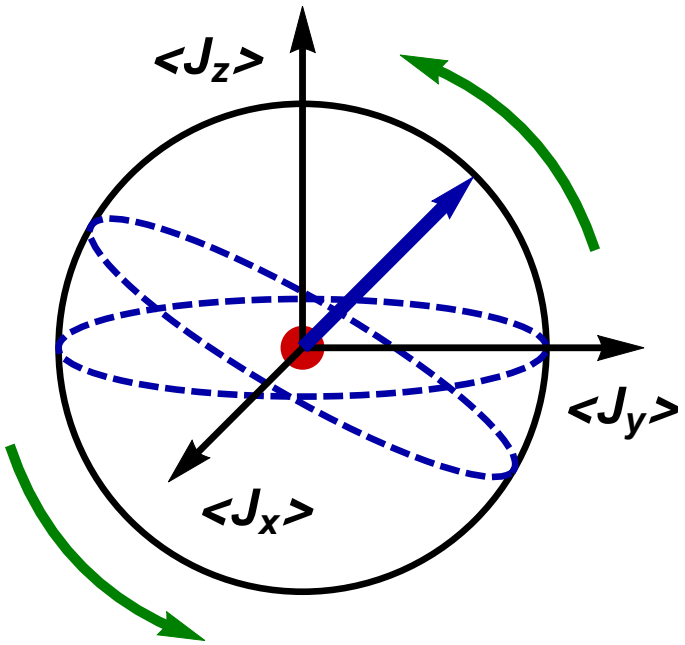

Figure 7.1: Sketch of the collective Bloch sphere with the coordinates $(\langle J_x\rangle, \langle J_y\rangle, \langle J_z\rangle)$. Many-body spin singlet states are represented by a dot at the center (Red), which does not change under any multilateral unitary transformations $U^{\otimes N}$ (Green arrows). Spin measurement in the z-direction is rotated randomly (Blue arrow). This paper proposes systematic methods to characterize spin-squeezing entanglement in an ensemble of particles by rotating a collective measurement direction randomly in this sphere. This figure is taken from Ref. [10].

ods to characterize entanglement in quantum ensembles with limited control over individual systems. The main idea is to perform *collective* random measurements on the quantum system and consider the moments of the resulting distribution. We will apply this idea to different scenarios and present several entanglement criteria.

We first show that spin-squeezing entanglement in permutationally symmetric N-particle systems can be detected in a necessary and sufficient manner. Second, even in non-permutationally symmetric cases, we demonstrate that the second-order moment can characterize multiparticle bound entanglement. Third, we further introduce a criterion to certify multiparticle bound entanglement with antisymmetric correlations via third-order moments. Finally, we generalize the method to verify entanglement between spatially-separated two quantum ensembles.

7.2 Collective randomized measurements

Consider a quantum ensemble that consists of N spin-$\frac{1}{2}$ particles, denoted by $\varrho \in \mathcal{H}_2^{\otimes N}$.Suppose that each particle in this ensemble cannot be controlled individually, and one can instead measure the collective angular momentum

$$J_l = \frac{1}{2}\sum_{i=1}^{N} \sigma_l^{(i)}, \tag{7.2.1}$$

with Pauli-l spin matrices $\sigma_l^{(i)}$ for $l = x, y, z$ acting on i-th subsystem.

Let us perform measurements with J_z and rotate the collective direction in an arbitrary manner. We introduce an expectation value and its variance according to a random unitary:

$$\langle J_z \rangle_U = \mathrm{tr}\left[\varrho U^{\otimes N} J_z (U^\dagger)^{\otimes N}\right], \tag{7.2.2a}$$

$$(\Delta J_z)_U^2 = \langle J_z^2 \rangle_U - \langle J_z \rangle_U^2. \tag{7.2.2b}$$

These depend on the choice of collective simultaneous multilateral unitary operations $U^{\otimes N}$. Now we define a linear function as

$$f_U(\varrho) = \alpha (\Delta J_z)_U^2 + \beta \langle J_z \rangle_U^2 + \gamma, \tag{7.2.3}$$

where α, β, γ are real constant parameters. The function $f_U(\varrho)$ can be measured experimentally and each parameter can be made artificially in the post-processing.

Now the key idea to detect entanglement in ϱ is to take a sample over collective local unitaries and consider the r-th moments of the resulting distribution

$$\mathcal{J}^{(r)}(\varrho) = \int dU \, [f_U(\varrho)]^r, \tag{7.2.4}$$

where the integral is taken according to the Haar measure. This collective unitary transformation can be written as $U^{\otimes N} = e^{i\boldsymbol{u}\cdot\boldsymbol{J}}$, where $\boldsymbol{u} = (u_x, u_y, u_z)$ is a three-dimensional unit vector and $\boldsymbol{J} = (J_x, J_y, J_z)$ is a vector of collective angular momenta. The randomization of Haar collective unitaries corresponds to the uniform randomization over the three-dimensional sphere in the coordinates $(\langle J_x \rangle, \langle J_y \rangle, \langle J_z \rangle)$. This sphere is known as the *collective Bloch sphere* [123, 161, 171] in an analogy of the standard Bloch sphere in a single-qubit system, illustrated in Fig. (7.1). Similar randomization strategies have already been discussed in Refs. [325, 326], but the detectable states are limited only to Dicke states.

It is essential that by definition, the moments are *invariant* under any collective local unitary transformation

$$\mathcal{J}^{(r)}\left[V^{\otimes N} \varrho (V^\dagger)^{\otimes N}\right] = \mathcal{J}^{(r)}(\varrho), \tag{7.2.5}$$

for a collective local unitary $V^{\otimes N}$ for 2×2 unitaries V. In the following, we will discuss entanglement detection based on the moments $\mathcal{J}^{(r)}$.

7.3 Permutationally symmetric state

To proceed, let us recall that a N-qubit state ϱ is called *permutationally symmetric (bosonic)* if it satisfies

$$P_{ab}\varrho = \varrho P_{ab} = \varrho, \tag{7.3.1}$$

for all $a, b \in \{1, 2, \ldots, N\}$ with $a \neq b$. Here P_{ab} is an orthogonal projector onto the so-called symmetric subspace that remains invariant under all the permutations. Note that P_{ab} can be written as $P_{ab} = (\mathbb{1} + \mathbb{S}_{ab})/2$ with the SWAP (flip) operator $\mathbb{S}_{ab} = \sum_{i,j} |ij\rangle\langle ji|$ that can exchange qubits a, b: $\mathbb{S}\,|a\rangle \otimes |b\rangle = |b\rangle \otimes |a\rangle$.

There are many studies on the entanglement of permutationally symmetric states in Refs. [89, 187, 198, 323, 328–330]. In general, a state ϱ is said to contain entanglement if it cannot be written as the fully separable state

$$\varrho_{\mathrm{fs}} = \sum_k p_k \varrho_k^{(1)} \otimes \cdots \otimes \varrho_k^{(N)}, \tag{7.3.2}$$

where the p_k form a probability distribution. In particular, a permutationally symmetric state ϱ is said to possess bipartite entanglement or often called *spin-squeezed* if a two-particle reduced state $\varrho_{ab} = \mathrm{tr}_{(a,b)^c}(\varrho)$ is entangled for all pairs (a, b) with the complement $(a, b)^c$. In previous works [135, 331, 332], such spin-squeezing entanglement has been completely characterized in a *necessary and sufficient* manner. On the other hand, they should require optimizations over measurement directions for a given state.

In the following, we will show that the collective randomized measurement scheme can reach the same conclusion without such an optimization. Now we can formulate the first main result of this Chapter:

Result 31. *For a N-qubit permutationally symmetric state ϱ, the first, second, and third moments $\mathcal{J}^{(r)}(\varrho)$ for $r = 1, 2, 3$ allows us to achieve the necessary and sufficient criterion for spin-squeezing entanglement, where $\alpha = 2/N_2$, $\beta = -2(N-2)/(NN_2)$, $\gamma = -1/[2(N-1)]$ and $N_2 = N(N-1)$.*

Remark 31. The proof of this Result is given below, and the technical calculation is shown in Sec. 9.6. As the proof's main idea, we will first explain that the necessary and sufficient condition is equivalent to the violation of $C \geq 0$ for the covariance matrix $C_{ij} = \langle \sigma_i \otimes \sigma_j \rangle_{\varrho_{ab}} - \langle \sigma_i \rangle_{\varrho_a} \langle \sigma_j \rangle_{\varrho_b}$, with the reduced state ϱ_{ab} for any choice a, b, for details, see Refs. [198, 199, 544]. Then we will analytically show that the violation can be accessible from the moments $\mathcal{J}^{(r)}(\varrho)$ for $r = 1, 2, 3$.

Remark 32. We remark that any N-qubit permutationally symmetric state can be given by a density matrix in the Dicke basis. Then mixed states of Dicke, W, and GHZ states are permutationally symmetric. Also, it is worthwhile to note that any N-particle permutationally symmetric state can be either fully separable or genuinely multipartite entangled (GME) [328, 330], where GME states cannot be written in any separable form for all bipartitions. Accordingly, Result 31 allows for the GME detection in a collective-reference-frame-independent manner.

Proof. In the following, we will first describe the logic of how to prove Result 31 and explain each line step-by-step

$$\begin{aligned}
\varrho_{\mathrm{PS}} \in \mathcal{H}_2^{\otimes N} \text{ is spin squeezed} &\iff \varrho_{ab} \in \mathcal{H}_2^{\otimes 2} \text{ is entangled} && \text{(7.3.3a)}\\
&\iff \varrho_{ab} \notin \mathrm{PPT} && \text{(7.3.3b)}\\
&\iff M \ngeq 0 && \text{(7.3.3c)}\\
&\iff C \ngeq 0 && \text{(7.3.3d)}\\
&\iff \text{obtained from } \mathrm{tr}(C^r) \text{ for } r = 1,2,3 && \text{(7.3.3e)}\\
&\iff \text{obtained from } \mathcal{C}^{(r)}(\varrho) \text{ for } r = 1,2,3 && \text{(7.3.3f)}\\
&\iff \text{obtained from } \mathcal{J}^{(r)}(\varrho) \text{ for } r = 1,2,3. && \text{(7.3.3g)}
\end{aligned}$$

In the first line, we denote a N-qubit permutationally symmetric state as ϱ_{PS} and recall again that it possesses bipartite entanglement or often spin squeezing if and only if any two-qubit reduced state $\varrho_{ab} = \mathrm{tr}_{(a,b)^c}(\varrho_{\mathrm{PS}})$ is entangled for $a, b = 1, 2, \ldots, N$, where X^c is the complement of a set X. This has been already discussed in Refs. [135, 331, 332]. In the second line, we also recall that any two-qubit state is entangled if and only if it has a negative eigenvalue under partial transposition, that is, it violates the so-called PPT criterion [194, 195].

In the third line, we first recall that any two-qubit state ϱ_{ab} can be written as

$$\varrho_{ab} = \frac{1}{4} \sum_{i,j=0}^{3} m_{ij} \sigma_i \otimes \sigma_j. \tag{7.3.4}$$

Here we note that a two-qubit state ϱ_{ab} is permutationally symmetric and separable if and only if it holds that $M \geq 0$, where $M = (m_{ij})$ for $i, j = 0, 1, 2, 3$. In the fourth line, this separability condition is equivalent to $C \geq 0$ for a permutationally symmetric ϱ_{ab}. Here the 3×3 matrix $C = (C_{ij})$ is the Schur complement of the 4×4 matrix M, which is given by $C_{ij} = m_{ij} - m_{i0} m_{0j}$ for $i, j = 1, 2, 3$ since $m_{00} = 1$. For details, see Refs. [198, 199, 544].

In the fifth line, we first discuss the explicit form of the covariance matrix C

$$C_{ij} = \mathrm{tr}[\varrho_{ab} \sigma_i \otimes \sigma_j] - \mathrm{tr}[\varrho_a \sigma_i] \mathrm{tr}[\varrho_b \sigma_j] = t_{ij} - a_i a_j, \tag{7.3.5}$$

where $m_{ij} = t_{ij} = t_{ji}$ and $m_{i0} = m_{0i} = a_i$ since ϱ_{ab} is permutationally symmetric. Then, the covariance matrix $C = T - \boldsymbol{a}\boldsymbol{a}^\top$ is symmetric $C = C^\top$, where $T = (t_{ij}) = T^\top$ with the constraint $\mathrm{tr}[T] = \sum_i t_{ii} = 1$ and $\boldsymbol{a} = (a_x, a_y, a_z)$. To proceed, let us remark that the matrix C can be diagonalized by a collective local unitary transformation $V \otimes V$, leads to that

$$OCO^\top = \mathrm{diag}(c_1, c_2, c_3), \tag{7.3.6}$$

with a rotation matrix $O \in SO(3)$. In fact, the eigenvalues c_1, c_2, c_3 can be found by computing the roots of the characteristic polynomial

$$p_C(\lambda) = \lambda^3 - \mathrm{tr}(C)\lambda^2 + \frac{1}{2}\left[\mathrm{tr}(C)^2 - \mathrm{tr}(C^2)\right]\lambda - \det(C), \tag{7.3.7}$$

where $\mathrm{tr}(C^r) = \sum_{i=1,2,3} c_i^r$ and the $\det(C)$ can be written as

$$\det(C) = \frac{1}{6}\left[\mathrm{tr}(C)^3 - 3\mathrm{tr}(C)\mathrm{tr}(C^2) + 2\mathrm{tr}(C^3)\right]. \tag{7.3.8}$$

That is, knowing the $\mathrm{tr}[C^r]$ for $r = 1, 2, 3$ can enable us to access its eigenvalues and therefore decide whether the matrix C is positive or negative.

In the sixth and seventh lines, it is sufficient to show that $\mathrm{tr}[C^r]$ for $r = 1, 2, 3$ can be obtained from the moments $\mathcal{J}^{(r)}(\varrho)$ in the collective randomized measurements. For the choice $\alpha = 2/N_2$, $\beta = -2(N-2)/(NN_2)$, $\gamma = -1/[2(N-1)]$, and $N_2 = N(N-1)$, we immediately find that the moments $\mathcal{J}^{(r)}(\varrho)$ can be equal to the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ of the random covariance matrix

$$\mathcal{J}^{(r)}(\varrho) = \mathcal{C}^{(r)}(\varrho_{ab}) \equiv \int dU \, [\mathrm{Cov}_U]^r, \tag{7.3.9a}$$

$$\mathrm{Cov}_U = \mathrm{tr}[\varrho_{ab} U^{\otimes 2} \sigma_z \otimes \sigma_z (U^\dagger)^{\otimes 2}] - \mathrm{tr}[\varrho_a U \sigma_z U^\dagger]\mathrm{tr}[\varrho_b U \sigma_z U^\dagger]. \tag{7.3.9b}$$

This results from the fact that

$$\langle J_z \rangle_U = \frac{N}{2}\mathrm{tr}[\varrho_a U \sigma_z U^\dagger], \tag{7.3.10}$$

$$\langle J_z^2 \rangle_U = \frac{N}{4} + \frac{N(N-1)}{2}\mathrm{tr}[\varrho_{ab} U^{\otimes 2} \sigma_z \otimes \sigma_z (U^\dagger)^{\otimes 2}]. \tag{7.3.11}$$

In Sec. 9.6, we will evaluate the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ and show that they are associated with $\mathrm{tr}[C^r]$. □

7.4 Multiparticle bound entanglement

Next, let us consider the more general case where ϱ is not permutationally symmetric. Even in this case, we will show that our approach with collective randomized measurements is still effective for detecting spin-squeezing entanglement. Now we can make the second result in this Chapter:

Result 32. *For a N-qubit state ϱ, the first moment $\mathcal{J}^{(1)}$ with $(\alpha, \beta, \gamma) = (3, 0, 0)$ can be given by*

$$\mathcal{J}^{(1)}(\varrho) = \sum_{l=x,y,z} (\Delta J_l)^2. \tag{7.4.1}$$

Any N-qubit fully separable state obeys

$$\mathcal{J}^{(1)}(\varrho) \geq \frac{N}{2}. \tag{7.4.2}$$

This violation implies the presence of multipartite entanglement.

Remark 33. The proof of this Result is given in Sec. 9.7. The criterion in Eq. (7.4.2) itself was already established [315], so we only have to show the derivation of Eq. (7.4.1) in the proof.

Remark 34. The criterion in Eq. (7.4.2) can be maximally violated by the so-called many-body spin singlet states ϱ_{singlet} [160, 275, 276, 315–317, 545, 546] and see Sec. 1.3.

Remark 35. Note that other quantum states can also be at the centre. Such states can be changed under $U^{\otimes N}$, but their expectations of J_l cannot be changed. Examples are the thermal states of several spin-chain models. These can be characterized by Result 32, see [160, 276].

Remark 36. Moreover, the violation of Eq. (7.4.2) is known to detect entanglement very strongly. In fact, it can verify the so-called multiparticle bound entangled states, which cannot be distilled into pure entangled states and can be PPT for all bipartitions [160, 276]. In the previous results in randomized measurements, bipartite bound entanglement has been detected using at least fourth-order moments [1, 255], while Result 32 only requires evaluating second-order Haar integrals in the collective Bloch sphere. This fact can reduce a large amount of measurement resources in practice.

Remark 37. As a further utility of Result 32, Refs. [318, 319] showed that it can detect many-body Bell nonlocality. Also, Refs. [170, 176, 320] discussed the improvement of the average sensitivity of phase estimation in quantum metrology. Below, we will generalize Result 32 to high-dimensional spin systems. This allows us to characterize bound entanglement and k-particle entanglement in spin-squeezed states [321, 322].

Remark 38. Finally, we remark that the criterion in Eq. (7.4.2) is known as one of the optimal inequalities to detect spin-squeezing entanglement [160, 276]. This optimality means a state that is not detected by the inequalities cannot be distinguished from a fully separable state by knowing the values of $\langle J_l \rangle$ and $(\Delta J_l)^2$ only for the three orthogonal directions $l = x, y, z$ for the case of large N. In fact, combining all the optimal inequalities can characterize spin-squeezing entanglement very efficiently, while some entangled states cannot be detected in this way.

Here we consider the generalization of Result 32 to high-dimensional spin systems. For that, let us denote the N-qudit collective operators

$$\Lambda_l = \frac{1}{d} \sum_{i=1}^{N} \lambda_l^{(i)}, \tag{7.4.3}$$

with the so-called Gell-Mann matrices $\lambda_l^{(i)}$ for $l = 1, 2, \ldots, d^2 - 1$ acting on i-th system. The Gell-Mann matrices are d-dimensional extensions of Pauli matrices satisfying the properties: $\lambda_l^\dagger = \lambda_l, \text{tr}(\lambda_l) = 0, \text{tr}(\lambda_k \lambda_l) = d\delta_{kl}$. For details, see [25–28]. Let us define the random expectation and its variance

$$\langle \Lambda_l \rangle_U = \text{tr}[\varrho U^{\otimes N} \Lambda_l (U^\dagger)^{\otimes N}], \qquad (\Delta \Lambda_l)_U^2 = \langle \Lambda_l^2 \rangle_U - \langle \Lambda_l \rangle_U^2, \tag{7.4.4}$$

which depends on the choice of collective unitaries $U^{\otimes N}$ with $U \in \mathcal{U}(d)$. Now we introduce the average of $(\Delta \Lambda_l)_U^2$ for any l over Haar random unitaries

$$\mathcal{D}(\varrho) = (d^2 - 1) \int dU \, (\Delta \Lambda_l)_U^2. \tag{7.4.5}$$

Now we can make the following:

Result 33. *For a N-qudit state ϱ, the average can be given by*

$$\mathcal{D}(\varrho) = \sum_{l=1}^{d^2-1} (\Delta\Lambda_l)^2. \tag{7.4.6}$$

Any N-qudit fully separable state obeys

$$\sum_{l=1}^{d^2-1} (\Delta\Lambda_l)^2 \geq \frac{N(d-1)}{d}. \tag{7.4.7}$$

This violation implies the presence of multipartite entanglement.

Remark 39. This proof is given in Sec. 9.7 and this result is the generalization of Result 32. The fully separable bound was already discussed in Refs. [321, 322].

7.5 Antisymmetric entanglement

We have considered the collective randomized measurements based on the function $f_U(\varrho)$ in Eq. (7.2.3) including $\langle J_z^2 \rangle_U$, so the detectable spin-squeezing entanglement may have large two-body correlations. Now a natural question arises: Can we extend this framework to incorporate k-body correlations for $k \geq 3$?

On the side of standard randomized measurements, the so-called sector length can be accessible as a tool to detect entanglement, which can quantify the amount of k-body quantum correlations for $1 \leq k \leq N$ discussed in Eq. (1.4.7). Apart from randomized measurements, similar questions have already been addressed to characterize such higher-order spin-squeezing entanglement on permutationally symmetric systems [135, 160, 276, 332, 420].

To proceed, let us begin by considering the three-qubit observable

$$\mathcal{S}(\sigma_x \otimes \sigma_y \otimes \sigma_z) \equiv \sigma_x \otimes \sigma_y \otimes \sigma_z + \sigma_y \otimes \sigma_z \otimes \sigma_x + \cdots, \tag{7.5.1}$$

where $\mathcal{S}$ denotes the average over all permutations of indices x, y, z. This observable is invariant under any particle exchange: $P_{ab}\,\mathcal{S}(\sigma_x \otimes \sigma_y \otimes \sigma_z)\,P_{ab} = \mathcal{S}(\sigma_x \otimes \sigma_y \otimes \sigma_z)$, with P_{ab} being the projector onto the symmetric subspace for any a, b. The N-qubit extension of this observable can be represented by the product of collective angular momenta

$$\mathcal{O}_{\mathcal{S}} \equiv \sum_{i<j<k} \mathcal{S}\left(\sigma_x^{(i)} \otimes \sigma_y^{(j)} \otimes \sigma_z^{(k)}\right) = \frac{8}{3!}\mathcal{S}(J_x J_y J_z), \tag{7.5.2}$$

where $\mathcal{S}(J_x J_y J_z) = J_x J_y J_z + J_y J_z J_x + J_z J_x J_y + \cdots$ and $P_{ab}\mathcal{O}_{\mathcal{S}}P_{ab} = \mathcal{O}_{\mathcal{S}}$. In general, any combination of products of collective angular momenta remains permutationally invariant under particle exchange [547].

An associated operator with $\mathcal{O}_S$ from Eq. (7.5.2) is the antisymmetric observable

$$\mathcal{O}_{\mathcal{A}} \equiv \sum_{i<j<k} \mathcal{A}\left(\sigma_x^{(i)} \otimes \sigma_y^{(j)} \otimes \sigma_z^{(k)}\right), \tag{7.5.3}$$

where $\mathcal{A}(\sigma_x \otimes \sigma_y \otimes \sigma_z)$ denotes the antisymmetrization of $\sigma_x \otimes \sigma_y \otimes \sigma_z$ by taking the sum over even permutations and subtracting the sum over odd permutations of indices x, y, z. Importantly, the observable $\mathcal{O}_{\mathcal{A}}$ lives in the antisymmetric subspace of the operator space, which does not overlap with the symmetric subspace. That is, $\mathcal{O}_{\mathcal{A}}$ cannot be constructed from collective angular momenta.

We have seen that symmetric observables based on collective angular momenta can detect symmetric entanglement in the collective randomized measurement. Then, one may wonder if antisymmetric observables such as $\mathcal{O}_{\mathcal{A}}$ can characterize antisymmetric entanglement. Similarly to Eq. (7.2.4), we define the average over random collective local unitary

$$\mathcal{T}(\varrho) = \int dU \, \mathrm{tr}\left[\varrho U^{\otimes N} \mathcal{O}_{\mathcal{A}} (U^\dagger)^{\otimes N}\right]. \tag{7.5.4}$$

Here we can formulate the third result in this Chapter:

Result 34. *The average $\mathcal{T}(\varrho)$ can be given by*

$$\mathcal{T}(\varrho) = \mathrm{tr}[\varrho \mathcal{O}_{\mathcal{A}}] = \sum_{i<j<k} \sum_{a,b,c} \varepsilon_{abc} \langle \sigma_a^{(i)} \otimes \sigma_b^{(j)} \otimes \sigma_c^{(k)} \rangle_\varrho, \tag{7.5.5}$$

where we denote ε_{abc} as the Levi-Civita symbol for $a, b, c = x, y, z$. Any N-qubit fully separable state may obey a certain bound

$$|\mathcal{T}(\varrho)| \leq p_{fs}^{(N)}. \tag{7.5.6}$$

This violation implies the presence of multipartite entanglement.

Remark 40. The derivation of Eq. (7.5.5) is given in Sec. 9.8. Here we explain how to derive the bound $p_{\mathrm{fs}}^{(N)}$. First, we note that the average $|\mathcal{T}(\varrho)|$ is a convex function of a quantum state. Then it is enough to maximize the average for all N-qubit pure fully separable states:

$$|\Phi_{\mathrm{fs}}\rangle = \bigotimes_{i=1}^{N} |\chi_i\rangle. \tag{7.5.7}$$

Each of single-qubit states $|\chi_i\rangle$ can be mapped into points on the surface in the single-qubit Bloch sphere, which can be parameterized as

$$\langle \sigma_x \rangle_{\chi_i} = \cos(\theta_i), \quad \langle \sigma_y \rangle_{\chi_i} = \sin(\theta_i)\cos(\phi_i), \quad \langle \sigma_z \rangle_{\chi_i} = \sin(\theta_i)\sin(\phi_i), \tag{7.5.8}$$

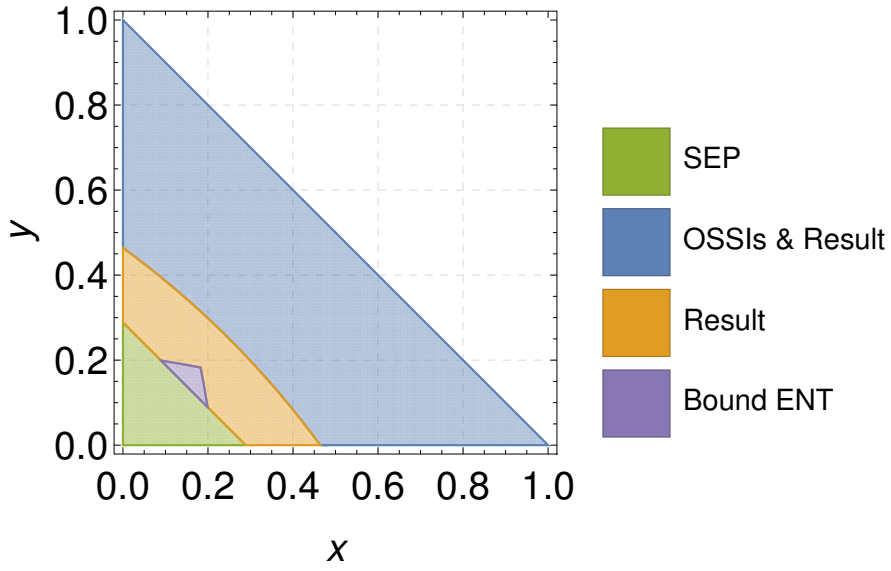

Figure 7.2: Entanglement criteria for the mixed state in Eq. (7.5.11) for $N = 3$ in the $x - y$ plane. The fully separable states are contained in Green area, which obeys all the optimal spin-squeezing inequalities (OSSIs) previously known [160, 276] and also our criterion in Result 34. Blue area corresponds to the spin-squeezed entangled states that can be detected by all OSSIs and Result 34. Yellow and Purple areas correspond to the entangled states that cannot be detected by all OSSIs but can be detected by Result 34, thus marking the improvement of this Chapter compared with previous results. In particular, Purple area corresponds to the multiparticle bound entangled states that are not detected by the PPT criterion for all bipartitions but detected by Result 34. This figure is taken from Ref. [10].

for $\chi_i = |\chi_i\rangle\langle\chi_i|$. Substituting these expressions into $|\mathcal{T}(\varrho)|$ and performing its maximization over parameters, we can find the bound $p_{\text{fs}}^{(N)}$. From numerical research, we collect much evidence that there may exist the tight bound

$$p_{\text{fs}}^{(N)} \stackrel{!}{=} \frac{N^2 \cot\left(\frac{\pi}{N}\right)}{3\sqrt{3}}, \tag{7.5.9}$$

which may be obtained by

$$\theta_i = 2\tan^{-1}\left(\sqrt{2-\sqrt{3}}\right), \qquad \phi_i = \frac{2\pi i}{N}, \qquad \text{for } i = 1, 2, \ldots, N. \tag{7.5.10}$$

We illustrate the geometrical expressions of these points $|\chi_i\rangle$ in the single-qubit Bloch sphere.

Let us test our criterion with the two-parameter family of states

$$\varrho_{x,y} = x\,|\zeta_N\rangle\langle\zeta_N| + y\,|\tilde{\zeta}_N\rangle\langle\tilde{\zeta}_N| + \frac{1-x-y}{2^N}\mathbb{1}_2^{\otimes N}, \tag{7.5.11}$$

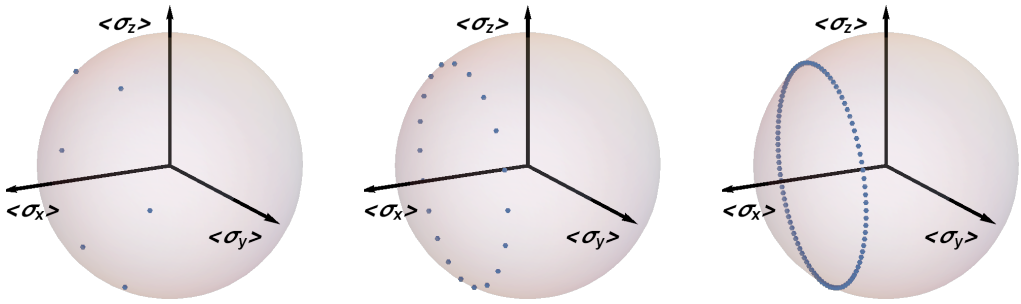

Figure 7.3: Geometry of N single-qubit states $|\chi_i\rangle$ represented as (Blue) points on the surface in the single-qubit Bloch sphere, for $i = 1, 2, \ldots N$ and $N = 6, 20, 100$. This figure is taken from Ref. [10].

where $0 \leq x, y \leq 1$. Here $|\zeta_N\rangle$ is the so-called phased Dicke state [147–152], up to normalization,

$$|\zeta_N\rangle \propto \sum_{k=1}^{N} e^{2\pi ik/N} |0\rangle_1 |0\rangle_2 \cdots |1\rangle_k \cdots |0\rangle_{N-1} |0\rangle_N , \tag{7.5.12}$$

and the state

$$|\tilde{\zeta}_N\rangle = \sigma_x^{\otimes N} |\zeta_N\rangle , \qquad \langle \zeta_N | \tilde{\zeta}_N \rangle = 0. \tag{7.5.13}$$

Note that the phased Dicke state is not equivalent to the Dicke state under collective unitary transformations. In Fig. 7.2, we illustrate the criterion of Result 34 for the state $\varrho_{x,y}$ for $N = 3$ on the $x - y$ plane. Our result allows us to detect entanglement undetected not only for Eq. (7.4.2) but also for all the other optimal spin-squeezing inequalities previously known [160, 276]. Moreover, multipartite bound entanglement of $\varrho_{x,y}$ can be also detected.

Remark 41. The inequality (7.5.6) can be maximally violated by several GME states. For small N, we have numerically confirmed that the states $|\zeta_N\rangle$ or $|\tilde{\zeta}_N\rangle$ can reach the maximal violation, since they can be the eigenstates with maximal/minimal eigenvalues of the antisymmetric observable $\mathcal{O}_A$. For cases with $N = 3, 4, 5, 6$, the matrix rank of $\mathcal{O}_\mathcal{A}$ is respectively given by $4, 6, 24, 38$.

Remark 42. Also, we can show that there exist three-qubit GME states that cannot be detected by all the optimal spin-squeezing inequalities. Such GME states violate the biseparable bound $|\mathcal{T}| \leq 2$, analytically shown in Result 36.

Remark 43. In Fig. 7.3, we illustrate the geometrical expressions of the points $|\chi_i\rangle$ on the surface in the single-qubit Bloch sphere for $N = 6, 20, 100$.

Remark 44. In Fig. 7.4, we illustrate the criterion of Result 34 for the state $\varrho_{x,y}$ in Eq. (7.5.11) for $N = 4, 5, 6$ on the $x - y$ plane.

Let us generalize Result 34 by focusing only on three-particle systems. We begin by denoting three-particle d-dimensional (three-qudit) operator as

$$W_S = \sum_{i,j,k} w_{ijk} s_i \otimes s_j \otimes s_k, \tag{7.5.14}$$

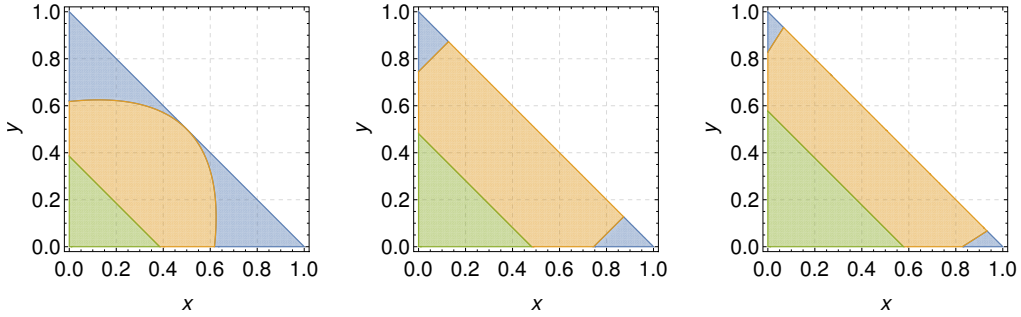

Figure 7.4: Entanglement criteria for the mixed state in Eq. (7.5.11) for $N = 4, 5, 6$ in the $x - y$ plane. The fully separable states are contained in Green area, which obeys all the optimal spin-squeezing inequalities (OSSIs) previously known [160, 276] and also our criterion in Result 34. Blue area corresponds to the spin-squeezed entangled states that can be detected by all OSSIs and Result 34. Yellow area corresponds to the entangled states that cannot be detected by all OSSIs but can be detected by Result 34, thus marking the improvement of this Chapter compared with previous results. This figure is taken from Ref. [10].

for some given three-fold tensor w_{ijk} and matrices $s_i \in \mathcal{H}_d$ with $s_i \neq \mathbb{1}_d$. If $d = 2$, $w_{ijk} = \varepsilon_{ijk}$, and $s_i = \sigma_i$, then it holds that $|\langle W_S \rangle| = |\mathcal{T}|$. To proceed, we recall that a three-particle state is called biseparable if

$$\varrho_{\text{bs}} = \sum_k p_k^A \varrho_k^A \otimes \varrho_k^{BC} + \sum_k p_k^B \varrho_k^B \otimes \varrho_k^{CA} + \sum_k p_k^C \varrho_k^C \otimes \varrho_k^{AB}, \tag{7.5.15}$$

where and p_k^X for $X = A, B, C$ are probability distributions. The state is called genuinely multiparticle entangled if it cannot be written in the form of ϱ_{bs}. Now we will make the following:

Result 35. *For a three-qudit state ϱ_{ABC}, we denote the vector $\boldsymbol{s}_X = (s_i^X)$ and the matrix $S_{XY} = (s_{ij}^{XY})$ with $s_i^X = \text{tr}[\varrho^X s_i]$ and $s_{ij}^{XY} = \text{tr}[\varrho^{XY} s_i \otimes s_j]$, where ϱ_X, ϱ_{XY} are marginal reduced states of ϱ_{ABC} for $X, Y, Z = A, B, C$. Any three-qudit fully separable state obeys*

$$|\langle W_S \rangle| \leq \max_{X,Y,Z=A,B,C} \|\boldsymbol{s}_X\| \, \|\boldsymbol{v}_{YZ}\| \,, \tag{7.5.16}$$

where $\|\boldsymbol{v}\|^2 = \sum_i v_i^2$ is the Euclidean vector norm of a vector $\boldsymbol{v}$ with elements v_i and the vector $\boldsymbol{v}_{YZ} = (v_i^{YZ})$ with $v_i^{YZ} = \sum_{j,k} s_j^Y s_k^Z w_{ijk}$. Also, any three-qudit biseparable state obeys

$$|\langle W_S \rangle| \leq \max_{X,Y,Z=A,B,C} \sum_i \sigma_i(S_{XY}) \sigma_i(Z^*), \tag{7.5.17}$$

where $\sigma_i(O)$ are singular values of a matrix O in decreasing order and the matrix $Z^* = (z_{ij}^*)$ with $z_{ij}^* = \sum_k s_k^Z w_{ijk}$.

Proof. Since $|\langle W_S\rangle|$ is a convex function for a state, it is sufficient to prove the cases of pure states. First, let us consider a pure fully separable state $\varrho^A \otimes \varrho^B \otimes \varrho^C$. Then we have

$$\begin{aligned}\langle W_S\rangle &= \sum_{i,j,k} w_{ijk} \mathrm{tr}[\varrho^A \otimes \varrho^B \otimes \varrho^C s_i \otimes s_j \otimes s_k] \\ &= \sum_i s_i^A \sum_{j,k} s_j^B s_k^C w_{ijk} \\ &= \sum_i s_i^A v_i^{BC} \\ &\leq \|\boldsymbol{s}_A\| \, \|\boldsymbol{v}_{BC}\| \,, \end{aligned} \tag{7.5.18}$$

where we used the Cauchy–Schwarz inequality to derive the inequality. Similarly, we can have cases that correspond to $\boldsymbol{s}_B$ and $\boldsymbol{s}_C$.

Second, let us consider a pure biseparable state for a fixed bipartition $XY|Z$. For a case $AB|C$, we have

$$\begin{aligned}\langle W_S\rangle &= \sum_{i,j} s_{ij}^{AB} \sum_k s_k^C w_{ijk} \\ &= \sum_{i,j} s_{ij}^{AB} c_{ij}^* \\ &= \mathrm{tr}[S_{AB} (C^*)^\top] \\ &\leq \sum_i \sigma_i(S_{AB}) \sigma_i(C^*), \end{aligned} \tag{7.5.19}$$

where we used von Neumann's trace inequality [548]. Similarly, we can obtain the bounds for the other bipartitions $B|CA$ and $C|AB$. Hence we can complete the proof. □

As a corollary, we obtain the following:

Result 36. *Consider the case where $d = 2$, $w_{ijk} = \varepsilon_{ijk}$, and $s_i = \sigma_i$. Any three-qubit fully separable state obeys $|\langle W_S\rangle| \leq 1$. Also, any three-qubit biseparable state obeys $|\langle W_S\rangle| \leq 2$.*

Proof. To show these, without loss of generality, we can take $\varrho^C = |0\rangle\langle 0|$. This can lead to that $\boldsymbol{v}_{BC} = (s_2^B, -s_1^B, 0)$. For single-qubit pure states, we have that $\|\boldsymbol{s}_A\| = 1$ and $\|\boldsymbol{v}_{BC}\| \leq 1$. Thus we can show the the fully separable bound. For the biseparable bound, since $\sigma_1(C^*) = \sigma_2(C^*) = 1$ and $\sigma_3(C^*) = 0$, we can immediately find that $\sigma_1(S_{AB}) + \sigma_2(S_{AB}) \leq 2$ for all pure ϱ^{AB}. □

7.6 Entanglement between two ensembles

Finally, let us apply the strategy of collective randomized measurements to another scenario where two ensembles are spatially separated [549–554]. We denote ϱ_{AB} as a $2N$-qubit state that contains the two ensembles of N spin-$\frac{1}{2}$ particles, where

$$\varrho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B, \quad \text{with } \mathcal{H}_X = \mathcal{H}_2^{\otimes N}, \tag{7.6.1}$$

for $X = A, B$. Supposing that each ensemble can be controlled individually, we can perform the collective randomized measurements to obtain the moments $\mathcal{J}_X^{(r)}$ with a fixed choice (α, β, γ).

The total collective observables are given by

$$J_l^{\pm} = J_{l,A} \pm J_{l,B}, \tag{7.6.2}$$

where

$$J_{l,X} = \frac{1}{2} \sum_{i=1}^{N} \sigma_l^{(X_i)} \in \mathcal{H}_X, \quad \text{for } l = x, y, z, \tag{7.6.3}$$

with Pauli matrices $\sigma_l^{(X_i)}$ acting on X_i-th subsystem in the ensemble $X = A, B$. In a similar manner to Eq. (7.2.2b), we can introduce the random variances $(\Delta J_z^{\pm})^2_{U_{AB}}$ with $U_{AB} = U_A \otimes U_B$. Denoting the gap as

$$\eta_{U_{AB}} \equiv (\Delta J_z^{+})^2_{U_{AB}} - (\Delta J_z^{-})^2_{U_{AB}}, \tag{7.6.4}$$

let us consider its moment

$$\mathcal{G}_{AB}^{(r)} = g \int dU_{AB} \, [\eta_{U_{AB}}]^r, \tag{7.6.5}$$

where g is a real constant parameter.

Now we can present the following criterion:

Result 37. *For a $2N$-qubit state ϱ_{AB} consisting of the two ensembles of N spin-$\frac{1}{2}$ particles, if each ensemble is permutationally symmetric, then any separable ϱ_{AB} obeys*

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)} \mathcal{J}_B^{(1)} \leq 1, \tag{7.6.6}$$

where $g = (3/N^2)^2$ and $(\alpha, \beta, \gamma) = (0, 12/N^2, 0)$.

Remark 45. The proof is given in Sec. 9.9. As the proof's main idea, we will first simply evaluate the integrals on the left-hand side in Eq. (7.6.6). Then we will adopt the so-called T_2 separability criterion presented in Ref. [416] (see, Proposition 5) in order to find the entanglement criterion in Eq. (7.6.6).

Remark 46. The violation of this inequality allows us to detect entanglement between the spatially separated two ensembles. In the following, we will demonstrate how the criterion in Eq. (7.6.6) can characterize entanglement between two ensembles. Also, we will show that Result 37 can be extended to the case of m ensembles for $m \geq 3$.

Remark 47. The right-hand-side in Eq. (7.6.6) in Result 37, can be rewritten as

$$\begin{aligned} &\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)} \mathcal{J}_B^{(1)} \\ =&\frac{1}{N^4} \left\{ \sum_{p,q} \eta_{pq}^2 + 4N^2 \sum_p \left[\langle J_{p,A} \rangle^2 + \langle J_{p,B} \rangle^2 \right] - 16 \sum_{p,q} \langle J_{p,A} \rangle^2 \langle J_{q,B} \rangle^2 \right\}, \end{aligned} \tag{7.6.7}$$

where

$$\sum_{p=x,y,z} a_p^2 = \left(\frac{2}{N}\right)^2 \sum_{p=x,y,z} \langle J_{p,A}\rangle^2, \tag{7.6.8a}$$

$$\sum_{p=x,y,z} b_p^2 = \left(\frac{2}{N}\right)^2 \sum_{p=x,y,z} \langle J_{p,B}\rangle^2, \tag{7.6.8b}$$

$$\sum_{p,q=x,y,z} C_{pq}^2 = \left(\frac{1}{N^2}\right)^2 \sum_{p,q=x,y,z} \left[(\Delta J_p^+)^2 - (\Delta J_q^-)^2\right]^2 \equiv \left(\frac{1}{N^2}\right)^2 \sum_{p,q=x,y,z} \eta_{pq}^2, \tag{7.6.8c}$$

and $\eta_{pq} \equiv (\Delta J_p^+)^2 - (\Delta J_q^-)^2$.

Let us test our criterion in Result 37 in the main text with the Dicke state as a bipartite state. The N_{AB}-qubit Dicke state with m_{AB} excitations is defined as

$$|N_{AB}, m_{AB}\rangle = \binom{N_{AB}}{m_{AB}}^{-\frac{1}{2}} \sum_{m_{AB}} \mathcal{P}_{m_{AB}}(|1_1, \ldots, 1_{m_{AB}}, 0_{m_{AB}+1}, \ldots, 0_{N_{AB}}\rangle), \tag{7.6.9}$$

where $\{\mathcal{P}_{m_{AB}}\}$ is the set of all distinct permutations in the qubits. Applying the Schmidt decomposition to the Dicke state, one can have

$$|N_{AB}, m_{AB}\rangle = \sum_{m=0}^{N_{AB}} \lambda_m |N_A, m_A\rangle \otimes |N_B, m_B\rangle, \tag{7.6.10}$$

where $N_A + N_B = N_{AB}$, $m_A + m_B = m_{AB}$, and $m = m_A$. Here, the Schmidt coefficients λ_m are given by

$$\lambda_m = \binom{N_{AB}}{m_{AB}}^{-\frac{1}{2}} \binom{N_A}{m_A}^{\frac{1}{2}} \binom{N_B}{m_B}^{\frac{1}{2}}. \tag{7.6.11}$$

The states $|N_A, m_A\rangle$ and $|N_B, m_B\rangle$ are permutationally symmetric states, for details, see [323, 324].

Let us consider the case where $N_A = N_B = N_{AB}/2$, and $m_{AB} = N_{AB}/2$. Then we have

$$\langle J_{p,A}\rangle = \langle J_{p,B}\rangle = 0, \quad \text{for} \quad p = x, y, z, \tag{7.6.12a}$$

$$\langle J_z^2\rangle = (\Delta J_z^+)^2 = 0, \tag{7.6.12b}$$

$$(\Delta J_z^-)^2 = -4\langle J_{z,A} \otimes J_{z,B}\rangle = \frac{N_{AB}^2}{4(N_{AB}-1)}, \tag{7.6.12c}$$

$$(\Delta J_x^+)^2 = (\Delta J_y^+)^2 = \frac{N_{AB}}{4}\left(\frac{N_{AB}}{2} + 1\right), \tag{7.6.12d}$$

$$(\Delta J_x^-)^2 = (\Delta J_y^-)^2 = \frac{N_{AB}}{8}\frac{N_{AB}-2}{N_{AB}-1}, \tag{7.6.12e}$$

where we used the results in Ref. [554]. Then we have the values of $(\Delta J_p^{\pm})^2$. In this paper, we set $N_{AB} = 2N$. This results in

$$\begin{aligned}\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} &= \frac{1}{N^4}\sum_{p,q=x,y,z}\left[(\Delta J_p^+)^2 - (\Delta J_q^-)^2\right]^2 \\ &= \frac{6N^4 - 2N^3 + 1}{(1-2N)^2N^2}. \end{aligned} \tag{7.6.13}$$

The right-hand side monotonically decreases as N increases, and it becomes $3/2$ when $N \to \infty$. Therefore the pure $2N$-qubit Dicke states can be detected in any N.

Finally, let us consider the case where the global depolarizing channel with noise p influences the state as follows: $\varrho_D \to \varrho'_D = p\varrho_D + (1-p)\varrho_{\rm mm}$ for $\varrho_D = |N_{AB}, m_{AB}\rangle\langle N_{AB}, m_{AB}|$ and the maximally mixed state $\varrho_{\rm mm}$. This noise effects can change $(\Delta J_l^{\pm})^2$ as follows:

$$(\Delta J_{x/y}^+)^2_{\varrho_D} \to (\Delta J_{x/y}^+)^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J_{x/y}^+)^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N(1+Np)}{2}, \tag{7.6.14a}$$

$$(\Delta J_{x/y}^-)^2_{\varrho_D} \to (\Delta J_{x/y}^-)^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J_{x/y}^-)^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N[N(2-p)-1]}{2(2N-1)}, \tag{7.6.14b}$$

$$(\Delta J_z^+)^2_{\varrho_D} \to (\Delta J_z^+)^2_{\varrho'_D} = \frac{N_{AB}(1-p)}{4} = \frac{N(1-p)}{2}, \tag{7.6.14c}$$

$$(\Delta J_z^-)^2_{\varrho_D} \to (\Delta J_z^-)^2_{\varrho'_D} = \frac{N_{AB}}{4} + p\left[(\Delta J_z^-)^2_{\varrho_D} - \frac{N_{AB}}{4}\right] = \frac{N(2N+p-1)}{2(2N-1)}. \tag{7.6.14d}$$

This leads to

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_A^{(1)} + \mathcal{J}_B^{(1)} - \mathcal{J}_A^{(1)}\mathcal{J}_B^{(1)} = \frac{\left(6N^4 - 2N^3 + 1\right)p^2}{(1-2N)^2N^2}. \tag{7.6.15}$$

Then we can find that the separability bound in Result 37 is violated when $p > p^*(N)$ for the critical point

$$p^*(N) = \frac{N(2N-1)}{\sqrt{6N^4 - 2N^3 + 1}}. \tag{7.6.16}$$

In Fig. 7.5, we illustrate the behavior of the critical point depending on N. In the limit $N \to \infty$, this point becomes $p^* \to \sqrt{2/3}$.

Remark 48. Here we consider the generalization of Result 37 to m ensembles for $m \geq 3$. For that, let us define a quantum state $\varrho \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$, where $\mathcal{H}_X = \mathcal{H}_2^{\otimes N}$ for $X = 1, \ldots, m$. Now it is essential to notice that the left-hand-side

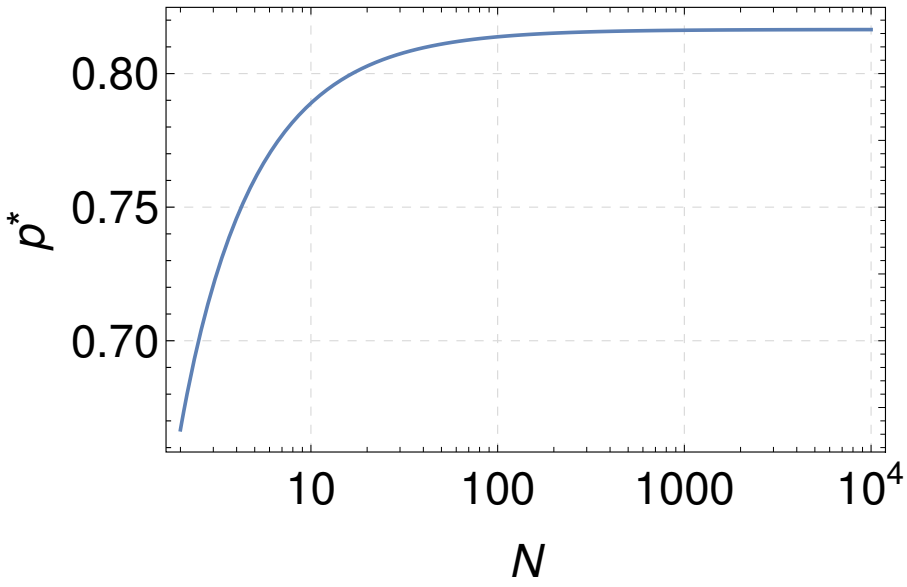

Figure 7.5: Linear-Log plot of the critical point $p^*(N)$. This figure is taken from Ref. [10].

in Result 37 can be available for any two-pair in m ensembles. Then, let us define the average over all pairs

$$\mathcal{P}(\varrho) = \frac{2}{m(m-1)} \sum_{X<Y} \mathcal{G}^{(2)}_{XY} + \mathcal{J}^{(1)}_X + \mathcal{J}^{(1)}_Y - \mathcal{J}^{(1)}_X \mathcal{J}^{(1)}_Y, \tag{7.6.17}$$

for $X, Y = 1, 2, \ldots, m$. Now we can formulate the following.

Result 38. *For this mN-qubit state ϱ consisting of the m ensembles of N spin-$\frac{1}{2}$ particles, if each N-qubit ensemble is permutationally symmetric, then any fully separable ϱ obeys*

$$\mathcal{P}(\varrho) \leq 1, \tag{7.6.18}$$

where $g = (3/N^2)^2$ and $(\alpha, \beta, \gamma) = (0, 12/N^2, 0)$.

Proof. In general, if a multipartite state ϱ is fully separable, then all the bipartite reduced states are clearly separable. For such separable reduced states, Result 37 holds. Thus we can complete the proof. □

7.7 Discussions

This Chapter proposed systematic methods to characterize entanglement in ensembles of particles in the collective randomized measurement scheme. We have shown that various types of spin-squeezing entanglement can be detected in this framework.

There are several research directions in which our work can be extended. First, it would be interesting to find criteria for higher-order spin-squeezing based on k-body correlations such as J_l^k. Next, the inequality (7.5.6) may remind us of entanglement witnesses [17]. On a more technical level, our results may trigger other extensions of witnesses for multipartite entanglement with antisymmetric correlations. Finally, our method may encourage the further development of genuine multipartite entanglement between spatially-separated ensembles [553], reference-frame-independent quantum metrology, higher-order nonlinear spin squeezing [327], or the characterization of invariants under collective unitaries.

Chapter 8

Entanglement detection with moments of the partial transpose

This Chapter focuses on the moments of the partially transposed quantum state. The moments are invariant under local unitaries and can be accessed from randomized measurements. This Chapter proposes systematic methods to advance entanglement criteria with the moments in an optimal and systematic manner. This Chapter is based on Ref. [3].

8.1 Introduction

We begin by recalling the positive partial transpose (PPT) criterion in Eq. (1.2.44): If a bipartite quantum state is separable, then its partial transpose is positive. That is,

$$\varrho_{AB} \in \text{SEP} \;\Rightarrow\; \varrho_{AB}^{\top_B} \geq 0. \tag{8.1.1}$$

The violation of the PPT criterion implies the presence of NPT entanglement. Although the PPT criterion can powerfully and straightforwardly detect entanglement, the implementation may require quantum state tomography in actual experiments.

A practical way to detect NPT entanglement is to consider the so-called PT (or negativity) moments

$$p_k = \text{tr}\left[\left(\varrho_{AB}^{\top_B}\right)^k\right]. \tag{8.1.2}$$

These quantities are local unitary (LU) invariant for any order k, since the eigenvalues of $\varrho_{AB}^{\top_B}$ are LU invariant. Similarly to the moments in Eq. (1.4.2) in Sec. 1.4, these moments can be determined by randomized measurements [105, 438] and also see [7].

In Ref. [105], the following entanglement criterion based on the PT moments was introduced:

$$\varrho_{AB} \in \text{SEP} \;\Rightarrow\; p_3 \geq p_2^2. \tag{8.1.3}$$

This is called the p_3-PPT criterion, which gives a necessary (not sufficient) condition for PPT states and therefore separable states. For a special case, it is

worthwhile to note that the PT-moment approach can detect entanglement of the Werner state in a necessary and sufficient way for any dimension even at lower orders, for more details see Appendix in Ref. [105].

The collection of the moments p_k for any k, that is, $\boldsymbol{p} = (p_0, p_1, p_2, \ldots, p_d)$ with $d = d_A d_B$ ($p_0 = d$ and $p_1 = 1$), enables us to evaluate the PPT criterion, since all the eigenvalues of $\varrho_{AB}^{\top_B}$ can be directly calculated [107]. However, it is demanding to measure all the PT moments in practice. Then the question arises as to whether entanglement can be detected from the moments of limited order. For the case of PT moments, we formulate this problem as follows:

PT-Moment Problem. Given the numbers $\boldsymbol{p}^{(n)} = (p_0, p_1, p_2, \ldots, p_n)$ with order n, is there a separable state ϱ_{AB} such that $p_k = \mathrm{tr}[(\varrho_{AB}^{\top_B})^k]$ for $k = 0, 1, \ldots, n$?

The aim of this Chapter is to develop the PT moment approach in two directions. First, we establish a connection between the PT-moment problem and the well-known moment problems in the mathematical literature. This results in a relaxation of the PT-moment problem, leading to a family of entanglement criteria, where the p_3-PPT criterion represents the lowest order. Second, we show that the p_3-PPT criterion is not sufficient for the PT-moment problem of order three. To address this, we reformulate the PT-moment problem as an optimization problem and derive an explicit necessary and sufficient criterion for $n = 3$. Furthermore, we extend and generalize it for the case where $n > 3$.

8.2 Relaxation to the classical moment problems

We start with a relaxation of the PT moment problem and establish a connection to the classical moment problems. Instead of defining the classical moment problems with respect to the Borel measure on the real line [555–557], we rewrite them with quantum states and observables.

Given a quantum state σ and an observable (Hermitian operator) X, the k-th moment is defined as

$$m_k = \mathrm{tr}\big(\sigma X^k\big). \tag{8.2.1}$$

The moment problems ask the converse: given a sequence of moments, does there exist a quantum state σ and an observable X (with some restrictions) giving the desired moments? Although formulated in a quantum language, this scenario is essentially classical, since σ can be taken diagonally in the eigenbasis of X. In particular, the (truncated) Hamburger and Stieltjes moment problems are defined as follows:

Hamburger Moment Problem. Given the numbers $\boldsymbol{m}^{(n)} = (m_0, m_1, \ldots, m_n)$ with order n, is there a quantum state σ and an observable X such that $m_k = \mathrm{tr}(\sigma X^k)$ for $k = 0, 1, \ldots, n$?

Stieltjes Moment Problem. Given the numbers $\boldsymbol{m}^{(n)} = (m_0, m_1, \ldots, m_n)$ with order n, is there a quantum state σ and a positive semidefinite observable X such that $m_k = \mathrm{tr}(\sigma X^k)$ for $k = 0, 1, \ldots, n$?

We define the corresponding two sets of moments as

$$\mathcal{M}_n = \left\{ \boldsymbol{m}^{(n)} \mid \mathrm{tr}(\sigma X^k) = m_k,\ \sigma \geq 0,\ X^\dagger = X \right\}, \tag{8.2.2}$$

$$\mathcal{M}_n^+ = \left\{ \boldsymbol{m}^{(n)} \mid \mathrm{tr}(\sigma X^k) = m_k,\ \sigma \geq 0,\ X \geq 0 \right\}. \tag{8.2.3}$$

Note that in the above definitions, there is no restriction on the dimension of σ and X. Also, since there is no bound on the eigenvalues of X, the sets $\mathcal{M}_n$ and $\mathcal{M}_n^+$ are not closed.

For $\sigma = \mathbb{1}$ and $X = \varrho_{AB}^{\top_B}$, the PT-moments $\boldsymbol{p}^{(n)}$ always satisfy that $\boldsymbol{p}^{(n)} \in \mathcal{M}_n$, and furthermore the PT-moments given by the PPT states satisfy that $\boldsymbol{p}^{(n)} \in \mathcal{M}_n^+$. Then, the set $\mathcal{M}_n^+$ can be characterized by a family of necessary conditions for the PT-moment problem. This is a relaxation, since more general σ are allowed in the definition of $\mathcal{M}_n$ and $\mathcal{M}_n^+$.

To proceed, we introduce the notion of Hankel matrices. The Hankel matrices $H_k(\boldsymbol{m})$ and $B_k(\boldsymbol{m})$ are $(k+1) \times (k+1)$ matrices defined by

$$[H_k(\boldsymbol{m})]_{ij} = m_{i+j}, \qquad [B_k(\boldsymbol{m})]_{ij} = m_{i+j+1}, \tag{8.2.4}$$

for $i, j = 0, 1, \ldots, k$. Hereafter, we will often suppress the argument ($\boldsymbol{m}$ or $\boldsymbol{p}$) in the notation when there is no risk of confusion. Examples are given by

$$H_1 = \begin{bmatrix} m_0 & m_1 \\ m_1 & m_2 \end{bmatrix}, \qquad B_1 = \begin{bmatrix} m_1 & m_2 \\ m_2 & m_3 \end{bmatrix}, \tag{8.2.5}$$

$$H_2 = \begin{bmatrix} m_0 & m_1 & m_2 \\ m_1 & m_2 & m_3 \\ m_2 & m_3 & m_4 \end{bmatrix}, \qquad B_2 = \begin{bmatrix} m_1 & m_2 & m_3 \\ m_2 & m_3 & m_4 \\ m_3 & m_4 & m_5 \end{bmatrix}. \tag{8.2.6}$$

From the definition of the Hankel matrices, one can prove the following result on the relations between $\mathcal{M}_n, \mathcal{M}_n^+$ and H_k, B_k.

Result 39. *Given $\boldsymbol{m}^{(n)} = (m_0, m_1, \ldots, m_n)$ with order n, it holds that*

$$\text{(a)} \quad \boldsymbol{m}^{(n)} \in \mathcal{M}_n \ \Rightarrow\ H_{\lfloor \frac{n}{2} \rfloor} \geq 0, \tag{8.2.7}$$

$$\text{(b)} \quad \boldsymbol{m}^{(n)} \in \mathcal{M}_n^+ \ \Rightarrow\ H_{\lfloor \frac{n}{2} \rfloor} \geq 0 \ \text{ and } \ B_{\lfloor \frac{n-1}{2} \rfloor} \geq 0. \tag{8.2.8}$$

Remark 49. The proof is given below. These results follow from well-known results in the classical moment problems expressed in the language of measure theory; see, for example, Refs. [556, Chapter 3] and [557, Chapter 9]. In the following, we give an elementary proof in terms of quantum theory.

Remark 50. The conditions are almost sufficient. Considering the moments $\boldsymbol{m}^{(n)}$ in the closure of $\mathcal{M}_n$ or $\mathcal{M}_n^+$ leads to the sufficient conditions of the positivity of Hankel matrices. For details, see Appendix in Ref. [3].

Proof. We take advantage of the Hilbert-Schmidt inner product in the operator space

$$\langle X, Y\rangle := \mathrm{tr}(X^\dagger Y). \tag{8.2.9}$$

Now, consider the sequence of operators $\boldsymbol{v} = (\varrho^{\frac{1}{2}}, \varrho^{\frac{1}{2}}X, \ldots, \varrho^{\frac{1}{2}}X^{\lfloor\frac{n}{2}\rfloor})$, and similarly the sequence of operators $\boldsymbol{u} = (\varrho^{\frac{1}{2}}X^{\frac{1}{2}}, \varrho^{\frac{1}{2}}X^{\frac{3}{2}}, \ldots, \varrho^{\frac{1}{2}}X^{\lfloor\frac{n-1}{2}\rfloor+\frac{1}{2}})$ when $X \geq 0$. Then, the Gram matrices for $\boldsymbol{v}$ and $\boldsymbol{u}$ are given by

$$\langle v_i, v_j\rangle = \mathrm{tr}(X^i\varrho^{\frac{1}{2}}\varrho^{\frac{1}{2}}X^j) = \mathrm{tr}(\varrho X^{i+j}) = m_{i+j}, \tag{8.2.10}$$

$$\langle u_i, u_j\rangle = \mathrm{tr}(X^{i+\frac{1}{2}}\varrho^{\frac{1}{2}}\varrho^{\frac{1}{2}}X^{j+\frac{1}{2}}) = \mathrm{tr}(\varrho X^{i+j+1}) = m_{i+j+1}, \tag{8.2.11}$$

which are just the Hankel matrices $H_{\lfloor\frac{n}{2}\rfloor}$ and $B_{\lfloor\frac{n-1}{2}\rfloor}$. Note that Gram matrices are always positive semidefinite [104], since for $[G]_{ij} = \langle v_i, v_j\rangle$, it holds that

$$\sum_{i,j} G_{ij}x_i^* x_j = \sum_{i,j}\langle x_i v_i, x_j v_j\rangle = \left\langle \sum_i x_i v_i, \sum_j x_j v_j \right\rangle = \left\| \sum_i x_i v_i \right\|^2 \geq 0. \tag{8.2.12}$$

Thus we get the results: (a) $H_{\lfloor\frac{n}{2}\rfloor} \geq 0$ when $\varrho \geq 0$; (b) $H_{\lfloor\frac{n}{2}\rfloor} \geq 0$ and $B_{\lfloor\frac{n-1}{2}\rfloor} \geq 0$ when $\varrho \geq 0$ and $X \geq 0$. □

By applying Result 39 to the PT-moment problem, we obtain a family of criteria for entanglement detection.

Result 40. *Given $\boldsymbol{p}^{(n)} = (p_0, p_1, p_2, \ldots, p_n)$ with order n, it holds that*

$$\varrho_{AB} \in \mathrm{SEP} \;\Rightarrow\; B_{\lfloor\frac{n-1}{2}\rfloor}(\boldsymbol{p}) \geq 0. \tag{8.2.13}$$

Remark 51. In Result 39(a), the condition $H_{\lfloor\frac{n}{2}\rfloor} \geq 0$ does not give an entanglement criterion. This is because this condition is satisfied by any (separable or entangled) state.

Remark 52. In Result 40, the lowest-order criterion, $B_1 \geq 0$, gives that $p_3 \geq p_2^2$, which is exactly the p_3-PPT condition in Eq. (8.1.3) from Ref. [105]. When $k > 1$, B_k gives stronger criteria for entanglement detection. Accordingly, we call the condition in Result 40 p_n-PPT criterion for $n = 3, 5, 7, \ldots$.

Remark 53. The p_n-PPT criteria are strictly stronger than the higher-order criteria proposed in Ref. [105]:

$$p_n^{n-2} \geq p_{n-1}^{n-1}, \quad \text{for } n = 3, 4, \ldots \tag{8.2.14}$$

This criterion only contains very limited information on the positive semidefinite property of the Hankel matrices, and for n is even, this holds for all states including the NPT states. The proof is given as follows. First, recall the positive semidefinite property of the Hankel matrices H_k and B_k. Then their principal submatrices are also positive semidefinite, leading to

$$\begin{bmatrix} p_{n-2} & p_{n-1} \\ p_{n-1} & p_n \end{bmatrix} \geq 0, \quad \text{for } n = 3, 4, \ldots. \tag{8.2.15}$$

This implies that

$$p_n \geq 0, \quad p_n p_{n-2} \geq p_{n-1}^2. \tag{8.2.16}$$

Note that Eq. (8.2.16) gives the criterion in Eq. (8.2.14) for $n = 3$, i.e., the p_3-PPT criterion. The result in Eq. (8.2.14) follows from induction: Assuming that Eq. (8.2.14) of order $n-1$ is true, i.e., $p_{n-1}^{n-3} \geq p_{n-2}^{n-2}$ implies that

$$p_n^{n-2} p_{n-1}^{n-3} \geq p_n^{n-2} p_{n-2}^{n-2} \geq p_{n-1}^{2n-4}, \tag{8.2.17}$$

which gives Eq. (8.2.14) of order n. For more details about this analysis, see Ref. [3].

8.3 Optimal solution to the PT-moment problem

Result 40 already provides a family of strong entanglement criteria, but they are not optimal. This is because σ in Eqs. (8.2.2, 8.2.3) can be arbitrary, but in the PT-moment problem σ is always $\mathbb{1}$. In the following, we give an optimal solution to the PT-moment problem.

By writing the spectrum of $\varrho_{AB}^{\top_B}$ as $(x_1, x_2, \ldots, x_d)$, one can easily see that the PT-moment problem is equivalent to characterizing the set

$$\mathcal{T}_n^+ = \left\{ \boldsymbol{p}^{(n)} \mid \sum_{i=1}^d x_i^k = p_k, \ x_i \geq 0 \right\}. \tag{8.3.1}$$

Indeed, for any $\boldsymbol{p}^{(n)} \in \mathcal{T}_n^+$ a compatible separable state can be constructed as follows: Relabel x_i for $i = 1, 2, \ldots, d$ as $x_{\alpha\beta}$ for $\alpha = 1, 2, \ldots, d_A$ and $\beta = 1, 2, \ldots, d_B$; then construct a separable state $\varrho_{AB} = \sum_{\alpha,\beta} x_{\alpha\beta} |\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|$, where $|\alpha\rangle, |\beta\rangle$ are states in the computational basis. This state has $p_k = \mathrm{tr}[(\varrho_{AB}^{\top_B})^k]$ for $k = 0, 1, \ldots, n$. For convenience, we also define the more general set

$$\mathcal{T}_n = \left\{ \boldsymbol{p}^{(n)} \mid \sum_{i=1}^d x_i^k = p_k, \ x_i \in \mathbb{R} \right\}. \tag{8.3.2}$$

Hereafter, the eigenvalues $(x_1, x_2, \ldots, x_d)$ are always assumed to be sorted in descending order, unless otherwise stated. In Eqs. (8.3.1, 8.3.2), the dimension $d = \dim(\mathcal{H}_A \otimes \mathcal{H}_B)$ is considered as fixed, but actually the optimal entanglement criteria in the following, e.g., Eq. (8.3.10), do not depend on d anymore.

The key idea of the optimal criteria is to consider the following optimization,

$$\begin{aligned} \min_{x_i} \,/\, \max_{x_i} \quad & \hat{p}_n := \sum_{i=1}^d x_i^n \\ \text{subject to} \quad & \sum_{i=1}^d x_i^k = p_k \ \text{ for } k = 1, 2, \ldots, n-1, \\ & x_i \geq 0 \ \text{ for } i = 1, 2, \ldots, d. \end{aligned} \tag{8.3.3}$$

Note that this may also be viewed as a minimization or maximization of the Rényi or Tsallis entropy of order n under the constraint that the entropies for lower integer orders are fixed.

Suppose that the solutions are given by $\hat{p}_n^{\min}$ and $\hat{p}_n^{\max}$, respectively, then $p_n \in [\hat{p}_n^{\min}, \hat{p}_n^{\max}]$ provides a necessary condition for ϱ_{AB} being separable. If one can further show that all $p_n \in [\hat{p}_n^{\min}, \hat{p}_n^{\max}]$ are attainable by some $(x_1, x_2, \ldots, x_d)$ from a separable state, this will imply the sufficiency of the condition. As Eq. (8.3.3) is a polynomial optimization, the sum-of-squares hierarchy can, in principle, be used for approximating the bounds [558, 559]. Remarkably, an alternative sum-of-squares method was used in Ref. [560] for bounding the negative eigenvalues from moments. Here, instead of using these approximation methods, we propose an exact method for solving Eq. (8.3.3) analytically.

We start from the simplest case $n = 3$. As shown below, the maximum and minimization are achieved by

$$\boldsymbol{x}_3^{\max} = (x_1, x_2, x_2, \ldots, x_2), \tag{8.3.4}$$

$$\boldsymbol{x}_3^{\min} = (x_1, x_1, \cdots, x_1, x_{\alpha+1}, 0, 0, \ldots, 0), \tag{8.3.5}$$

respectively, where x_1 appears $\alpha = \lfloor 1/p_2 \rfloor$ times in Eq. (8.3.5). Thus, we obtain the following necessary and sufficient condition for the PT-moment problem of order three.

Result 41. (a) *There exists a d-dimensional separable state ϱ_{AB} satisfying that $p_k = \mathrm{tr}[(\varrho_{AB}^{\top_B})^k]$ for $k = 1, 2, 3$, if and only if*

$$p_1 = 1, \quad \frac{1}{d} \leq p_2 \leq 1, \tag{8.3.6}$$

$$p_3 \leq [1 - (d-1)y]^3 + (d-1)y^3, \tag{8.3.7}$$

$$p_3 \geq \alpha x^3 + (1 - \alpha x)^3, \tag{8.3.8}$$

where

$$\alpha = \left\lfloor \frac{1}{p_2} \right\rfloor, \quad x = \frac{\alpha + \sqrt{\alpha[p_2(\alpha+1) - 1]}}{\alpha(\alpha+1)}, \quad y = \frac{d - 1 - \sqrt{(d-1)(p_2 d - 1)}}{d(d-1)}. \tag{8.3.9}$$

(b) *More importantly, suppose that the p_k for $k = 1, 2, 3$ are PT-moments from a quantum state. Then, they are compatible with a separable state if and only if*

$$p_3 \geq \alpha x^3 + (1 - \alpha x)^3, \tag{8.3.10}$$

where α and x are as above.

Remark 54. The proof is given below. Result 41(a) fully characterizes the set $\mathcal{T}_3^+$, while Result 41(b) characterizes the difference between $\mathcal{T}_3^+$ and $\mathcal{T}_3 \setminus \mathcal{T}_3^+$. In other words, Eqs. (8.3.6, 8.3.7) are satisfied by any (separable or entangled) state, and Eq. (8.3.10) should be used for entanglement detection in practice. Thus, we will refer to Eq. (8.3.10) as the p_3-OPPT (optimal PPT) criterion. We emphasize that the p_3-OPPT criterion is dimension-independent.

Proof. It is well-known that $p_1 = \mathrm{tr}[\varrho_{AB}^{\top_B}] = \mathrm{tr}[\varrho_{AB}] = 1$, and further the optimization problems in Eq. (8.3.3) for $n = 3$ are feasible if and only if $1/d \leq p_2 \leq 1$. To solve the optimization problems in Eq. (8.3.3) for $n = 3$, we start from the simplest nontrivial case that $d = 3$. Then, the optimization reads

$$\begin{aligned} \min_{x_i} / \max_{x_i} \quad & \hat{p}_3 := x_1^3 + x_2^3 + x_3^3 \\ \text{subject to} \quad & x_1 + x_2 + x_3 = p_1, \\ & x_1^2 + x_2^2 + x_3^2 = p_2, \\ & x_1 \geq x_2 \geq x_3 \geq 0, \end{aligned} \tag{8.3.11}$$

where p_1 and p_2 are constants and $\hat{p}_3$ is the objective function that we want to optimize. From Eq. (8.3.11) we can get how $\hat{p}_3$ varies with x_i, i.e., the relations between the differentials $\mathrm{d}\hat{p}_3$ and $\mathrm{d}x_i$,

$$\begin{aligned} \mathrm{d}x_1 + \quad \mathrm{d}x_2 + \quad \mathrm{d}x_3 &= 0, \\ x_1 \mathrm{d}x_1 + x_2 \mathrm{d}x_2 + x_3 \mathrm{d}x_3 &= 0, \\ x_1^2 \mathrm{d}x_1 + x_2^2 \mathrm{d}x_2 + x_3^2 \mathrm{d}x_3 &= \frac{1}{3}\mathrm{d}\hat{p}_3. \end{aligned} \tag{8.3.12}$$

Equivalently, we have

$$V \begin{bmatrix} \mathrm{d}x_1 \\ \mathrm{d}x_2 \\ \mathrm{d}x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{3}\mathrm{d}\hat{p}_3 \end{bmatrix}, \qquad V = \begin{bmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{bmatrix}. \tag{8.3.13}$$

This can be viewed as a system of linear equations on $\mathrm{d}x_i$ and can be directly solved by taking advantage of Cramer's rule and the Vandermonde determinant [104], whenever x_i are all different. In fact, according to Cramer's rule, we find

$$\mathrm{d}x_1 = \frac{\det D_1}{\det V}, \quad \mathrm{d}x_2 = \frac{\det D_2}{\det V}, \quad \mathrm{d}x_3 = \frac{\det D_3}{\det V}, \tag{8.3.14}$$

where

$$D_1 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & x_2 & x_3 \\ \frac{1}{3}\mathrm{d}\hat{p}_3 & x_2^2 & x_3^2 \end{bmatrix}, \quad D_2 = \begin{bmatrix} 1 & 0 & 1 \\ x_1 & 0 & x_3 \\ x_1^2 & \frac{1}{3}\mathrm{d}\hat{p}_3 & x_3^2 \end{bmatrix}, \quad D_3 = \begin{bmatrix} 1 & 1 & 0 \\ x_1 & x_2 & 0 \\ x_1^2 & x_2^2 & \frac{1}{3}\mathrm{d}\hat{p}_3 \end{bmatrix}. \tag{8.3.15}$$

The determinant of the Vandermonde determinant V can be written in the simple form:

$$\det V = \Pi_{i>j}(x_i - x_j) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1). \tag{8.3.16}$$

Since $\det D_1 = -\frac{1}{3}\mathrm{d}\hat{p}_3(x_3 - x_2)$, the relation $\mathrm{d}x_1 = \frac{\det D_1}{\det V}$ leads to that $\mathrm{d}\hat{p}_3 = 3(x_1 - x_2)(x_1 - x_3)\mathrm{d}x_1$. In summary, we have the following relations between $\mathrm{d}\hat{p}_3$ and $\mathrm{d}x_i$

$$\begin{aligned} \mathrm{d}\hat{p}_3 =& 3(x_1 - x_2)(x_1 - x_3)\mathrm{d}x_1 \\ =& 3(x_2 - x_3)(x_2 - x_1)\mathrm{d}x_2 \\ =& 3(x_3 - x_1)(x_3 - x_2)\mathrm{d}x_3. \end{aligned} \tag{8.3.17}$$

Recalling that $x_1 \geq x_2 \geq x_3$ by assumption, Eq. (8.3.17) implies that $\mathrm{d}x_i$ are not independent and an alternating relation exists between them. In fact, we have

$$\mathrm{d}x_1 > 0, \quad \mathrm{d}x_2 < 0, \quad \mathrm{d}x_3 > 0 \;\Rightarrow\; \mathrm{d}\hat{p}_3 > 0, \tag{8.3.18}$$

$$\mathrm{d}x_1 < 0, \quad \mathrm{d}x_2 > 0, \quad \mathrm{d}x_3 < 0 \;\Rightarrow\; \mathrm{d}\hat{p}_3 < 0. \tag{8.3.19}$$

Then, without the boundary condition $x_i \geq 0$, the maximum of $\hat{p}_3$ will be achieved when $x_1 \geq x_2 = x_3$, while the minimum will be achieved when $x_1 = x_2 \geq x_3$. When the boundary condition $x_3 \geq 0$ is taken into consideration, the minimum may also be achieved when x_3 decreases to zero. That is,

$$\boldsymbol{x}_3^{\max} = (x_1, x_2, x_2), \tag{8.3.20}$$

$$\boldsymbol{x}_3^{\min} = (x_1, x_1, 0). \tag{8.3.21}$$

Note that the above analysis does not depend on the actual values of p_1 and p_2 (even if $p_1 \neq 1$). This implies that if the optimization problems in Eq. (8.3.3) for $\hat{p}_3$ ($n = 3$) are feasible, the (local) maximum and minimum will be achieved only if

$$\boldsymbol{x}_3^{\max} = (x_1, \underbrace{x_2, x_2, \ldots, x_2}_{d-1 \text{ times}}), \tag{8.3.22}$$

$$\boldsymbol{x}_3^{\min} = (\underbrace{x_1, x_1, \cdots, x_1}_{\alpha \text{ times}}, x_{\alpha+1}, \underbrace{0, 0, \ldots, 0}_{d-\alpha-1 \text{ times}}). \tag{8.3.23}$$

This is because for the maximization any tuple $(x_{i_1}, x_{i_2}, x_{i_3})$ with $i_1 < i_2 < i_3$ needs to satisfy that $x_{i_2} = x_{i_3}$, and for the minimization it needs to satisfy that $x_{i_1} = x_{i_2}$ or $x_{i_3} = 0$. Without loss of generality, we assume that $x_{\alpha+1} \neq x_1$ in Eq. (8.3.23), then the integer α is uniquely determined by

$$\alpha = \left\lfloor \frac{1}{p_2} \right\rfloor. \tag{8.3.24}$$

This is because the majorization relation

$$\left(\underbrace{\frac{1}{\alpha+1}, \frac{1}{\alpha+1}, \ldots, \frac{1}{\alpha+1}}_{\alpha+1 \text{ times}}, \underbrace{0, 0, \ldots, 0}_{d-\alpha-1 \text{ times}} \right) \tag{8.3.25}$$

$$\prec \left(\underbrace{x_1, x_1, \cdots, x_1}_{\alpha \text{ times}}, x_{\alpha+1}, \underbrace{0, 0, \ldots, 0}_{d-\alpha-1 \text{ times}} \right) \tag{8.3.26}$$

$$\prec \left(\underbrace{\frac{1}{\alpha}, \frac{1}{\alpha}, \ldots, \frac{1}{\alpha}}_{\alpha \text{ times}}, \underbrace{0, 0, \ldots, 0}_{d-\alpha \text{ times}} \right). \tag{8.3.27}$$

and the strict Schur-convexity of $p_2 = \sum_{i=1}^{d} x_i^2$ [561] imply that

$$\frac{1}{\alpha+1} < p_2 \leq \frac{1}{\alpha}. \tag{8.3.28}$$

Now, from Eq. (8.3.22), we can get that

$$\begin{aligned} &x_1 + (d-1)x_2 = 1, \\ &x_1^2 + (d-1)x_2^2 = p_2, \\ &x_1 \geq x_2 \geq 0. \end{aligned} \tag{8.3.29}$$

Given the feasibility condition $1/d \leq p_2 \leq 1$, Eq. (8.3.29) has a unique solution

$$x_1 = \frac{\sqrt{(d-1)(p_2 d - 1)} + 1}{d}, \quad x_2 = \frac{d - 1 - \sqrt{(d-1)(p_2 d - 1)}}{d(d-1)}. \tag{8.3.30}$$

From Eq. (8.3.23), we can get that

$$\begin{aligned} &\alpha x_1 + x_{\alpha+1} = 1, \\ &\alpha x_1 + x_{\alpha+1}^2 = p_2, \\ &x_1 \geq x_{\alpha+1} \geq 0, \end{aligned} \tag{8.3.31}$$

which also has a unique solution

$$x_1 = \frac{\alpha + \sqrt{\alpha[p_2(\alpha+1) - 1]}}{\alpha(\alpha+1)}, \quad x_{\alpha+1} = \frac{1 - \sqrt{\alpha[p_2(\alpha+1) - 1]}}{\alpha+1}. \tag{8.3.32}$$

So far, we only considered the conditions for local extrema and found that the minimum and maximum are unique as in Eqs. (8.3.30, 8.3.32). This implies that these are the global extrema. Further, the uniqueness of the extrema and the continuity of $\hat{p}_3$ also imply that the closed feasible region is connected. Thus, all values between the minimum and the maximum are achievable. All these arguments lead to the optimal result in Result 41(a).

For Result 41(b), as $p_1 = \mathrm{tr}[\varrho_{AB}^{\top_B}] = \mathrm{tr}[\varrho_{AB}]$ and $p_2 = \mathrm{tr}[(\varrho_{AB}^{\top_B})^2] = \mathrm{tr}[\varrho_{AB}^2]$, the conditions that $p_1 = 1$ and $1/d \leq p_2 \leq 1$ are always satisfied by all (separable or entangled) states. To show the redundancy of $p_3 \leq \hat{p}_3^{\max}$, we need to consider the optimization problems in Eq. (8.3.3) without the positivity constraints $x_i \geq 0$. From Eq. (8.3.17), we can see that the maximization is still achieved when $\boldsymbol{x}$ is of the form in Eq. (8.3.22). Given the above conditions $p_1 = 1$ and $1/d \leq p_2 \leq 1$, the solution is always positive from Eq. (8.3.30). Thus, we prove the optimal result in Result 41(b). □

Remark 55. We note that for the case $n = 3$ the bounds in Result 41(a) can also be derived from the optimization of Rényi/Tsallis entropy [562], but our method has the advantages that the refined result in Result 41(b) is given, and more importantly, it can be directly generalized to higher-order optimizations in Eq. (8.3.3). However, an important difference to the case $n = 3$ is that although solving the problem analytically is still possible, writing down the optimal values is no longer straightforward. This is because the roots of higher-order polynomials are much more complicated [563]. For details see Ref. [3].

D	NPT	NPT3	ONPT3	ONPT4	NPT5	ONPT5
2	75.68%	25.53%	39.97%	75.68%	64.78%	75.68%
3	99.99%	25.32%	39.46%	91.63%	97.51%	98.97%
4	100%	23.29%	33.69%	98.68%	100.00%	100.00%
5	100%	21.80%	34.54%	99.95%	100%	100%
6	100%	20.93%	31.20%	100.00%	100%	100%

Table 8.1: Fraction of (small) $D \times D$ states in the Hilbert-Schmidt distribution (1,000,000 samples) that can be detected with various criteria. Here, NPT denotes the states violating the PPT criterion, NPTn (NPT3, NPT5) denotes the states violating the p_n-PPT criterion in Eq. (40), and ONPTn (ONPT3, ONPT4, ONPT5) denotes the states violating the p_n-OPPT criterion.

8.4 Example

In Table 8.1, we investigate the entanglement of randomly generated states. Here, we sample the random $D \times D$ states ($\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = D$) with the Hilbert-Schmidt distribution [565]. From the sampling, one can see a few remarkable advantages of our criteria. First, most of the entangled states can already be detected by the p_5-PPT or the p_4-OPPT criterion, discussed in more details in Ref.[3]. Second, although the p_3-PPT and p_3-OPPT criteria are both based on the PT-moments p_2 and p_3, the optimal criterion p_3-OPPT is significantly stronger than the p_3-PPT criterion in Ref. [105]. Third, compared with the usual entanglement witness method, our criteria have the advantage that neither common reference frames nor prior information are needed for the entanglement detection, see Sec. 1.4. Also, compared with the widely-used fidelity-based entanglement witness, many more entangled states can be detected by comparing Table 8.1 with the results in Refs. [216, 220].

In Fig. 8.1, we plot Result 41 for two-qutrit systems based on the PT moments. There we consider the following thermal state with spin Hamiltonian H_{spin}:

$$\varrho(T, h_y, h_z) = \frac{e^{-\frac{H_{\text{spin}}}{T}}}{Z}, \quad H_{\text{spin}} = S_x^2 + h_y S_y^2 + h_z S_z^2, \quad S_l = s_l^A + s_l^B, \tag{8.4.1}$$

$$s_x = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad s_y = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{bmatrix}, \quad s_z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}. \tag{8.4.2}$$

In the plot, the area inside of Blue but outside of Orange marks our improvement, meaning entangled states that can be detected. Finally, we note that a similar plot has been already discussed in Ref. [564].

8.5 Discussions

This Chapter developed two systematic methods for detecting entanglement from PT-moments. The first method is based on the classical moment prob-

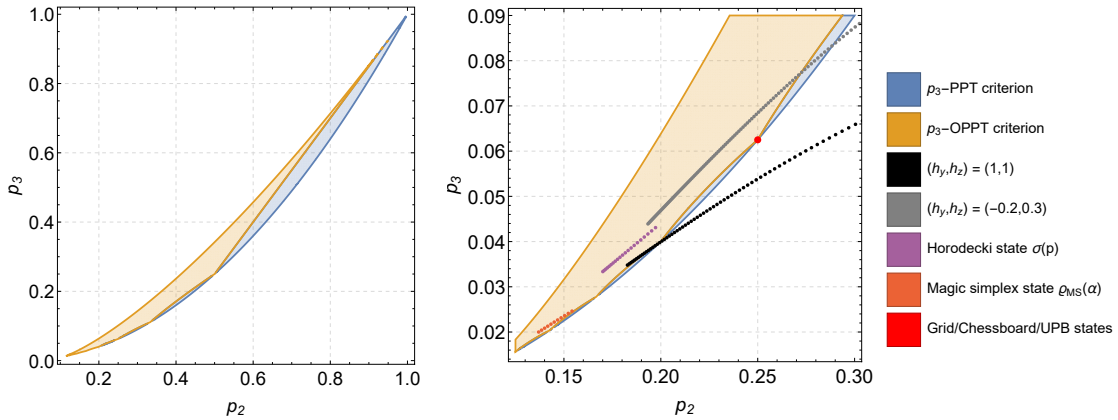

Figure 8.1: Entanglement criteria based on the PT moments for two-qutrit systems with $D = 3$. Blue area contains states that obey the p_3-PPT criterion, while Orange area contains states that obey the p_3-OPPT criterion presented in Result 41. Thus the area inside of Blue but outside of Orange marks our improvement, meaning entangled states that can be detected. (Right) Black and Gray dots, respectively, represent the thermal state $\varrho(T, h_y, h_z)$ in Eq. (8.4.1) with temperature ranges $T_{\text{Black}} \in (0, 3]$ and $T_{\text{Black}} \in (0, 0.8]$. In fact, since PPT entangled states cannot be detected in the PT-moment approach, we demonstrate several examples introduced in Sec. 1.2. Note that a similar plot has been already discussed in Ref. [564].

lems, whose lowest order yields the p_3-PPT criterion in Ref. [105] and higher orders provide strictly stronger criteria. The second method is the optimal method, which gives necessary and sufficient conditions for entanglement detection based on PT-moments. We demonstrated that our criteria are significantly better than existing criteria for physically relevant states.

For future research, it would be highly desirable to extend the presented theory to the characterization of multiparticle entanglement. Indeed, potential generalizations of the PPT criterion for the multiparticle case exist [424], but how to evaluate this using randomized measurements remains an open question. We note that our approach has been extended in terms of permutation criteria [255], moments of realignment [566, 567], and positive maps [568]. Also, detailed analyses of quantum systems have been contacted in terms of two-qubit states Refs. [569–572] and entanglement phase diagram of Haar random states [573]. Finally, while finishing this project, we became aware of a related work by Ref. [564].

Chapter 9

Technical calculations associated with Haar integrals

This Chapter involves several technical calculations associated with Haar integrals. In particular, this Chapter includes the derivations or proofs of Results in Chapters 2, 4, 5, 6, 7. Thus, this Chapter contains the descriptions of Refs. [1, 4, 6, 10].

9.1 Proof of Result 9 in Chapter 2

Proof. Ley us begin by recalling the moments $\mathcal{S}_{AB}^{(r)}$:

$$\mathcal{S}_{AB}^{(r)} = N(r,d) \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 [\mathrm{tr}(\varrho_{AB} \boldsymbol{\alpha}_1 \cdot \boldsymbol{\lambda} \otimes \boldsymbol{\alpha}_2 \cdot \boldsymbol{\lambda})]^r, \tag{9.1.1}$$

where $\boldsymbol{\alpha}_i$ denote (d^2-1)-dimensional unit real vectors uniformly distributed from the pseudo-Bloch sphere, and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_{d^2-1})$ is the vector of Gell-Mann matrices. Furthermore, $N(r,d)$ is a normalization factor. We substitute the two-qudit state (2.3.1) into the moments $\mathcal{S}_{AB}^{(r)}$. In the following, we always add a normalization $N = N(r,d)$, which is later chosen such that $\mathcal{S}_{AB}^{(r)} = 1$ for pure product states, see also Eq. (2.4.7) below. Then we have

$$\begin{aligned}
\mathcal{S}_{AB}^{(r)} &= N \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 \left\{ \mathrm{tr} \left[\left(\frac{1}{d^2} \sum_{i,j=0}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j \right) \boldsymbol{\alpha}_1 \cdot \boldsymbol{\lambda} \otimes \boldsymbol{\alpha}_2 \cdot \boldsymbol{\lambda} \right] \right\}^r \\
&= \frac{N}{d^{2r}} \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 \left\{ \sum_{i,j=1}^{d^2-1} t_{ij} \mathrm{tr} \left[\lambda_i \boldsymbol{\alpha}_1 \cdot \boldsymbol{\lambda} \right] \cdot \mathrm{tr} \left[\lambda_j \boldsymbol{\alpha}_2 \cdot \boldsymbol{\lambda} \right] \right\}^r \\
&= N \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 \left[\sum_{i,j=1}^{d^2-1} t_{ij} \alpha_1^{(i)} \alpha_2^{(j)} \right]^r ,
\end{aligned}$$

where we use $\mathrm{tr}(\boldsymbol{\alpha}_i \cdot \boldsymbol{\lambda}) = 0$. Using the multinomial theorem

$$\left(\sum_{i=1}^{n} x_i \right)^r = \sum_{r_1+r_2+\cdots+r_n=r} \frac{r!}{r_1! r_2! \cdots r_n!} \prod_{i=1}^{n} x_i^{r_i}, \tag{9.1.2}$$

we have

$$\begin{aligned}
\mathcal{S}_{AB}^{(r)} &= N \int d\boldsymbol{\alpha}_1 \int d\boldsymbol{\alpha}_2 \sum_{r_{i,j}} \frac{r!}{r_{1,1}! \cdots r_{d^2-1,d^2-1}!} \prod_{i,j=1}^{d^2-1} \left[t_{ij} \alpha_1^{(i)} \alpha_2^{(j)} \right]^{r_{i,j}} \\
&= N \sum_{r_{i,j}} \frac{r!}{r_{1,1}! \cdots r_{d^2-1,d^2-1}!} \prod_{i,j=1}^{d^2-1} t_{ij}^{r_{i,j}} \int d\boldsymbol{\alpha}_1 \prod_{i=1}^{d^2-1} \left[\alpha_1^{(i)} \right]^{a_i} \int d\boldsymbol{\alpha}_2 \prod_{j=1}^{d^2-1} \left[\alpha_2^{(j)} \right]^{a'_j} \\
&= 4N \sum_{r_{i,j}} \frac{r!}{r_{1,1}! \cdots r_{d^2-1,d^2-1}!} \prod_{i,j=1}^{d^2-1} t_{ij}^{r_{i,j}} B(b_1, b_2, \ldots, b_{d^2-1}) B(b'_1, b'_2, \ldots, b'_{d^2-1}),
\end{aligned} \tag{9.1.3}$$

where the sum $\sum_{r_{i,j}}$ means $\sum_{r_{1,1}+\cdots+r_{1,d^2-1}+r_{2,1}+\cdots+r_{d^2-1,d^2-1}=r}$. We define that

$$a_i = \sum_{j=1}^{d^2-1} r_{i,j}, \quad a'_j = \sum_{i=1}^{d^2-1} r_{i,j}, \quad b_i = (a_i + 1)/2, \quad b'_j = (a'_j + 1)/2. \tag{9.1.4}$$

Note that in general, the integral over the n-dimensional unit sphere is written as $2B(\beta_1, \beta_2, \ldots, \beta_n)$ (see Ref. [574]), where $B(\beta_1, \beta_2, \ldots, \beta_n)$ denotes the multivariable beta function, for $\beta_i = (\alpha_i + 1)/2$ and the gamma function $\Gamma(\beta_i)$, given by

$$B(\beta_1, \beta_2, \ldots, \beta_n) = \frac{\Gamma(\beta_1)\Gamma(\beta_2) \cdots \Gamma(\beta_n)}{\Gamma(\beta_1 + \beta_2 + \ldots + \beta_n)}. \tag{9.1.5}$$

This integral vanishes if any of α_i is odd.

Case of $r = 2$

Let us evaluate the moment at $r = 2$. The condition $r = 2$ means $r_{1,1} + \cdots + r_{d^2-1,d^2-1} = 2$. To make this more explicit, we introduce the square matrix $\boldsymbol{R}$

$$\boldsymbol{R} = \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,d^2-1} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,d^2-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{d^2-1,1} & r_{d^2-1,2} & \cdots & r_{d^2-1,d^2-1} \end{pmatrix}. \tag{9.1.6}$$

Recall here that $a_i = \sum_{j=1}^{d^2-1} r_{i,j}$ and $a'_j = \sum_{i=1}^{d^2-1} r_{i,j}$. Thus, a_i and a'_j respectively correspond to the i-th row vector and the j-th column vector of the matrix $\boldsymbol{R}$.

There are two candidates that satisfy the condition $r_{1,1} + \cdots + r_{d^2-1,d^2-1} = 2$:

(1) one of elements is equal to 2 and all other elements are zero, that is, fixed $r_{\alpha,\beta} = 2$ and $r_{k,l\neq\alpha,\beta} = 0$. An example is given by

$$\boldsymbol{R} = \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{9.1.7}$$

(2) two of elements are equal to 1 and all other elements are zero, that is, fixed $r_{\alpha,\beta} = r_{\gamma,\delta} = 1$ and all other $r_{k,l} = 0$. Examples are

$$\boldsymbol{R} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{9.1.8}$$

In any case of the candidate (2), either or both of a_i and a'_j are always 1, that is, odd. This results in the vanishing of the integral over the sphere. Accordingly, it is sufficient to focus only on the candidate (1) in Eq. (9.1.7). Concerning the expression of moments (9.1.3), we have

$$\begin{aligned} &\frac{2!}{0!\cdots 2!\cdots 0!} = 1, \quad \prod_{i,j=1}^{d^2-1} t_{ij}^{r_{i,j}} = t_{\alpha\beta}^2, \\ &a_\alpha = \sum_j r_{\alpha,j} = 2, \; a_{i\neq\alpha} = 0, \quad a'_\beta = \sum_i r_{i,\beta} = 2, \; a'_{i\neq\beta} = 0, \\ &b_\alpha = \frac{3}{2}, \; b_{i\neq\alpha} = \frac{1}{2}, \quad b'_\beta = \frac{3}{2}, \; b'_{i\neq\beta} = \frac{1}{2}, \\ &B(b_1,\ldots,b_\alpha,\ldots,b_{d^2-1}) = B(b'_1,\ldots,b'_\beta,\ldots,b'_{d^2-1}) \\ &= B\left(\frac{1}{2},\ldots,\frac{3}{2},\ldots,\frac{1}{2}\right) = \frac{(\sqrt{\pi})^{d^2-1}}{2\Gamma\left(\frac{d^2+1}{2}\right)}. \end{aligned} \tag{9.1.9}$$

Then we have

$$\mathcal{S}_{AB}^{(2)} = V\sum_{i,j} t_{ij}^2, \qquad V = 4N\frac{\pi^{d^2-1}}{4\left[\Gamma\left(\frac{d^2+1}{2}\right)\right]^2} = \frac{1}{(d-1)^2}. \tag{9.1.10}$$

Case of $r = 4$

Let us evaluate the moment at $r = 4$. The condition $r = 4$ means $r_{1,1} + \cdots + r_{d^2-1,d^2-1} = 4$. There are several candidates that satisfy the condition $r_{1,1} + \cdots + r_{d^2-1,d^2-1} = 4$. In the following, we will only describe the three candidates with nonzero values of the integral over the sphere.

(1) one of the elements is equal to 4 and all other elements are zero, that is, fixed $r_{\alpha,\beta} = 4$ and $r_{k,l\neq\alpha,\beta} = 0$. An example is

$$\boldsymbol{R} = \begin{pmatrix} 4 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{9.1.11}$$

(2) two of elements are equal to 2 and all other elements are zero, that is, fixed $r_{\alpha,\beta} = r_{\gamma,\delta} = 2$ and others $r_{k,l} = 0$. Examples are divided into three types.

$$\boldsymbol{R} = \begin{pmatrix} 0 & 2 & \cdots & 0 \\ 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{9.1.12}$$

We call these (a), (b), and (c) cases, respectively.

(3) four of elements are equal to 1 and all other elements are zero, that is, fixed $r_{\alpha,\beta} = r_{\gamma,\delta} = r_{\epsilon,\zeta} = r_{\eta,\theta} = 1$ and others are zero. An example is

$$\boldsymbol{R} = \begin{pmatrix} 1 & 1 & \cdots & 0 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{9.1.13}$$

- *Candidate (1).* Let us consider the candidate (1). For fixed $r_{\alpha,\beta} = 4$ and $r_{k,l\neq\alpha,\beta} = 0$, we have

$$\begin{aligned} &a_\alpha = 4,\ a'_\beta = 4,\ \ b_\alpha = \frac{5}{2},\ b'_\beta = \frac{5}{2}, \\ &B(b_1,\ldots,b_\alpha,\ldots,b_{d^2-1}) = B(b'_1,\ldots,b'_\beta,\ldots,b'_{d^2-1}) \\ &= B\left(\frac{1}{2},\ldots,\frac{5}{2},\ldots,\frac{1}{2}\right) = \frac{3(\sqrt{\pi})^{d^2-1}}{4\Gamma\left(\frac{d^2+3}{2}\right)}. \end{aligned} \tag{9.1.14}$$

Therefore, the corresponding term is given by

$$4N\frac{9\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2}\sum_{i,j} t_{ij}^4. \tag{9.1.15}$$

- *Candidate (2).* Let us consider the candidate (2). For fixed $r_{\alpha,\beta} = r_{\gamma,\delta} = 2$, we have the three types (a), (b), and (c), as the three examples described in (9.1.12):

(a) $\alpha \neq \gamma$ and $\beta = \delta$.

(b) $\alpha = \gamma$ and $\beta \neq \delta$.

(c) $\alpha \neq \gamma$ and $\beta \neq \delta$.

For the type (a), we have

$$
\begin{aligned}
&a_n = 2, \text{ for } n = \alpha, \gamma, \ a'_\beta = 4, \ \ b_n = \frac{3}{2}, \ b'_\beta = \frac{5}{2}, \\
&B(b_1, \ldots, b_\alpha, \ldots, b_\gamma, \ldots, b_{d^2-1}) = B\left(\frac{1}{2}, \ldots, \frac{3}{2}, \ldots, \frac{3}{2}, \ldots, \frac{1}{2}\right) = \frac{(\sqrt{\pi})^{d^2-1}}{4\Gamma\left(\frac{d^2+3}{2}\right)}, \\
&B(b'_1, \ldots, b'_\beta, \ldots, b'_{d^2-1}) = B\left(\frac{1}{2}, \ldots, \frac{5}{2}, \ldots, \frac{1}{2}\right) = \frac{3(\sqrt{\pi})^{d^2-1}}{4\Gamma\left(\frac{d^2+3}{2}\right)}. \qquad (9.1.16)
\end{aligned}
$$

Moreover, to avoid the over-counting of summation, we multiply it by $1/2$ in order to be able to write the contribution as the following sum:

$$
4N \times 6 \times \frac{1}{2} \times \frac{3\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2} \sum_{i,j,k,i\neq j} t_{ik}^2 t_{jk}^2. \qquad (9.1.17)
$$

For the type (b), we have the similar result with (a):

$$
4N \times 6 \times \frac{1}{2} \times \frac{3\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2} \sum_{i,j,k,i\neq j} t_{ki}^2 t_{kj}^2. \qquad (9.1.18)
$$

For the type (c), we have

$$
\begin{aligned}
&a_n = 2, \ a'_m = 2, \text{ for } n = \alpha, \gamma, \ m = \beta, \delta, \ \ b_n = \frac{3}{2}, \ b'_m = \frac{3}{2}, \\
&B(b_1, \ldots, b_\alpha, \ldots, b_\gamma, \ldots, b_{d^2-1}) = B(b'_1, \ldots, b'_\beta, \ldots, b'_\delta, \ldots, b'_{d^2-1}) \\
&= B\left(\frac{1}{2}, \ldots, \frac{3}{2}, \ldots, \frac{3}{2}, \ldots, \frac{1}{2}\right) = \frac{(\sqrt{\pi})^{d^2-1}}{4\Gamma\left(\frac{d^2+3}{2}\right)}. \qquad (9.1.19)
\end{aligned}
$$

Therefore, the corresponding term is given by

$$
4N \times 6 \times \frac{1}{2} \times \frac{\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2} \sum_{i,j,k,l,i\neq k,j\neq l} t_{ij}^2 t_{kl}^2. \qquad (9.1.20)
$$

- *Candidate (3).* Let us consider the candidate (3). For fixed $r_{\alpha,\beta} = r_{\gamma,\delta} = r_{\epsilon,\zeta} = r_{\eta,\theta} = 1$, only one case yields finite values of the integral: $\alpha = \gamma$,

$\beta = \zeta$, $\epsilon = \eta$, and $\delta = \theta$. Here, rewriting the condition as $r_{\alpha,\beta} = r_{\alpha,\delta} = r_{\epsilon,\beta} = r_{\epsilon,\delta} = 1$, we have

$$\begin{aligned} &a_n = 2,\ a'_m = 2,\ \text{for}\, n = \alpha, \epsilon,\ m = \beta, \delta,\ \ b_n = \frac{3}{2},\ b'_m = \frac{3}{2}, \\ &B(b_1, \ldots, b_\alpha, \ldots, b_\epsilon, \ldots, b_{d^2-1}) = B(b'_1, \ldots, b'_\beta, \ldots, b'_\delta, \ldots, b'_{d^2-1}) \\ &= B\left(\frac{1}{2}, \ldots, \frac{3}{2}, \ldots, \frac{3}{2}, \ldots, \frac{1}{2}\right) = \frac{(\sqrt{\pi})^{d^2-1}}{4\Gamma\left(\frac{d^2+3}{2}\right)}. \end{aligned} \tag{9.1.21}$$

Moreover, to avoid the over-counting of summation, we multiply it by $1/4$. Therefore, the corresponding term is given by

$$4N \times 24 \times \frac{1}{4} \times \frac{\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2} \sum_{i,j,k,l, i\neq k, j\neq l} t_{ij} t_{il} t_{kj} t_{kl}. \tag{9.1.22}$$

According to the candidates (1), (2), and (3), we finally arrive at

$$\mathcal{S}^{(4)}_{AB} = W\left\{3\sum_{i,j} t^4_{ij} + 3\sum_{i,j,k, i\neq j} t^2_{ik} t^2_{jk} + 3\sum_{i,j,k, i\neq j} t^2_{ki} t^2_{kj} + \sum_{i,j,k,l, i\neq k, j\neq l}\left(t^2_{ij} t^2_{kl} + 2 t_{ij} t_{il} t_{kj} t_{kl}\right)\right\}, \tag{9.1.23}$$

where

$$W = 4N \frac{3\pi^{d^2-1}}{16\left[\Gamma\left(\frac{d^2+3}{2}\right)\right]^2} = \frac{1}{3\,(d-1)^4}. \tag{9.1.24}$$

□

9.2 Proof of Result 10 in Chapter 2

Proof. Analogous to the calculation in the case of $\mathcal{S}^{(r)}_{AB}$ shown in Eq. (9.1.3), after some lengthy calculations and using the fact that M_d is traceless, we obtain

$$\begin{aligned} \mathcal{R}^{(r)}_{AB} = &\sum_{r_{i,j}} \frac{r!}{r_{1,1}! \cdots r_{d^2-1,d^2-1}!} \prod_{i,j=1}^{d^2-1} t_{ij}^{r_{i,j}} \\ &\times \int dU_A \prod_{i=1}^{d^2-1} \mathrm{tr}[U_A M_d U_A^\dagger \lambda_i]^{a_i} \int dU_B \prod_{j=1}^{d^2-1} \mathrm{tr}[U_B M_d U_B^\dagger \lambda_j]^{a'_j}, \end{aligned} \tag{9.2.1}$$

where the sum spans over all non-negative integer assignments to the $r_{i,j}$ such that $\sum_{i,j=1}^{d^2-1} r_{i,j} = r$, and $a_i = \sum_{j=1}^{d^2-1} r_{i,j}$, $a'_j = \sum_{i=1}^{d^2-1} r_{i,j}$.

We start with the discussion of the case $r = 4$, where we focus on one of the integrals and evaluate it for all possible exponent vectors $\boldsymbol{a} = (a_1, \ldots, a_{d^2-1})$. As all the entries are positive integers that sum to 4, there are five families of vectors to be considered:

(a) $a_k = 4$, $a_{l\neq k} = 0$,

(b) $a_k = 3$, $a_l = 1$, $a_{m\neq k,l} = 0$,

(c) $a_k = 2$, $a_l = 2$, $a_{m\neq k,l} = 0$,

(d) $a_k = 2$, $a_l = 1$, $a_m = 1$, $a_{n\neq k,l,m} = 0$,

(e) $a_k = 1$, $a_l = 1$, $a_m = 1$, $a_n = 1$, $a_{o\neq k,l,m,n} = 0$.

We aim to prove that the whole integral coincides with the one obtained from integration over the orthogonal group. To that end, we compare the integrals occurring in Eq. (9.2.1) with those in Eq. (9.1.3). In particular, we try to tweak the observable such that for all vectors $\boldsymbol{a}$ with $\sum a_i = 4$,

$$\int dU_A \prod_{i=1}^{d^2-1} \mathrm{tr}[U_A M_d U_A^\dagger \lambda_i]^{a_i} = MB(b_1, b_2, \ldots, b_{d^2-1}), \tag{9.2.2}$$

where B is defined in Eq. (9.1.5) and $b_i = (a_i + 1)/2$. The prefactor M can be absorbed into the observable, as long as it is independent from $\boldsymbol{a}$. To certify equality, we will show

1. that the cases (b), (d), and (e) vanish for all choices of k, l, m, n, as they contain odd numbers,

2. that the results of all integrals in the family (a) coincide, as well as those in the family (c), as the function B is symmetric w.r.t. its parameters,

3. that the relative factor between the results in family (a) and those in family (c) is given by 3. This comes from that $B(\frac{5}{2}, \frac{1}{2}, \ldots, \frac{1}{2}) = 3B(\frac{3}{2}, \frac{3}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$.

With the help of Eq. (3) in Ref. [66], we can represent the integrals in terms of Weingarten functions and evaluate the five families case by case. Let us recall that we fixed the form of M_d in Eq. (2.4.14) as an ansatz. The conditions $\mathrm{tr}(M_d) = 0, \mathrm{tr}(M_d^2) = d$ allow us to treat the eigenvalue of y as a free variable with one degree of freedom.

- *Case (a).* Depending on the value of k, s.t. $a_k = 4$, we obtain as a result of the integral either one of the polynomials

$$P_1 = C\left(\frac{(d+1)^2(d+3)}{32} - \frac{(d+1)(d+3)}{4}y + \frac{d^2+8d+3}{4}y^2 - 2dy^3 + dy^4\right), \tag{9.2.3}$$

$$P_2 = C\left(\frac{(d+1)^2(d+2)}{32} - \frac{(d+1)(d+2)}{4}y + \frac{d^2+9d-6}{4}y^2 - (3d-4)y^3\right) + C\left(\frac{3d-4}{2}y^4 + \frac{1}{d-1}\left(\frac{d+1}{4} - 2y + 3y^2 - 2y^3 + y^4\right)\right), \tag{9.2.4}$$

  or linear combinations of them with prefactors added to one. Setting $P_1 = P_2$, we obtain the two real solutions for y given by Eq. (2.4.17).

- *Case (b).* Depending on k and l, there are two types of integrals: One vanishes directly, the other yields a multiple of $P_1 - P_2$, which vanishes for our choice of y.

- *Case (c).* This case yields a couple of different results, all of them given by linear combinations of P_1 and P_2 with prefactors adding to $1/3$. Substituting the solution for y, we obtain in every case the same result, given by $1/3$ of the result obtained in case (a).

- *Cases (d) and (e).* These cases are analogous to case (b), yielding zero in each case for the obtained solution of y.

Altogether, we have shown that for the observable M_d in odd dimensions with y given by Eq. (2.4.17), the fourth moment of random unitary measurements coincides with that of random orthogonal ones.

Finally, we consider the second moment. First, it has been shown in Ref. [350] that the second moments do not depend on the eigenvalues, as long as the observable is traceless. Then, note that the result given in Theorem 2 of Ref. [350] also holds for mixed states, the proof given there directly applies to the mixed state case. This theorem states that the second moments $\mathcal{R}^{(2)}$ have the same expression as the one we derived for the second moments $\mathcal{S}^{(2)}$ in Eq. (2.4.8). So the claim follows. □

9.3 Proof of Result 17 in Chapter 4

Useful formulas:

Before we show the proof, let us summarize several useful formulas for Haar unitary integrals, following the description in Ref. [6]. Let us begin by considering the operator

$$\mathcal{O}_U^{(i)} = \mathrm{tr}[\sigma_i U \sigma_z U^\dagger], \tag{9.3.1}$$

with σ_i Pauli matrices for $i = x, y, z$. We introduce the following quantities

$$\mathcal{I}^{(1)}(i,j) = \int dU\, \mathcal{O}_U^{(i)} \mathcal{O}_U^{(j)}, \tag{9.3.2a}$$

$$\mathcal{I}^{(2)}(i,j,k,l) = \int dU\, \mathcal{O}_U^{(i)} \mathcal{O}_U^{(j)} \mathcal{O}_U^{(k)} \mathcal{O}_U^{(l)}, \tag{9.3.2b}$$

$$\mathcal{I}^{(3)}(i,j,k,l,m,n) = \int dU\, \mathcal{O}_U^{(i)} \mathcal{O}_U^{(j)} \mathcal{O}_U^{(k)} \mathcal{O}_U^{(l)} \mathcal{O}_U^{(m)} \mathcal{O}_U^{(n)}. \tag{9.3.2c}$$

In Ref. [6], these integrals can be simplified as follows

$$\mathcal{I}^{(1)}(i,j) = \frac{4}{3}\delta_{ij}, \tag{9.3.3a}$$

$$\mathcal{I}^{(2)}(i,j,k,l) = \frac{16}{15}\left(\delta_{ij}\delta_{kl} + \delta_{ik}\delta_{jl} + \delta_{il}\delta_{jk}\right), \tag{9.3.3b}$$

$$\begin{aligned}\mathcal{I}^{(3)}(i,j,k,l,m,n) = \frac{64}{105}\Big\{&\delta_{ij}[\delta_{kl}\delta_{mn}+\delta_{km}\delta_{ln}+\delta_{kn}\delta_{lm}]+\delta_{ik}[\delta_{jl}\delta_{mn}+\delta_{jm}\delta_{ln}+\delta_{jn}\delta_{lm}]\\ &+\delta_{il}[\delta_{jk}\delta_{mn}+\delta_{jm}\delta_{kn}+\delta_{jn}\delta_{km}]+\delta_{im}[\delta_{jk}\delta_{ln}+\delta_{jl}\delta_{kn}+\delta_{jn}\delta_{kl}]\\ &+\delta_{in}[\delta_{jk}\delta_{lm}+\delta_{jl}\delta_{km}+\delta_{jm}\delta_{kl}]\Big\}.\end{aligned} \tag{9.3.3c}$$

Also, Ref. [6] presents the following formula

$$\int dU\,\mathrm{tr}[\sigma_a U\sigma_x U^\dagger]\mathrm{tr}[\sigma_b U\sigma_y U^\dagger]\mathrm{tr}[\sigma_c U\sigma_z U^\dagger] = \frac{4}{3}\varepsilon_{abc}. \tag{9.3.4}$$

Proof. To proceed, we recall the moments

$$\mathcal{R}^{(t)}_{\mathcal{M}}(\varrho) = \int dU_A \int dU_B \{\mathrm{tr}[(U_A\otimes U_B)\varrho(U_A^\dagger\otimes U_B^\dagger)\mathcal{M}]\}^t. \tag{9.3.5}$$

First, we consider the general form of product observables:

$$\mathcal{M} = (k_A\mathbb{1} + l_A Z)\otimes(k_B\mathbb{1} + l_B Z). \tag{9.3.6}$$

Hereafter for the sake of simplicity, we represent the Pauli matrix σ_z as Z.

- **For $t = 2$:** For $\mathcal{M} = Z\otimes\mathbb{1}$, Eq. (9.3.3a) yields

$$\begin{aligned}\mathcal{R}^{(2)}_{Z\otimes\mathbb{1}}(\varrho) &= \int dU_A\{\mathrm{tr}[\varrho_A U_A Z U_A^\dagger]\}^2\\ &= \frac{1}{4}\sum_{i,j=1}^{3}\alpha_i\alpha_j\int dU\mathrm{tr}[\sigma_i UZU^\dagger]\mathrm{tr}[\sigma_j UZU^\dagger]\\ &= \frac{1}{4}\sum_{i,j=1}^{3}\alpha_i\alpha_j\mathcal{I}^{(1)}(i,j) = \frac{1}{3}\alpha^2.\end{aligned} \tag{9.3.7}$$

  In a similar manner, β^2 can be obtained by measuring $\mathcal{R}^{(2)}_{\mathbb{1}\otimes Z}$. For the case $\mathcal{M} = Z\otimes Z$, we obtain

$$\mathcal{R}^{(2)}_{Z\otimes Z} = \frac{1}{16}\sum_{ijkl=1}^{3}T_{ij}T_{kl}\mathcal{I}^{(1)}(i,k)\mathcal{I}^{(1)}(j,l) = \frac{1}{9}\mathrm{tr}(TT^\top). \tag{9.3.8}$$

- **For $t = 3$:** For $k_A = k_B \equiv k$, $l_A = l_B \equiv l$, that is, $\mathcal{M} = (k\mathbb{1} + lZ)^{\otimes 2}$, we obtain

$$\mathcal{R}^{(3)}_{(k\mathbb{1}+lZ)^{\otimes 2}} = k^6 + k^4l^2[\alpha^2+\beta^2] + \frac{1}{3}k^2l^4[\mathrm{tr}(TT^\top) + 2\boldsymbol{\alpha}^\top T\boldsymbol{\beta}]. \tag{9.3.9}$$

- **For $t = 4$:** For $\mathcal{M} = Z \otimes Z$, Eq. (9.3.3b) yields

$$\mathcal{R}^{(4)}_{Z\otimes Z} = \frac{1}{75}[2\mathrm{tr}(TT^\top TT^\top) + \mathrm{tr}(TT^\top)^2]. \tag{9.3.10}$$

For $\mathcal{M} = \mathcal{M} = (k\mathbb{1} + lZ)^{\otimes 2}$, we obtain

$$\begin{aligned}
&\mathcal{R}^{(4)}_{(k\mathbb{1}+lZ)^{\otimes 2}} \\
&= k^8 + 2k^6l^2[\alpha^2 + \beta^2] \\
&+ \frac{2}{3}k^4l^4[\frac{3}{10}(\alpha^4 + \beta^4) + \alpha^2\beta^2 + \mathrm{tr}(TT^\top) + 4\boldsymbol{\alpha}^\top T\boldsymbol{\beta}] \\
&+ \frac{2}{15}k^2l^6[(\alpha^2 + \beta^2)\mathrm{tr}(TT^\top) + 2([\boldsymbol{\alpha}T]^2 + [T\boldsymbol{\beta}]^2)] \\
&+ \frac{1}{75}l^8[2\mathrm{tr}(TT^\top TT^\top) + \mathrm{tr}(TT^\top)^2].
\end{aligned} \tag{9.3.11}$$

The combination $[\boldsymbol{\alpha}T]^2 + [T\boldsymbol{\beta}]^2$ can be obtained from this symmetric measurement. Choosing $k_A \neq k_B$, $l_A \neq l_B$ leads to the individual terms.

- **For $t = 5$:** For $\mathcal{M} = Z \otimes Z$, we find

$$\begin{aligned}
&\mathcal{R}^{(5)}_{(k\mathbb{1}+lZ)^{\otimes 2}} \\
&= k^{10} + \frac{10}{3}k^8l^2[\alpha^2 + \beta^2] \\
&+ \frac{10}{3}k^6l^4[\frac{3}{10}(\alpha^4 + \beta^4) + \alpha^2\beta^2 + \frac{1}{3}\mathrm{tr}(TT^\top) + 2\boldsymbol{\alpha}^\top T\boldsymbol{\beta}] \\
&+ \frac{2}{3}k^4l^6[(\alpha^2 + \beta^2)(\mathrm{tr}(TT^\top) + 2\boldsymbol{\alpha}^\top T\boldsymbol{\beta}) + 2([\boldsymbol{\alpha}T]^2 + [T\boldsymbol{\beta}]^2)] \\
&+ \frac{1}{15}k^2l^8[2\mathrm{tr}(TT^\top TT^\top) + \mathrm{tr}(TT^\top)(\mathrm{tr}(TT^\top) + 4\boldsymbol{\alpha}^\top T\boldsymbol{\beta}) + 8\boldsymbol{\alpha}^\top TT^\top T\boldsymbol{\beta}].
\end{aligned} \tag{9.3.12}$$

- **For $t = 6$:** For $\mathcal{M} = (k\mathbb{1} + lZ)^{\otimes 2}$, Eq. (9.3.3c) yields

$$\begin{aligned}
&\mathcal{R}^{(6)}_{(k\mathbb{1}+lZ)^{\otimes 2}} \\
&= k^{12} + 5k^{10}l^2[\alpha^2 + \beta^2] \\
&+ \frac{1}{3}k^8 l^4[9(\alpha^4 + \beta^4) + 30\alpha^2\beta^2 + 5\mathrm{tr}(TT^\top) + 40\boldsymbol{\alpha}^\top T\boldsymbol{\beta}] \\
&+ k^6 l^6[(\alpha^2+\beta^2)(\alpha^2\beta^2+2\mathrm{tr}(TT^\top)+8\boldsymbol{\alpha}^\top T\boldsymbol{\beta})+4([\boldsymbol{\alpha}T]^2+[T\boldsymbol{\beta}]^2)+\frac{1}{7}(\alpha^6+\beta^6)] \\
&+ \frac{1}{5}k^4 l^8[2\mathrm{tr}(TT^\top TT^\top)+\mathrm{tr}(TT^\top)(\mathrm{tr}(TT^\top) + 8\boldsymbol{\alpha}^\top T\boldsymbol{\beta}+\frac{5}{7}(\alpha^4 + \beta^4) + 2\alpha^2\beta^2)] \\
&+ \frac{1}{5}k^4 l^8[16\boldsymbol{\alpha}^\top TT^\top T\boldsymbol{\beta}+(\frac{20}{7}\alpha^2 + 4\beta^2)[\boldsymbol{\alpha}T]^2+(\frac{20}{7}\beta^2 + 4\alpha^2)[T\boldsymbol{\beta}]^2+8[\boldsymbol{\alpha}^\top T\boldsymbol{\beta}]^2] \\
&+ \frac{1}{35}k^2 l^{10}[(\alpha^2 + \beta^2)(2\mathrm{tr}(TT^\top TT^\top) + \mathrm{tr}(TT^\top)^2) + 4([\boldsymbol{\alpha}T]^2 + [T\boldsymbol{\beta}]^2)\mathrm{tr}(TT^\top)] \\
&+ \frac{8}{35}k^2 l^{10}[[\boldsymbol{\alpha}TT^\top]^2 + [T^\top T\boldsymbol{\beta}]^2] \\
&+ \frac{1}{735}l^{12}[8\mathrm{tr}(TT^\top TT^\top TT^\top) + \mathrm{tr}(TT^\top)(6\mathrm{tr}(TT^\top TT^\top) + \mathrm{tr}(TT^\top)^3)].
\end{aligned} \tag{9.3.13}$$

Next, we consider nonproduct observables to obtain two invariants; $I_1 = \det(T)$ and $I_{14} = \mathrm{tr}(H_\alpha T H_\beta^\top T^\top)$.

- **For $t = 3$:** For $\mathcal{M}_{\mathrm{det}} = \sum_{i=1}^3 \sigma_i \otimes \sigma_i$, we obtain

$$\begin{aligned}
\mathcal{R}^{(3)}_{\mathcal{M}_{\mathrm{det}}}(\varrho) = \int dU_A \int dU_B \Bigg[&\sum_i \mathrm{tr}(\varrho_U \sigma_i \otimes \sigma_i)^3 \\
&+ 3\sum_{i\neq j} \mathrm{tr}(\varrho_U \sigma_i \otimes \sigma_i)^2 \mathrm{tr}(\varrho_U \sigma_j \otimes \sigma_j) \\
&+ 6\mathrm{tr}(\varrho_U X \otimes X)\mathrm{tr}(\varrho_U Y \otimes Y)\mathrm{tr}(\varrho_U Z \otimes Z)\Bigg],
\end{aligned} \tag{9.3.14}$$

where we denote $\varrho_U = (U_A \otimes U_B)\varrho(U_A^\dagger \otimes U_B^\dagger)$. Now Eq. (9.3.4) leads to

$$\begin{aligned}
\mathcal{R}^{(3)}_{\mathcal{M}_{\mathrm{det}}}(\varrho) &= 6\int dU_A \int dU_B \mathrm{tr}(\varrho_U X \otimes X)\mathrm{tr}(\varrho_U Y \otimes Y)\mathrm{tr}(\varrho_U Z \otimes Z) \\
&= \frac{6\cdot 4\cdot 4}{4^3\cdot 3\cdot 3}\sum_{i_1 i_2 i_3 j_1 j_2 j_3} T_{i_1 j_1} T_{i_2 j_2} T_{i_3 j_3} \epsilon_{i_1 i_2 i_3} \epsilon_{j_1 j_2 j_3} \\
&= \det(T) = I_1.
\end{aligned} \tag{9.3.15}$$

- **For $t = 4$:** For $\mathcal{M}^+_{\mathrm{H}} = \mathbb{1}\otimes X + X \otimes \mathbb{1} + Y \otimes Z + Z \otimes Y$, we have

$$\mathcal{R}^{(4)}_{\mathcal{M}^+_{\mathrm{H}}} = \mathrm{tr}\left[\varrho^{\otimes 4}\int dU_A \int dU_B (U_A \otimes U_B \mathcal{M}^+_{\mathrm{H}} U_A^\dagger \otimes U_B^\dagger)^{\otimes 4}\right], \tag{9.3.16}$$

where

$$\begin{aligned}
&\int dU_A \int dU_B (U_A \otimes U_B \mathcal{M}_{\mathrm{H}}^{+} U_A^\dagger \otimes U_B^\dagger)^{\otimes 4} \\
&= \int dU_A \int dU_B (U_A \otimes U_B)^{\otimes 4} (\mathbb{1}^{\otimes 4} \otimes X^{\otimes 4} + X^{\otimes 4} \otimes \mathbb{1}^{\otimes 4} \\
&+ \mathbb{1}\mathbb{1}XX \otimes XX\mathbb{1}\mathbb{1} + \text{perms.} \\
&+ \mathbb{1}\mathbb{1}YY \otimes XXZZ + \text{perms.} + \mathbb{1}\mathbb{1}ZZ \otimes XXYY + \text{perms.} + \\
&+ XXZZ \otimes \mathbb{1}\mathbb{1}YY + \text{perms.} + XXYY \otimes \mathbb{1}\mathbb{1}ZZ + \text{perms.} + \\
&+ YYZZ \otimes ZZYY + \text{perms.} + Y^{\otimes 4} \otimes Z^{\otimes 4} + Z^{\otimes 4} \otimes Y^{\otimes 4} + \\
&+ \mathbb{1}XYZ \otimes X\mathbb{1}ZY + \text{perms.} + \ldots)(U_A^\dagger \otimes U_B^\dagger)^{\otimes 4}, \qquad (9.3.17)
\end{aligned}$$

where perms. denotes all permutations among the A and B parties of the preceding term. A long but straightforward calculation yields

$$\begin{aligned}
&\mathcal{R}^{(4)}_{\mathcal{M}_{\mathrm{H}}^{+}}(\varrho) \\
&= \ldots + 24 \int dU_A \int dU_B \mathrm{tr}(\varrho_U \mathbb{1} \otimes X)\mathrm{tr}(\varrho_U X \otimes \mathbb{1})\mathrm{tr}(\varrho_U Y \otimes Z)\mathrm{tr}(\varrho_U Z \otimes Y) \\
&= \ldots + \frac{24}{4^4} \sum_{i_2 i_3 i_4 j_1 j_3 j_4} \beta_{j_1} \alpha_{i_2} T_{i_3 j_3} T_{i_4 j_4} \times \\
&\quad \times \int dU_A \mathrm{tr}(\sigma_{i_2} U_A X U_A^\dagger)\mathrm{tr}(\sigma_{i_3} U_A Y U_A^\dagger)\mathrm{tr}(\sigma_{i_4} U_A Z U_A^\dagger) \times \\
&\quad \times \int \mathrm{d}U_B \mathrm{tr}(\sigma_{j_1} U_B X U_B^\dagger)\mathrm{tr}(\sigma_{j_3} U_B Z U_B^\dagger)\mathrm{tr}(\sigma_{j_4} U_B Y U_B^\dagger) \\
&= \ldots - \frac{24 \cdot 4 \cdot 4}{4^4 \cdot 3 \cdot 3} \sum_{i_2 i_3 i_4 j_1 j_3 j_4} \beta_{j_1} \alpha_{i_2} T_{i_3 j_3} T_{i_4 j_4} \epsilon_{i_2 i_3 i_4} \epsilon_{j_1 j_3 j_4} \\
&= \ldots - \frac{1}{6} \sum_{ijklmn} \epsilon_{ijk} \epsilon_{lmn} \alpha_i \beta_l T_{jm} T_{kn} = \ldots - \frac{1}{6} \mathrm{tr}(H_\alpha T H_\beta^\top T^\top). \qquad (9.3.18)
\end{aligned}$$

Similarly, for the case with $\mathcal{M}_{\mathrm{H}}^{-}$, we can obtain the term $\frac{1}{6}\mathrm{tr}(H_\alpha T H_\beta^\top T^\top)$.

□

9.4 Proof of Results 24 and 25 in Chapter 5

Before we show the proof, let us summarize two formulas for Haar unitary integrals, mentioned already in Sec. 1.5:

$$\int dU\, UXU^\dagger = \frac{\mathrm{tr}(X)}{d} \mathbb{1}_d, \qquad (9.4.1)$$

$$\int dU\, U^{\otimes 2} X (U^\dagger)^{\otimes 2} = \frac{1}{d^2 - 1} \left\{ \left[\mathrm{tr}(X) - \frac{\mathrm{tr}(X\mathbb{S})}{d} \right] \mathbb{1}_d^{\otimes 2} - \left[\frac{\mathrm{tr}(X)}{d} - \mathrm{tr}(X\mathbb{S}) \right] \mathbb{S} \right\}, \qquad (9.4.2)$$

where $\mathbb{S}$ is the SWAP operator.

Proof. Let us show Result 24. We begin by writing the TPM work average for a fixed unitary as

$$
\begin{aligned}
&W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)\\
&=\sum_{i,j,k,l} m_{ij}m_{kl|ij}w_{ijkl} \qquad (9.4.3)\\
&=\sum_{i,j} m_{ij}e_{ij}-\sum_{i,j,k,l} m_{ij}m_{kl|ij}e'_{kl}\\
&=\sum_{i,j}\mathrm{tr}[P_i^A\otimes P_j^B\varrho_{AB}]e_{ij}-\sum_{i,j,k,l} m_{ij}\mathrm{tr}[P_k^A\otimes P_l^B\sigma'_{ij}]e'_{kl}\\
&=\mathrm{tr}[\varrho_{AB}H_D]-\sum_{i,j}\mathrm{tr}\left[(U_A\otimes U_B)\sqrt{P_i^A}\otimes\sqrt{P_j^B}\varrho_{AB}\sqrt{P_i^A}\otimes\sqrt{P_j^B}(U_A\otimes U_B)^\dagger H_D\right], \qquad (9.4.4)
\end{aligned}
$$

by virtue of Eq. (5.3.13). In order to derive the unitary average $\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)}$, we first note that

$$\sqrt{P_i^A}=f_{\varepsilon_A}\Pi_i^A+g_{\varepsilon_A}\mathbb{1}_A,\qquad \sqrt{P_i^B}=f_{\varepsilon_B}\Pi_i^B+g_{\varepsilon_B}\mathbb{1}_B, \qquad (9.4.5)$$

with $\mathbb{1}_X=\Pi_i^X+\sum_{j\neq i}\Pi_j^X$. We then define

$$f_{\varepsilon_X}\equiv\sqrt{\varepsilon_X+\frac{1-\varepsilon_X}{d}}-\sqrt{\frac{1-\varepsilon_X}{d}},\qquad g_{\varepsilon_X}\equiv\sqrt{\frac{1-\varepsilon_X}{d}}, \qquad (9.4.6)$$

with the normalization condition

$$f_{\varepsilon_X}^2+2f_{\varepsilon_X}g_{\varepsilon_X}+dg_{\varepsilon_X}^2=1. \qquad (9.4.7)$$

Abbreviating $\Pi_{ij}^{AB}\equiv\Pi_i^A\otimes\Pi_j^B$, a straightforward calculation leads to

$$\sum_{i,j}\sqrt{P_i^A}\otimes\sqrt{P_j^B}\varrho_{AB}\sqrt{P_i^A}\otimes\sqrt{P_j^B}=f_{\varepsilon_A}^2f_{\varepsilon_B}^2\xi_{AB}+\kappa_A\xi_A+\kappa_B\xi_B+\kappa_{AB}\varrho_{AB}, \qquad (9.4.8)$$

where we define

$$
\begin{aligned}
\xi_{AB}&\equiv\sum_{i,j}\Pi_{ij}^{AB}\varrho_{AB}\Pi_{ij}^{AB}, && (9.4.9)\\
\xi_A&\equiv\sum_i\Pi_i^A\otimes\mathbb{1}_B\varrho_{AB}\Pi_i^A\otimes\mathbb{1}_B, && (9.4.10)\\
\xi_B&\equiv\sum_j\mathbb{1}_A\otimes\Pi_j^B\varrho_{AB}\mathbb{1}_A\otimes\Pi_j^B, && (9.4.11)\\
\kappa_{AB}&\equiv\kappa_A\kappa_B/(f_{\varepsilon_A}^2f_{\varepsilon_B}^2), && (9.4.12)\\
\kappa_A&\equiv f_{\varepsilon_A}^2g_{\varepsilon_B}\left(2f_{\varepsilon_B}+dg_{\varepsilon_B}\right), && (9.4.13)\\
\kappa_B&\equiv f_{\varepsilon_B}^2g_{\varepsilon_A}\left(2f_{\varepsilon_A}+dg_{\varepsilon_A}\right). && (9.4.14)
\end{aligned}
$$

From this follows

$$\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)} = \mathrm{tr}[\varrho_{AB}H_D] - \int dU_A \int dU_B \,\mathrm{tr}\left[\left(f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \xi'_{AB} + \kappa_A \xi'_A + \kappa_B \xi'_B + \kappa_{AB}\varrho'_{AB}\right) H_D\right], \tag{9.4.15}$$

where $\chi' = (U_A \otimes U_B)\chi(U_A^\dagger \otimes U_B^\dagger)$ for any $\chi = \xi_{AB}, \xi_A, \xi_B, \varrho_{AB}$. With the help of the formula in Eq. (9.4.1) we straightforwardly arrive at

$$\int dU_A \int dU_B \,\mathrm{tr}\left[\chi' H_D\right] = \frac{\mathrm{tr}[H_D]}{d^2}, \tag{9.4.16}$$

provided that $\mathrm{tr}[\chi'] = 1$. Finally, by applying the normalization condition in Eq. (9.4.7), the proof of Result 24 is completed. □

Proof. Next, let us show Result 25. We begin by recalling that $(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)})^2 = \overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)^2} - \overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)}^2$. Based on the assumption $\mathrm{tr}[H_D] = 0$ and the result of Result 24, the second term simplifies to

$$\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)}^2 = \mathrm{tr}\left[\varrho_{AB}H_D\right]^2. \tag{9.4.17}$$

For the first term $\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)^2}$, let us consider the expansion

$$\begin{aligned}
&\overline{W_{\mathrm{TPM}}(\varepsilon_A,\varepsilon_B)^2} \\
&= \int dU_A \int dU_B \left\{\mathrm{tr}[\varrho_{AB}H_D] - \mathrm{tr}\left[\left(f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \xi'_{AB} + \kappa_A \xi'_A + \kappa_B \xi'_B + \kappa_{AB}\varrho'_{AB}\right) H_D\right]\right\}^2 \\
&= \mathrm{tr}[\varrho_{AB}H_D]^2 + \int dU_A \int dU_B \left\{\mathrm{tr}\left[\left(f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \xi'_{AB} + \kappa_A \xi'_A + \kappa_B \xi'_B + \kappa_{AB}\varrho'_{AB}\right) H_D\right]\right\}^2 \\
&\quad - 2\mathrm{tr}[\varrho_{AB}H_D] \int dU_A \int dU_B \left\{\mathrm{tr}\left[\left(f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \xi'_{AB} + \kappa_A \xi'_A + \kappa_B \xi'_B + \kappa_{AB}\varrho'_{AB}\right) H_D\right]\right\}.
\end{aligned} \tag{9.4.18}$$

By virtue of Eq. (9.4.16) and the assumption $\mathrm{tr}[H_D] = 0$, the third line vanishes. Expanding the second term in the second line, we identify ten types of unitary integrals,

$$\Xi_{\xi_{AB}} = f_{\varepsilon_A}^4 f_{\varepsilon_B}^4 \int dU_A \int dU_B \,\mathrm{tr}\left[\xi'_{AB}H_D\right]^2, \tag{9.4.19}$$

$$\Xi_{\xi_A} = \kappa_A^2 \int dU_A \int dU_B \,\mathrm{tr}\left[\xi'_A H_D\right]^2, \tag{9.4.20}$$

$$\Xi_{\xi_B} = \kappa_B^2 \int dU_A \int dU_B \,\mathrm{tr}\left[\xi'_B H_D\right]^2, \tag{9.4.21}$$

$$\Xi_{\varrho_{AB}} = \kappa_{AB}^2 \int dU_A \int dU_B \,\mathrm{tr}\left[\varrho'_{AB}H_D\right]^2, \tag{9.4.22}$$

and

$$\Xi_{c_1} = f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_A \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_{AB} H_D\right] \cdot \mathrm{tr}\left[\xi'_A H_D\right], \tag{9.4.23}$$

$$\Xi_{c_2} = f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_B \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_{AB} H_D\right] \cdot \mathrm{tr}\left[\xi'_B H_D\right], \tag{9.4.24}$$

$$\Xi_{c_3} = \kappa_A \kappa_B \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_A H_D\right] \cdot \mathrm{tr}\left[\xi'_B H_D\right], \tag{9.4.25}$$

$$\Xi_{c_4} = f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_{AB} \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_{AB} H_D\right] \cdot \mathrm{tr}\left[\varrho'_{AB} H_D\right], \tag{9.4.26}$$

$$\Xi_{c_5} = \kappa_A \kappa_{AB} \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_A H_D\right] \cdot \mathrm{tr}\left[\varrho'_{AB} H_D\right], \tag{9.4.27}$$

$$\Xi_{c_6} = \kappa_B \kappa_{AB} \int dU_A \int dU_B \, \mathrm{tr}\left[\xi'_B H_D\right] \cdot \mathrm{tr}\left[\varrho'_{AB} H_D\right]. \tag{9.4.28}$$

Hence we have

$$\begin{aligned}(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)})^2 &= \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)^2} - \overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)}^2 \\ &= \Xi_{\xi_{AB}} + \Xi_{\xi_A} + \Xi_{\xi_B} + \Xi_{\varrho_{AB}} + 2\sum_{i=1}^{6} \Xi_{c_i}.\end{aligned} \tag{9.4.29}$$

We notice that the fourth term $\Xi_{\varrho_{AB}}/\kappa_{AB}^2$ is equal to the theoretical work variance $(\Delta\overline{W})_D^2$ for the diagonal Hamiltonian H_D in Result 21. The first three terms, $\Xi_{\xi_{AB}}, \Xi_{\xi_A}, \Xi_{\xi_B}$, can be attributed to the noiseless local TPM, and their sum corresponds to the variance $(\Delta\overline{W_{\mathrm{Proj}}})^2$ in Result 23. Finally, all the cross terms Ξ_{c_i} for $i = 1, 6$ vanish in the limits $\varepsilon_A, \varepsilon_B \to 0, 1$; they constitute the additional noise contribution $(\Delta\overline{W_{\mathrm{Noisy}}})^2$ in Result 23.

In order to find the explicit form of $(\Delta\overline{W_{\mathrm{TPM}}(\varepsilon_A, \varepsilon_B)})^2$, we must evaluate all these terms. We begin by recalling the generalized Bloch representation of ϱ_{AB}:

$$\varrho_{AB} = \frac{1}{d^2}\left(\mathbb{1}_{AB} + R_1^A \otimes \mathbb{1}_B + \mathbb{1}_A \otimes R_1^B + T_2\right), \tag{9.4.30}$$

introducing the traceless Hermitian operators

$$R_1^A = \sum_{i=1}^{d^2-1} r_i^A \lambda_i, \quad R_1^B = \sum_{i=1}^{d^2-1} r_i^B \lambda_i, \quad T_2 = \sum_{i,j=1}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j. \tag{9.4.31}$$

For these expressions, we define the quantities

$$r_A^2 = \frac{1}{d}\mathrm{tr}\left[(R_1^A)^2\right] = \sum_{i=1}^{d^2-1} (r_i^A)^2, \tag{9.4.32}$$

$$r_B^2 = \frac{1}{d}\mathrm{tr}\left[(R_1^B)^2\right] = \sum_{i=1}^{d^2-1} (r_i^B)^2, \tag{9.4.33}$$

$$t^2 = \frac{1}{d^2}\mathrm{tr}\left[T_2^2\right] = \sum_{i,j=1}^{d^2-1} t_{ij}^2, \tag{9.4.34}$$

which capture the magnitude of the one- and two-body quantum correlations of ϱ_{AB}. With these expressions, we rewrite the state ξ_{AB} in Eq. (9.4.9) as

$$\xi_{AB} = \sum_{i,j} \Pi_{ij}^{AB} \varrho_{AB} \Pi_{ij}^{AB} = \sum_{i,j} p_{ij}^{AB} \Pi_{ij}^{AB}, \tag{9.4.35}$$

where

$$p_{ij}^{AB} \equiv \mathrm{tr}[\Pi_{ij}^{AB} \varrho_{AB}] = (1/d^2) \left\{ 1 + \mathrm{tr}[\Pi_i^A R_1^A] + \mathrm{tr}[\Pi_j^B R_1^B] + \mathrm{tr}[\Pi_{ij}^{AB} T_2] \right\}. \tag{9.4.36}$$

Also, we define $p_i^A \equiv \sum_j p_{ij}^{AB}$ and $p_j^B \equiv \sum_i p_{ij}^{AB}$. Let us introduce that

$$p_A^2 = \sum_i (p_i^A)^2, \quad p_B^2 = \sum_j (p_j^B)^2, \quad p_{AB}^2 = \sum_{i,j} (p_{ij}^{AB})^2. \tag{9.4.37}$$

By using the formulas in Eq. (9.4.2), a long calculation leaves us with

$$\Xi_{\xi_{AB}} = \frac{f_{\varepsilon_A}^4 f_{\varepsilon_B}^4}{d^2-1} \left[Q_{AB} + \frac{\left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1\right) g^2 v^2}{d^2-1} \right], \tag{9.4.38}$$

$$\Xi_{\xi_A} = \frac{\kappa_A^2}{d^2-1} \left[\left(d p_A^2 - 1\right) h_A^2 + r_B^2 h_B^2 + \frac{g^2 v^2}{d^2-1} \sum_{a,b,c} t_{ab} t_{cb} \zeta_{ac}^A \right], \tag{9.4.39}$$

$$\Xi_{\xi_B} = \frac{\kappa_B^2}{d^2-1} \left[r_A^2 h_A^2 + \left(d p_B^2 - 1\right) h_B^2 + \frac{g^2 v^2}{d^2-1} \sum_{a,b,c} t_{ab} t_{ac} \zeta_{bc}^B \right], \tag{9.4.40}$$

and

$$\Xi_{c_1} = \frac{f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_A}{d^2-1} \left[Q_{AB} + \frac{\left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1\right) g^2 v^2}{d^2-1} \right], \tag{9.4.41}$$

$$\Xi_{c_2} = \frac{f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_B}{d^2-1} \left[Q_{AB} + \frac{\left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1\right) g^2 v^2}{d^2-1} \right], \tag{9.4.42}$$

$$\Xi_{c_3} = \frac{\kappa_A \kappa_B}{d^2-1} \left[Q_{AB} + \frac{(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1) g^2 v^2}{d^2-1} \right], \tag{9.4.43}$$

$$\Xi_{c_4} = \frac{f_{\varepsilon_A}^2 f_{\varepsilon_B}^2 \kappa_{AB}}{d^2-1} \left[Q_{AB} + \frac{\left(d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1\right) g^2 v^2}{d^2-1} \right], \tag{9.4.44}$$

$$\Xi_{c_5} = \frac{\kappa_A \kappa_{AB}}{d^2-1} \left[\left(d p_A^2 - 1\right) h_A^2 + r_B^2 h_B^2 + \frac{g^2 v^2}{d^2-1} \sum_{a,b,c} t_{ab} t_{cb} \zeta_{ac}^A \right], \tag{9.4.45}$$

$$\Xi_{c_6} = \frac{\kappa_B \kappa_{AB}}{d^2-1} \left[r_A^2 h_A^2 + \left(d p_B^2 - 1\right) h_B^2 + \frac{g^2 v^2}{d^2-1} \sum_{a,b,c} t_{ab} t_{ac} \zeta_{bc}^B \right]. \tag{9.4.46}$$

where for the sake of simplicity we denote that

$$Q_{AB} \equiv \left(d p_A^2 - 1\right) h_A^2 + \left(d p_B^2 - 1\right) h_B^2. \tag{9.4.47}$$

Here we introduced

$$\zeta_{ab}^{A} \equiv \sum_{i} \frac{\mathrm{tr}(\Pi_i^A \lambda_a \Pi_i^A \lambda_b)}{d}, \qquad \zeta_{ab}^{B} \equiv \sum_{i} \frac{\mathrm{tr}(\Pi_i^B \lambda_a \Pi_i^B \lambda_b)}{d}. \tag{9.4.48}$$

Summarizing these terms, we can complete the proof of Result 25. Here, it might be useful for some readers to note that

$$\begin{aligned}
\sum_{a,b,c,d} t_{ab} t_{cd} \zeta_{ac}^{A} \zeta_{bd}^{B} &= \frac{1}{d^2} \sum_{i,j} \mathrm{tr}[\Pi_{ij}^{AB} T_2 \Pi_{ij}^{AB} T_2] \\
&= \frac{1}{d^2} \sum_{i,j} \{\mathrm{tr}[\Pi_{ij}^{AB} T_2]\}^2 \\
&= \frac{1}{d^2} \sum_{i,j} \left(d^2 p_{ij}^{AB} - d p_i^A - d p_j^B + 1 \right)^2 \\
&= d^2 p_{AB}^2 - d p_A^2 - d p_B^2 + 1,
\end{aligned} \tag{9.4.49}$$

where we use that $\mathrm{tr}[\Pi_{ij}^{AB} T_2] = d^2 p_{ij}^{AB} - d p_i^A - d p_j^B + 1$. □

9.5 Proof of Result 28 in Chapter 6

Proof. We begin by evaluating the form of $\langle M_4 \rangle$ as follows

$$\begin{aligned}
\langle M_4 \rangle &= \sum_{i=1}^{N} \mathrm{tr}\left[\varrho_i^{\otimes 4} \Phi_4(\sigma_z^{(i)}) \right] \\
&= \frac{1}{2^4} \sum_{i=1}^{N} \sum_{a,b,c,d} r_a^{(i)} r_b^{(i)} r_c^{(i)} r_d^{(i)} \mathcal{I}(a,b,c,d) \\
&= \frac{1}{5} F_1(\theta).
\end{aligned} \tag{9.5.1}$$

Here in the first line, we use that $\Phi(\sigma_z^{(i)})$ only acts on the copies of the i-th system. In the second line, we denote that for $r_p^{(i)} = \mathrm{tr}[\varrho_i \sigma_p^{(i)}]$ for $p = a, b, c, d = x, y, z$ and

$$\mathcal{I}(a,b,c,d) = \int dU \, Z_{U,a}^{(i)} Z_{U,b}^{(i)} Z_{U,c}^{(i)} Z_{U,d}^{(i)}, \tag{9.5.2}$$

where $Z_{U,a}^{(i)} = \mathrm{tr}[\sigma_a^{(i)} U^\dagger \sigma_z^{(i)} U]$. In the third line, we apply the following formula

$$\mathcal{I}(a,b,c,d) = \frac{16}{15} \left(\delta_{a,b}\delta_{c,d} + \delta_{a,c}\delta_{b,d} + \delta_{a,d}\delta_{b,c} \right), \tag{9.5.3}$$

given in Eq. (9.3.3b) and introduce the fourth-order quantity

$$F_1(\theta) = \sum_{i=1}^{N} r_i^4, \tag{9.5.4}$$

where $r_i^2 = \sum_{p=x,y,z}[r_p^{(i)}]^2 = 2\mathrm{tr}[\varrho_i^2] - 1$.

Next, we will evaluate the expression of the variance: $(\Delta M_4)^2 = \langle M_4^2\rangle - \langle M_4\rangle^2$, where

$$\langle M_4^2\rangle = \sum_i \langle \Phi_4(\sigma_z^{(i)})^2\rangle + \sum_{i\neq j}\langle \Phi_4(\sigma_z^{(i)})\Phi_4(\sigma_z^{(j)})\rangle. \tag{9.5.5}$$

The first term in $\langle M_4^2\rangle$ can be given by

$$\begin{aligned}
\sum_i \langle \Phi_4(\sigma_z^{(i)})^2\rangle &= \sum_i \mathrm{tr}\left\{ \left[\varrho_i^{\otimes 4}\Phi_4(\sigma_z^{(i)})\right]_X \otimes [\Phi_4(\sigma_z^{(i)})]_Y \mathbb{S}_{X,Y}\right\} \\
&= \frac{1}{2^4}\sum_i \int dU_X \int dU_Y \left[\mathrm{tr}\left(\chi_x^{(i)} \otimes v_y^{(i)}\mathbb{S}_{x,y}\right)\right]^4 \\
&= \frac{1}{2^4\cdot 2^4}\sum_i \int dU_X \int dU_Y \left[\sum_\alpha \mathcal{Z}_{U_X,\alpha}^{(i)} Z_{U_Y,\alpha}^{(i)}\right]^4 \\
&= \frac{1}{2^4\cdot 2^4}\sum_i \sum_{\alpha,\beta,\gamma,\delta} \mathcal{I}(\alpha,\beta,\gamma,\delta)\sum_{j=0}^4 \mathcal{C}_j^{(i)} \\
&= \frac{1}{5\cdot 15}\left[15N - 20S_1(\theta) + 8F_1(\theta)\right].
\end{aligned} \tag{9.5.6}$$

Here in the first equality, we divide the squared term into two different spaces X, Y using the SWAP trick mentioned in the proof of Result 27. The SWAP $\mathbb{S}_{X,Y}$ acts on the eight-qubit system, where each system $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4\}$ is the four-copy of a single-qubit system.

In the second equality, we use that the SWAP operator in many qubits can be realized by the SWAP operators in individual qubits [107], that is,

$$\mathbb{S}_{X,Y} = \mathbb{S}_{x_1,y_1} \otimes \mathbb{S}_{x_2,y_2} \otimes \mathbb{S}_{x_3,y_3} \otimes \mathbb{S}_{x_4,y_4}. \tag{9.5.7}$$

Also we denote that

$$\begin{aligned}
\chi_x^{(i)} &= U_X^\dagger \sigma_z^{(i)} U_X + \sum_{a=x,y,z} r_a^{(i)}\sigma_a^{(i)} U_X^\dagger \sigma_z^{(i)} U_X, \\
v_y^{(i)} &= U_Y^\dagger \sigma_z^{(i)} U_Y,
\end{aligned} \tag{9.5.8}$$

where $r_a^{(i)} = \mathrm{tr}[\varrho_i \sigma_a^{(i)}]$.

In the third equality, we apply the formulas

$$\begin{aligned}
\mathbb{S} &= \frac{1}{2}\left(\mathbb{1}_2^{\otimes 2} + \sum_{\alpha=x,y,z}\sigma_\alpha \otimes \sigma_\alpha\right), \\
\sigma_p\sigma_q &= \delta_{p,q}\mathbb{1}_2 + i\sum_{r=x,y,z}\varepsilon_{p,q,r}\sigma_r,
\end{aligned} \tag{9.5.9}$$

with the Kronecker-delta symbol $\delta_{p,q}$ and the Levi-Civita symbol $\varepsilon_{p,q,r}$, and denote that

$$\mathcal{Z}^{(i)}_{U_X,\alpha} = Z^{(i)}_{U_X,\alpha} + i \sum_{a,k=x,y,z} \varepsilon_{\alpha,a,k} r^{(i)}_a Z^{(i)}_{U_X,k}, \tag{9.5.10}$$

where $Z^{(i)}_{U_X,\alpha} = \mathrm{tr}[\sigma^{(i)}_\alpha U_X^\dagger \sigma^{(i)}_z U_X]$.

In the fourth equality, we denote that

$$\int dU_X \, \mathcal{Z}^{(i)}_{U_X,\alpha} \mathcal{Z}^{(i)}_{U_X,\beta} \mathcal{Z}^{(i)}_{U_X,\gamma} \mathcal{Z}^{(i)}_{U_X,\delta} = \sum_{j=0}^{4} \mathcal{C}^{(i)}_j, \tag{9.5.11}$$

where $\alpha, \beta, \gamma, \delta = x, y, z$ and the label j in $\mathcal{C}^{(i)}_j$ represents the number of times the imaginary unit i is multiplied.

In the final equality, we indeed evaluate all the terms in $\mathcal{C}^{(i)}_j$ and simplify the expression. Note that $\mathcal{C}^{(i)}_1 = \mathcal{C}^{(i)}_3 = 0$ for any i due to the properties of the Kronecker delta and Levi-Civita symbol.

Let us continue the computation of the variance. The second term in $\langle M_4^2 \rangle$ can be given by

$$\begin{aligned}
\sum_{i \neq j} \langle \Phi_4(\sigma^{(i)}_z) \Phi_4(\sigma^{(j)}_z) \rangle &= \sum_{i \neq j} \mathrm{tr}[\varrho_{ij}^{\otimes 4} \Phi_4(\sigma^{(i)}_z) \Phi_4(\sigma^{(j)}_z)] \\
&= \frac{1}{4^4} \sum_{i \neq j} \sum_{\boldsymbol{a},\boldsymbol{b}} t^{(ij)}_{a_1 b_1} t^{(ij)}_{a_2 b_2} t^{(ij)}_{a_3 b_3} t^{(ij)}_{a_4 b_4} \mathcal{I}(\boldsymbol{a}) \mathcal{I}(\boldsymbol{b}) \\
&= \frac{2}{5 \cdot 15} F_2(\theta).
\end{aligned} \tag{9.5.12}$$

In the second equality, we denote that $\boldsymbol{a} = (a_1, a_2, a_3, a_4)$, $\boldsymbol{b} = (b_1, b_2, b_3, b_4)$, and $t^{(ij)}_{a_p b_p} = \mathrm{tr}(\varrho_{ij} \sigma_{a_p} \otimes \sigma_{b_p})$ for $a_p, b_p = x, y, z$. In the third equality, we use that the sector length can be given by $S_2(\theta) = \sum_{i<j} \mathrm{tr}(T_{ij} T_{ij}^\top) = \sum_{i<j} [4\mathrm{tr}(\varrho_{ij}^2) - 1 - S_1(\theta)]$ with the matrix $[T_{ij}]_{ab} = t^{(ij)}_{ab}$ and introduce the fourth-order two-body quantity

$$F_2(\theta) = \sum_{i<j} \left\{ [\mathrm{tr}(T_{ij} T_{ij}^\top)]^2 + 2\mathrm{tr}(T_{ij} T_{ij}^\top T_{ij} T_{ij}^\top) \right\}. \tag{9.5.13}$$

Hence we can complete the proof. □

9.6 Proof of Result 31 in Chapter 7

Proof. Let us begin by rewriting the moments $\mathcal{C}^{(r)}(\varrho_{ab})$ as

$$\mathcal{C}^{(r)}(\varrho_{ab}) = \frac{1}{4^r} \int dU \left[\sum_{i,j=x,y,z} C_{ij} \mathcal{O}^{(i)}_U \mathcal{O}^{(j)}_U \right]^r, \tag{9.6.1}$$

where we define that $\mathcal{O}_U^{(i)} = \mathrm{tr}[\sigma_i U \sigma_z U^\dagger]$. Using the formulas in Eqs. (9.3.3a, 9.3.3b, 9.3.3b), we can straightforwardly obtain the following expressions

$$\mathcal{C}^{(1)}(\varrho_{ab}) = \frac{1}{3}\mathrm{tr}(C), \tag{9.6.2a}$$

$$\mathcal{C}^{(2)}(\varrho_{ab}) = \frac{1}{15}\left[\mathrm{tr}(C)^2 + \mathrm{tr}(CC^\top) + \mathrm{tr}(C^2)\right], \tag{9.6.2b}$$

$$\mathcal{C}^{(3)}(\varrho_{ab}) = \frac{1}{105}\Big\{\mathrm{tr}(C)\left[\mathrm{tr}(C)^2 + 3\mathrm{tr}(C^2) + 3\mathrm{tr}(CC^\top)\right] + 4\mathrm{tr}(C^2C^\top) + 2\mathrm{tr}(CC^\top C^\top) + 2\mathrm{tr}(C^3)\Big\}. \tag{9.6.2c}$$

Furthermore, using the symmetric condition $C = C^\top$, we can finally arrive at

$$\mathcal{C}^{(1)}(\varrho_{ab}) = \frac{1}{3}\mathrm{tr}(C), \tag{9.6.3a}$$

$$\mathcal{C}^{(2)}(\varrho_{ab}) = \frac{1}{15}\left[\mathrm{tr}(C)^2 + 2\mathrm{tr}(C^2)\right], \tag{9.6.3b}$$

$$\mathcal{C}^{(3)}(\varrho_{ab}) = \frac{1}{105}\left\{\mathrm{tr}(C)\left[\mathrm{tr}(C)^2 + 6\mathrm{tr}(C^2)\right] + 8\mathrm{tr}(C^3)\right\}. \tag{9.6.3c}$$

The moments $\mathcal{C}^{(r)}(\varrho_{ab})$, equivalently $\mathcal{J}^{(r)}(\varrho)$, are directly connected to $\mathrm{tr}[C^r]$. Hence we complete the proof. □

9.7 Proof of Results 32 and 33 in Chapter 7

Proof. Here we give the derivation of Eq. (7.4.1). Let us begin by writing that

$$\mathcal{J}^{(1)}(\varrho) = 3\int dU\,(\Delta J_z)_U^2, \tag{9.7.1}$$

and

$$\begin{aligned}
&(\Delta J_z)_U^2 \\
&= \langle U^{\otimes N} J_z^2 (U^\dagger)^{\otimes N}\rangle_\varrho - \langle U^{\otimes N} J_z (U^\dagger)^{\otimes N}\rangle_\varrho^2 \\
&= \frac{1}{4}\sum_{i,j=1}^N \langle U^{\otimes N}\sigma_z^{(i)} \otimes \sigma_z^{(j)} (U^\dagger)^{\otimes N}\rangle_\varrho - \frac{1}{4}\sum_{i,j=1}^N \langle U^{\otimes N}\sigma_z^{(i)} (U^\dagger)^{\otimes N}\rangle_\varrho \langle U^{\otimes N}\sigma_z^{(j)} (U^\dagger)^{\otimes N}\rangle_\varrho \\
&= \frac{1}{4}\left\{N + \sum_{i\neq j}^N \mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)} \otimes \sigma_z^{(j)} (U^\dagger)^{\otimes 2}\varrho_{ij}\right] - \sum_{i,j=1}^N \mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\varrho_j\right]\right\},
\end{aligned} \tag{9.7.2}$$

where ϱ_{ij} and ϱ_i are the two-qubit and single-qubit reduced states of ϱ. Let us focus on the second term in Eq. (9.7.2) and take the Haar unitary average

$$\begin{aligned}
&\sum_{i\neq j}^{N}\int dU \,\mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right]\\
&=\frac{1}{4}\sum_{i\neq j}^{N}\int dU \,\mathrm{tr}\left[U^{\otimes 2}\sigma_z^{(i)}\otimes\sigma_z^{(j)}(U^\dagger)^{\otimes 2}\sum_{k,l=x,y,z}t_{kl}^{(i,j)}\sigma_k^{(i)}\otimes\sigma_l^{(j)}\right]\\
&=\frac{1}{4}\sum_{i\neq j}^{N}\sum_{k,l=x,y,z}t_{kl}^{(i,j)}\int dU \,\mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\sigma_k^{(i)}\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\sigma_l^{(j)}\right]\\
&=\frac{1}{3}\sum_{i\neq j}^{N}\sum_{l=x,y,z}t_{ll}^{(i,j)}=\frac{4}{3}\sum_{l=x,y,z}\langle J_l^2\rangle-N,
\end{aligned}\tag{9.7.3}$$

where $t_{kl}^{(i,j)}=\langle\sigma_k^{(i)}\otimes\sigma_l^{(j)}\rangle_{\varrho_{ij}}$. Similarly, the third term in Eq. (9.7.2) can be given by

$$\sum_{i,j=1}^{N}\int dU \,\mathrm{tr}\left[U\sigma_z^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\sigma_z^{(j)}U^\dagger\varrho_j\right]=\frac{4}{3}\sum_{l=x,y,z}\langle J_l\rangle^2.\tag{9.7.4}$$

Summarizing these results, we can thus arrive at

$$\mathcal{J}^{(1)}(\varrho)=\frac{3}{4}\left\{N+\frac{4}{3}\sum_{l=x,y,z}\langle J_l^2\rangle-N+\frac{4}{3}\sum_{l=x,y,z}\langle J_l\rangle^2\right\}=\sum_{l=x,y,z}(\Delta J_l)^2.\tag{9.7.5}$$

□

Proof. Next, let us show Result 33. Similarly to Eq. (9.7.2), the random variance $(\Delta\Lambda_l)_U^2$ can be written as

$$(\Delta\Lambda_l)_U^2=\frac{1}{d^2}\Bigg\{\sum_{i=1}^{N}\mathrm{tr}[U(\lambda_l^{(i)})^2U^\dagger\varrho_i]+\sum_{i\neq j}^{N}\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right]\tag{9.7.6}$$

$$-\sum_{i,j=1}^{N}\mathrm{tr}\left[U\lambda_l^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\lambda_l^{(j)}U^\dagger\varrho_j\right]\Bigg\},\tag{9.7.7}$$

where ϱ_{ij} and ϱ_i are the two-qudit and single-qudit reduced states of ϱ. To evaluate the Haar unitary integral, let us recall the formulas in Eqs. (9.4.1,9.4.2). Thus we first obtain

$$\sum_{i=1}^{N}\int dU \,\mathrm{tr}[U(\lambda_l^{(i)})^2U^\dagger\varrho_i]=\sum_{i=1}^{N}\frac{\mathrm{tr}[(\lambda_l^{(i)})^2]}{d}\mathrm{tr}[\varrho_i]=N.\tag{9.7.8}$$

Next, we have

$$\begin{aligned}
&\sum_{i\neq j}^{N}\int dU\,\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\varrho_{ij}\right]\\
&=\frac{1}{d^2}\sum_{i\neq j}^{N}\int dU\,\mathrm{tr}\left[U^{\otimes 2}\lambda_l^{(i)}\otimes\lambda_l^{(j)}(U^\dagger)^{\otimes 2}\sum_{m,n=1}^{d^2-1}t_{mn}^{(i,j)}\lambda_m^{(i)}\otimes\lambda_n^{(j)}\right]\\
&=\frac{1}{d^2}\frac{1}{d^2-1}\sum_{i\neq j}^{N}\sum_{m,n=1}^{d^2-1}t_{mn}^{(i,j)}\mathrm{tr}\left[(d\mathbb{S}-\mathbb{1}_d^{\otimes 2})\lambda_m^{(i)}\otimes\lambda_n^{(j)}\right]\\
&=\frac{1}{d^2-1}\sum_{i\neq j}^{N}\sum_{l=1}^{d^2-1}t_{ll}^{(i,j)}\\
&=\frac{d^2}{d^2-1}\sum_{l=1}^{d^2-1}\langle\Lambda_l^2\rangle-N.
\end{aligned}\tag{9.7.9}$$

In the first line, we denote that $t_{mn}^{(i,j)}=\langle\lambda_m^{(i)}\otimes\lambda_n^{(j)}\rangle_{\varrho_{ij}}$. In the second line, we used the formula in Eq. (9.4.2) and the so-called SWAP trick: $\mathrm{tr}[\mathbb{S}X]=\mathrm{tr}[\mathbb{S}(X_A\otimes X_B)]=\mathrm{tr}[X_AX_B]$ for an operator $X=X_A\otimes X_B$. In the final line, we used that $\sum_{l=1}^{d^2-1}\lambda_l^2=(d^2-1)\mathbb{1}_d$, which can be derived from the facts that $\mathbb{S}=\frac{1}{d}\sum_{l=0}^{d^2-1}\lambda_l\otimes\lambda_l$ and $\mathbb{S}^2=\mathbb{1}_d^{\otimes 2}$. Similarly, we obtain

$$\begin{aligned}
\sum_{i,j=1}^{N}\int dU\,\mathrm{tr}\left[U\lambda_l^{(i)}U^\dagger\varrho_i\right]\mathrm{tr}\left[U\lambda_l^{(j)}U^\dagger\varrho_j\right]&=\frac{1}{d^2-1}\sum_{i,j=1}^{N}\left[d\mathrm{tr}(\varrho_i\varrho_j)-1\right]\\
&=\frac{d^2}{d^2-1}\sum_{l=1}^{d^2-1}\langle\Lambda_l\rangle^2.
\end{aligned}\tag{9.7.10}$$

Summarizing these results, we can complete the proof. □

9.8 Proof of Result 34 in Chapter 7

Proof. Here we give the derivation of Eq. (7.5.5). Let us begin by recalling

$$\mathcal{T}(\varrho)=\int dU\,\mathrm{tr}\left[\varrho U^{\otimes N}\mathcal{O}_{\mathcal{A}}(U^\dagger)^{\otimes N}\right],\quad \mathcal{O}_{\mathcal{A}}=\sum_{i<j<k}\mathcal{A}\left(\sigma_x^{(i)}\otimes\sigma_y^{(j)}\otimes\sigma_z^{(k)}\right),\tag{9.8.1}$$

where $\mathcal{A}$ represents a linear mapping that can make the antisymmetrization (or alternatization) by summing over even permutations and subtracting the sum over odd permutations. More precisely, the observable can be rewritten as

$$\mathcal{O}_{\mathcal{A}}=\sum_{i<j<k}\sum_{l,m,n=x,y,z}\varepsilon_{lmn}\sigma_l^{(i)}\otimes\sigma_m^{(j)}\otimes\sigma_n^{(k)}.\tag{9.8.2}$$

For instance, in the three-qubit system ABC, it is given by

$$\begin{aligned}\mathcal{O}_{\mathcal{A}} = &\sigma_x^{(A)} \otimes \sigma_y^{(B)} \otimes \sigma_z^{(C)} + \sigma_y^{(A)} \otimes \sigma_z^{(B)} \otimes \sigma_x^{(C)} + \sigma_z^{(A)} \otimes \sigma_x^{(B)} \otimes \sigma_y^{(C)} \\ &- \sigma_x^{(A)} \otimes \sigma_z^{(B)} \otimes \sigma_y^{(C)} - \sigma_y^{(A)} \otimes \sigma_x^{(B)} \otimes \sigma_z^{(C)} - \sigma_z^{(A)} \otimes \sigma_y^{(B)} \otimes \sigma_x^{(C)}. \end{aligned} \tag{9.8.3}$$

Then we have

$$\begin{aligned}\mathcal{T}(\varrho) &= \sum_{i<j<k} \sum_{l,m,n=x,y,z} \varepsilon_{lmn} \left\{ \int dU \operatorname{tr}\left[\varrho_{ijk} U^{\otimes 3} \sigma_l^{(i)} \otimes \sigma_m^{(j)} \otimes \sigma_n^{(k)} (U^\dagger)^{\otimes 3}\right] \right\} \\ &= \frac{1}{2^3} \sum_{i<j<k} \sum_{l,m,n=x,y,z} \sum_{a,b,c=x,y,z} \varepsilon_{lmn} \xi_{abc}^{(i,j,k)} \\ &\times \int dU \operatorname{tr}[\sigma_a^{(i)} U \sigma_l^{(i)} U^\dagger] \operatorname{tr}[\sigma_b^{(j)} U \sigma_m^{(j)} U^\dagger] \operatorname{tr}[\sigma_c^{(k)} U \sigma_n^{(k)} U^\dagger], \end{aligned} \tag{9.8.4}$$

where ϱ_{ijk} is the three-qubit reduced state of ϱ for $i,j,k = 1,2,\ldots,N$ with the three-body correlation $\xi_{abc}^{(i,j,k)} = \operatorname{tr}[\varrho_{ijk} \sigma_a^{(i)} \sigma_b^{(j)} \sigma_c^{(k)}]$ for $a,b,c = x,y,z$.

To evaluate the Haar unitary integral, we use the formula in Eq. (9.3.4), which leads to

$$\begin{aligned}\mathcal{T}(\varrho) &= \frac{1}{2^3} \frac{4}{3} \sum_{i<j<k} \sum_{l,m,n=x,y,z} \sum_{a,b,c=x,y,z} \varepsilon_{lmn} \xi_{abc}^{(i,j,k)} \varepsilon_{abc} \\ &= \sum_{i<j<k} \sum_{a,b,c=x,y,z} \xi_{abc}^{(i,j,k)} \varepsilon_{abc}. \end{aligned} \tag{9.8.5}$$

Hence we can complete the proof. □

9.9 Proof of Result 37 in Chapter 7

Proof. We begin by writing

$$\mathcal{G}_{AB}^{(r)} = g \int dU_A \int dU_B \, [\eta_{U_{AB}}]^r, \;\; \eta_{U_{AB}} = (\Delta J_z^+)^2_{U_{AB}} - (\Delta J_z^-)^2_{U_{AB}}, \tag{9.9.1a}$$

$$\mathcal{J}_X^{(r)}(\varrho_X) = \int dU_X \, [f_U(\varrho_X)]^r, \;\; f_U(\varrho_X) = \alpha (\Delta J_{z,X})^2_{U_X} + \beta \langle J_{z,X} \rangle^2_{U_X} + \gamma, \tag{9.9.1b}$$

where

$$\langle J_z^\pm \rangle_{U_{AB}} = \operatorname{tr}\left[\varrho_{AB} U_{AB}^{\otimes N} J_z^\pm (U_{AB}^\dagger)^{\otimes N}\right], \;\; (\Delta J_z^\pm)^2_{U_{AB}} = \langle (J_z^\pm)^2 \rangle_{U_{AB}} - \langle J_z^\pm \rangle^2_{U_{AB}}, \tag{9.9.2a}$$

$$J_z^\pm = J_{z,A} \pm J_{z,B}, \;\; J_{z,X} = \frac{1}{2} \sum_{i=1}^N \sigma_z^{(X_i)}, \;\; U_{AB} = U_A \otimes U_B. \tag{9.9.2b}$$

Then we can have

$$\langle J_z^\pm \rangle^2_{U_{AB}} = \langle J_{z,A} \rangle^2_{U_A} + \langle J_{z,B} \rangle^2_{U_B} \pm 2 \langle J_{z,A} \rangle_{U_A} \langle J_{z,B} \rangle_{U_B}, \tag{9.9.3a}$$

$$\begin{aligned}(\Delta J_z^\pm)^2_{U_{AB}} &= (\Delta J_{z,A})^2_{U_A} + (\Delta J_{z,B})^2_{U_B} \\ &\quad \pm 2 \left[\langle J_{z,A} \otimes J_{z,B} \rangle_{U_{AB}} - \langle J_{z,A} \rangle_{U_A} \langle J_{z,B} \rangle_{U_B}\right], \end{aligned} \tag{9.9.3b}$$

$$\eta_{U_{AB}} = 4 \left[\langle J_{z,A} \otimes J_{z,B} \rangle_{U_{AB}} - \langle J_{z,A} \rangle_{U_A} \langle J_{z,B} \rangle_{U_B}\right]. \tag{9.9.3c}$$

Let us evaluate the form of $\mathcal{G}^{(2)}_{AB}(\varrho_{AB})$. Applying the assumption that ϱ_A and ϱ_B are permutational symmetric, we can further simplify the form of $\eta_{U_{AB}}$

$$\begin{aligned}\eta_{U_{AB}} &= 4\frac{1}{2}\frac{1}{2}\Big\{ \sum_{i,j=1}^{N} \mathrm{tr}[\varrho_{A_iB_j} U_A \sigma_z^{(A_i)} U_A^\dagger \otimes U_B \sigma_z^{(B_j)} U_B^\dagger] \\ &\quad - \sum_{i,j=1}^{N} \mathrm{tr}[\varrho_{A_i} U_A \sigma_z^{(A_i)} U_A^\dagger]\mathrm{tr}[\varrho_{B_i} U_B \sigma_z^{(B_i)} U_B^\dagger] \Big\} \\ &= \frac{N^2}{4} \sum_{p,q=x,y,z} C_{pq} \mathcal{O}^{(p)}_{U_A} \mathcal{O}^{(q)}_{U_B}, \end{aligned} \tag{9.9.4}$$

where the covariance matrix $C = (C_{pq})$ is given by

$$C_{pq} = \mathrm{tr}[\varrho_{A_iB_j} \sigma_p^{(A_i)} \otimes \sigma_q^{(B_j)}] - \mathrm{tr}[\varrho_{A_i} \sigma_p^{(A_i)}]\mathrm{tr}[\varrho_{B_j} \sigma_q^{(B_j)}] = t_{pq} - a_p b_q, \tag{9.9.5}$$

for the two-qubit reduced state $\varrho_{A_iB_j} = \mathrm{tr}_{\overline{ij}}(\varrho_{AB})$ such that both particles are still spatially separated, defined in $\mathcal{H}_{A_i} \otimes \mathcal{H}_{B_j}$. Here we denote that

$$\mathcal{O}^{(p)}_{U_X} = \mathrm{tr}\left[\sigma_p^{(X_i)} U_X \sigma_z^{(X_i)} U_X^\dagger\right], \tag{9.9.6}$$

for $X_i = A_i, B_i$. Notice that C_{pq} and $\mathcal{O}^{(p)}_{U_X}$ are independent of indices i, j due to the permutational symmetry.

To avoid confusion, we have to stress that the above covariance matrix $C = (C_{pq})$ is different from Eq. (7.3.5) in general. If the spatially-separated reduced state $\varrho_{A_iB_j}$ is also permutationally symmetric, both are the same, but here we do not require the assumption.

Using the formula in Eq. (9.3.3a), we have that

$$\begin{aligned}\mathcal{G}^{(2)}_{AB}(\varrho_{AB}) &= g\frac{N^4}{4^2} \sum_{p,q,r,s=x,y,z} C_{pq}C_{rs} \int dU_A\, \mathcal{O}^{(p)}_{U_A}\mathcal{O}^{(r)}_{U_A} \int dU_B\, \mathcal{O}^{(q)}_{U_B}\mathcal{O}^{(s)}_{U_B} \\ &= \sum_{p,q=x,y,z} C_{pq}^2, \end{aligned} \tag{9.9.7}$$

where we set that $g = (3/N^2)^2$. Also, since $\langle J_{z,A}\rangle_{U_A} = (N/4)\sum_{p=x,y,z} a_p \mathcal{O}^{(p)}_{U_A}$ and $\beta = 12/N^2$, we can find

$$\mathcal{J}^{(1)}_A(\varrho_A) = \beta\frac{N^2}{4^2} \sum_{p,q=x,y,z} a_p a_q \int dU_A\, \mathcal{O}^{(p)}_{U_A}\mathcal{O}^{(q)}_{U_A} = \sum_{p=x,y,z} a_p^2, \tag{9.9.8}$$

as well as $\mathcal{J}^{(1)}_B(\varrho_B) = \sum_{p=x,y,z} b_p^2$. In summary, for the choice $g = (3/N^2)^2$ and $(\alpha, \beta, \gamma) = (0, 12/N^2, 0)$, we have that

$$\mathcal{G}^{(2)}_{AB} + \mathcal{J}^{(1)}_A + \mathcal{J}^{(1)}_B - \mathcal{J}^{(1)}_A\mathcal{J}^{(1)}_B = \sum_{p,q=x,y,z} C_{pq}^2 + \sum_{p=x,y,z}(a_p^2 + b_p^2) - \sum_{p,q=x,y,z} a_p^2 b_q^2. \tag{9.9.9}$$

To derive the entanglement criterion, we rewrite the above right-hand side as

$$\mathcal{G}_{AB}^{(2)} + \mathcal{J}_{A}^{(1)} + \mathcal{J}_{B}^{(1)} - \mathcal{J}_{A}^{(1)}\mathcal{J}_{B}^{(1)} = \sum_{p,q=x,y,z} (t_{pq}^2 - 2a_p b_q t_{pq}) + \sum_{p=x,y,z} (a_p^2 + b_p^2), \tag{9.9.10}$$

where we use that $C_{pq}^2 = t_{pq}^2 + a_p^2 b_q^2 - 2a_p b_q t_{pq}$. To proceed furthermore, we recall the so-called T_2 separability criterion presented in Ref. [416] (see, Proposition 5): if a bipartite quantum state ϱ_{XY} is separable, then it obeys that

$$\mathrm{tr}(\varrho_{XY}^2) + \mathrm{tr}(\varrho_{X}^2) + \mathrm{tr}(\varrho_{Y}^2) - 2\mathrm{tr}[\varrho_{XY}(\varrho_X \otimes \varrho_Y)] \leq 1. \tag{9.9.11}$$

If ϱ_{XY} is a two-qubit state, we can rewrite this inequality as

$$\sum_{i,j=x,y,z} (z_{ij}^2 - 2x_i y_j z_{ij}) + \sum_{i=x,y,z} (x_i^2 + y_i^2) \leq 1, \tag{9.9.12}$$

where $x_i = \mathrm{tr}(\varrho_X \sigma_i)$, $y_i = \mathrm{tr}(\varrho_Y \sigma_i)$, and $z_{ij} = \mathrm{tr}(\varrho_{XY} \sigma_i \otimes \sigma_j)$. Let us apply this criterion to Eq. (9.9.10). Exchanging the symbols

$$x_i \longleftrightarrow a_p, \quad y_i \longleftrightarrow b_p \quad z_{ij} \longleftrightarrow t_{pq}, \tag{9.9.13}$$

we can connect this criterion to Eq. (9.9.10) and arrive at the inequality in Result 37. Hence we can complete the proof. □

Part III

Geometry of quantum states

Chapter 10

Geometry of two-body correlations in three-qubit states

This thesis has developed several methods to detect and analyze quantum entanglement in terms of local unitary invariants. This Chapter addresses the question of whether one can characterize three-qubit states only using two-body marginal quantities which are invariant under local unitaries. This Chapter provides several bounds on quantum states from geometrical perspectives. This Chapter is based on Ref. [11].

10.1 Introduction

The characterization of quantum states from a restricted and accessible set of parameters is of interest in quantum theory [23]. A famous example is the so-called Bloch sphere, where the state space of a single-qubit is represented by a three-dimensional unit ball, each quantum state corresponding uniquely to a point of the ball [19, 575]. A surface (or interior) point of this sphere corresponds to a pure (or mixed state), and the length of its radius describes the state's purity, a quantity that remains invariant under unitary rotations. The state space of higher-dimensional and multipartite quantum systems, however, is a complicated high-dimensional object. Describing relevant properties of this object from a reduced set of parameters is interesting for several reasons.

First, it allows us to see regularities and structures and describe them in a compact way. Second, a full description of a high-dimensional quantum state is often not available for computational limitations. Third, a reduced set of parameters allows to visualize relevant properties of the quantum state space in lower dimensions. Many efforts have been devoted to the geometrical characterization of quantum features in terms of separable balls [576], single qutrits [30, 31], two qubits [64, 577], three qubits [352], many qubits [160, 320, 578], and Majorana representation [579].

In this Chapter, we study the problem of characterizing multipartite quantum states from limited information on their two-body marginal correlations. This

is connected to the quantum marginal problem, where properties of a global multipartite state can be inferred from the local properties of the parties and correlations between a reduced number of parties [203, 580–588]. We study restrictions on the allowed two-body correlations of a three-qubit system and derive several properties of the global state from its two-body correlations.

Let ϱ_{ABC} be a three-qubit state and let $\varrho_{AB} = \mathrm{tr}_C(\varrho_{ABC})$ be its two-qubit reduced state between the systems A and B, as well as ϱ_{BC} and ϱ_{CA}. Consider the two-body correlations of the reduced states based on the Pauli matrices σ_i for $i = 1, 2, 3$:

$$S_2^{AB} = \sum_{i,j=1}^{3} \langle \sigma_i \otimes \sigma_j \rangle_{\varrho_{AB}}^2 , \tag{10.1.1}$$

$$S_2^{BC} = \sum_{i,j=1}^{3} \langle \sigma_i \otimes \sigma_j \rangle_{\varrho_{BC}}^2 , \tag{10.1.2}$$

$$S_2^{CA} = \sum_{i,j=1}^{3} \langle \sigma_i \otimes \sigma_j \rangle_{\varrho_{CA}}^2 . \tag{10.1.3}$$

The quantities S_2^{XY} for $X, Y = A, B, C$ are invariant under local unitaries, and they can be understood as the generalization of the length in the Bloch sphere. We aim to characterize a three-qubit ϱ_{ABC} in the three-dimensional state space with three coordinates $(x, y, z) = (S_2^{AB}, S_2^{BC}, S_2^{CA})$.

Several works have analyzed quantum states in similar directions. One research line is to extend it to k-body correlations for a N-particle quantum state, and their average overall subsystems are called k-body sector length in Eq. (1.4.7), e.g., $S_2 = S_2^{AB} + S_2^{BC} + S_2^{CA}$. For two-qubits there exists a full restriction of one- and two-body sectors [352, 589, 590]. It was shown that any three-qubit pure state obeys $S_2 = 3$, which can be proven based on the Schmidt decomposition (see [19]).

Another research line is to develop practical methods for accessing S_2^{XY} or more generally sector lengths without state tomography. Recently, randomized measurement schemes with Haar random local unitaries have been used to obtain them in Sec. 1.4. In this scheme, spatially-separated parties do not need to align the same coordinate measurement settings.

The goal of this Chapter is to address the following issues. First, we find bounds on three-qubit pure states, which are tighter than the existing condition $S_2 = 3$ in the state space. Our bounds can be expressed in non-linear combinations of each coordinate. Second, we present systematic methods to obtain linear polytopes for mixed separable states. These results allow us to detect multipartite entanglement from marginal correlations that are invariant under local unitaries. Finally, we discuss the necessary conditions for the two-body correlations based on the rank of the states.

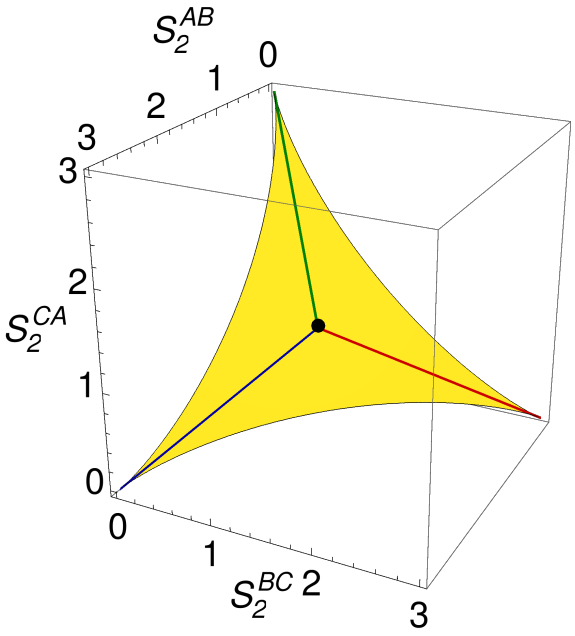

Figure 10.1: The nonlinear allowed set of the pure three-qubit states in the coordinate space $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ based on Result 42. The Blue, Red, and Green lines, respectively represent the states that are biseparable in the $AB|C$, $BC|A$, and $CA|B$ partitions. The black dot contains the fully separable states. This figure is a modified version of a figure from Ref. [11].

10.2 Pure states

In this section, we consider a three-qubit pure state ϱ_{ABC}. We begin by noting that for any three-qubit pure state, the condition $S_2 = 3$ holds. At the same time, this is not the strongest restriction on the set of points $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ compatible with a pure three-qubit state. Here, we can present the first main result of this Chapter:

Result 42. *For any three-qubit pure state the linear condition* $S_2^{AB} + S_2^{BC} + S_2^{CA} = 3$ *holds. It further holds that*

$$\sqrt{S_2^{AB}} + \sqrt{S_2^{BC}} - \sqrt{S_2^{CA}} \leq \sqrt{3}, \tag{10.2.1a}$$

$$\sqrt{S_2^{AB}} - \sqrt{S_2^{BC}} + \sqrt{S_2^{CA}} \leq \sqrt{3}, \tag{10.2.1b}$$

$$-\sqrt{S_2^{AB}} + \sqrt{S_2^{BC}} + \sqrt{S_2^{CA}} \leq \sqrt{3}, \tag{10.2.1c}$$

Remark 56. The proof of this Result will be given after Result 43. The set of points attainable by pure three-qubit states is displayed in Fig. 10.1.

There are several noteworthy facts on Result 42. The non-linear inequalities in Eqs. (10.2.1a)-(10.2.1c) describe a two-dimensional region that is strictly smaller than the previously known region described by $S_2 = 3$, see Fig. 10.1. In

fact, the inequalities are tight, for every point in this region there exists a pure state that is mapped to this point. Each inequality is saturated by one of the following state families belonging to the W class:

$$|\xi_1(p)\rangle = p\,|001\rangle + f_p^+\,|010\rangle + f_p^-\,|100\rangle\,, \tag{10.2.2a}$$
$$|\xi_2(p)\rangle = p\,|010\rangle + f_p^+\,|100\rangle + f_p^-\,|001\rangle\,, \tag{10.2.2b}$$
$$|\xi_3(p)\rangle = p\,|100\rangle + f_p^+\,|001\rangle + f_p^-\,|010\rangle\,, \tag{10.2.2c}$$

where $0 \leq p \leq 1/\sqrt{2}$ and $f_p^\pm = (\sqrt{2-3p^2} \pm p)/2$.

If a state is product with respect to a bipartition $A|BC$ written as $|\psi_{A|BC}\rangle = |\psi_A\rangle \otimes |\psi_{BC}\rangle$, then it follows that $S_2^{AB} = S_2^{CA} \leq 1$. This can be shown using the condition $S_2^{AB} + S_2^{BC} + S_2^{CA} = 3$ and the product formula $S_2^{XY}(\varrho_X \otimes \varrho_Y) = S_1^X(\varrho_X)S_1^Y(\varrho_Y)$ (see Sec. 1.4) for single-particle states ϱ_X and ϱ_Y. Similarly, one can find the cases for the other two bipartitions $B|CA$ and $C|AB$. These separability conditions for $A|BC$, $B|CA$, and $C|AB$ are respectively represented by the Red, Green, and Blue lines in Fig. 10.1, where a state on each line corresponds, up to local unitaries, to one of the following biseparable states

$$|\phi(\theta)\rangle_{X|YZ} = |0\rangle_X \otimes (\cos(\theta)\,|00\rangle_{YZ} + \sin(\theta)\,|11\rangle_{YZ}) \tag{10.2.3}$$

for $\theta \in [0, \pi/2]$ and $X, Y = A, B, C$. Since it has to obey all three conditions, any full-product state $|\psi_{\text{fs}}\rangle = |a\rangle \otimes |b\rangle \otimes |c\rangle$ is mapped to the center point $(1, 1, 1)$. Any pure state mapped outside of these lines is genuinely three-qubit entangled.

However, the converse is not true, there exist pure entangled states that are mapped to the biseparable lines. If a three-qubit state ϱ_{ABC} is permutationally invariant under the exchange of two qubits $X, Y = A, B, C$, that is, $\mathbb{S}_{XY}\varrho_{ABC}\mathbb{S}_{XY} = \varrho_{ABC}$ with the swap operator between X, Y qubits, then it holds that $S_2^{XZ} = S_2^{YZ}$, which can be immediately shown using $\mathbb{S}(A \otimes B)\mathbb{S} = B \otimes A$ for any operators A, B. States that are invariant under the exchange of all three qubits such as the symmetric Greenberger–Horne–Zeilinger (GHZ) state $|\text{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ and the W state $|\text{W}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ are mapped to the point $(1, 1, 1)$. This means that any pure state with some symmetry cannot be distinguished from a biseparable or fully separable state from its two-body correlations alone. In the following, we will overcome this issue by adding the three-body correlations as another parameter.

To proceed, let us first define the three-body sector length as

$$S_3^{ABC} = \sum_{i,j,k=1}^{3} \langle \sigma_i \otimes \sigma_j \otimes \sigma_k \rangle_{\varrho_{ABC}}^2 . \tag{10.2.4}$$

Again, this is invariant under local unitaries. Here we can make the following result:

Result 43. *For any three-qubit pure state, it holds that*

$$S_3^{ABC} \leq 3 + \min(S_2^{AB}, S_2^{BC}, S_2^{CA}), \tag{10.2.5}$$

and

$$\sqrt{S_2^{AB}+\Delta}+\sqrt{S_2^{BC}+\Delta}-\sqrt{S_2^{CA}+\Delta}\leq\sqrt{3}, \tag{10.2.6a}$$

$$\sqrt{S_2^{AB}+\Delta}-\sqrt{S_2^{BC}+\Delta}+\sqrt{S_2^{CA}+\Delta}\leq\sqrt{3}, \tag{10.2.6b}$$

$$-\sqrt{S_2^{AB}+\Delta}+\sqrt{S_2^{BC}+\Delta}+\sqrt{S_2^{CA}+\Delta}\leq\sqrt{3}, \tag{10.2.6c}$$

where $\Delta\equiv 3-S_3^{ABC}\in[-1,2]$.

Proof. First, we note that Result 42 follows from Result 43 for $\Delta=0$. According to Ref. [352], any three-qubit pure state obeys

$$S_2^{AB}+S_2^{BC}+S_2^{CA}=3, \tag{10.2.7}$$

$$S_1^{A}+S_1^{B}+S_1^{C}+S_3^{ABC}=4. \tag{10.2.8}$$

The purity of any two marginals is equal, which we reformulate to

$$S_1^{X}+S_1^{Y}+S_2^{XY}=1+2S_1^{Z}, \tag{10.2.9}$$

where $X,Y,Z=A,B,C$. From this, it follows

$$S_1^{X}=1+\tfrac{1}{3}S_2^{YZ}-\tfrac{1}{3}S_3^{XYZ}. \tag{10.2.10}$$

Eq. (10.2.5) follows immediately by noting that $S_1^X\geq 0$. In Ref. [590], it was shown that for any three-qubit pure states, it holds that

$$\sqrt{S_1^{X}}+\sqrt{S_1^{Y}}-\sqrt{S_1^{Z}}\leq 1, \tag{10.2.11}$$

where $X,Y,Z=A,B,C$ and $S_1^X=\sum_{i=1}^3\langle\sigma_i\rangle^2_{\varrho_X}$ for $X=A,B,C$ and the single-qubit reduced state ϱ_X. Substituting Eq. (10.2.10) into all three permutations of Eq. (10.2.11) and multiplying with $\sqrt{3}$, we immediately arrive at the inequality in Result 43

$$\sqrt{3+S_2^{AB}-S_3^{ABC}}+\sqrt{3+S_2^{BC}-S_3^{ABC}}-\sqrt{3+S_2^{CA}-S_3^{ABC}}\leq\sqrt{3} \tag{10.2.12}$$

and permutations thereof. Noting that this holds for all values $1\leq S_3^{ABC}\leq 4$ and that the condition is the least restrictive for $S_3^{ABC}=3$, we complete the proof of Result 42. □

We have several remarks on Result 43. First, similarly to the Result 42, these non-linear inequalities are tight, they exactly describe the set of all points corresponding to pure states. The boundary can be attained by states of the form

$$|\Xi(x,y)\rangle=\sqrt{\frac{x-y}{2}}|001\rangle+\sqrt{\frac{1+y}{2}}|010\rangle+\sqrt{\frac{1-x}{2}}|100\rangle, \tag{10.2.13}$$

where $-1 < y \leq x < 1$.

Second, any pure separable state with respect to the bipartition $A|BC$ satisfies $S_3^{ABC} \leq 3$, while any pure fully separable state also satisfies $S_3^{ABC} \leq 1$. Thus, we are able to identify GME for permutationally invariant states, as long as $S_3^{ABC} > 3$ and bipartite entanglement as long as $S_3^{ABC} > 1$. More specifically, by including the S_3^{ABC} coordinate we are able to distinguish GHZ and W states as being GME states.

10.3 Mixed states

10.3.1 Global constraints

In this section, we extend our previous analysis to mixed states and characterize the set of two-body correlations $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ attainable by various classes of mixed three-qubit states ϱ_{ABC}. Let us begin by noting the convex property of the two-body sector lengths:

$$S_2(\varrho_{ABC}) \leq \sum_i p_i S_2(\varrho_i), \tag{10.3.1}$$

for $\varrho_{ABC} = \sum_i p_i \varrho_i$ (this holds for all k-body sector lengths). Thus, any three-qubit state obeys that $S_2(\varrho_{ABC}) \leq 3$. This means that no three-qubit mixed state can go outside the boundaries of pure states in the state space.

For any three-qubit state the inequality $S_2 = S_2^{AB} + S_2^{BC} + S_2^{CA} \leq 3$ holds. We further conjecture that the same three non-linear inequalities as for pure states given in Result 42 hold:

Conjecture. *For any three-qubit state, it holds that*

$$\sqrt{S_2^{AB}} + \sqrt{S_2^{AC}} - \sqrt{S_2^{BC}} \leq \sqrt{3}, \tag{10.3.2a}$$

$$\sqrt{S_2^{AB}} - \sqrt{S_2^{AC}} + \sqrt{S_2^{BC}} \leq \sqrt{3}, \tag{10.3.2b}$$

$$-\sqrt{S_2^{AB}} + \sqrt{S_2^{AC}} + \sqrt{S_2^{BC}} \leq \sqrt{3}. \tag{10.3.2c}$$

Remark 57. The corresponding set $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ is displayed in Fig. 10.2. There is some evidence indicating the validity of this conjecture. One expects states that form the boundary of the state space in $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ to be of low rank, whereas states increase in rank when coming closer to the origin $(0, 0, 0)$, see Sec. 10.4.

In case the inequalities (10.3.2a, 10.3.2c, 10.3.2c) hold, they would be tight, as they are saturated by the states

$$\kappa_1(p,q) = q\,|\xi_1(p)\rangle\langle\xi_1(p)| + \bar{q}\,|\xi_1(\bar{p})\rangle\langle\xi_1(\bar{p})|\,, \tag{10.3.3a}$$

$$\kappa_2(p,q) = q\,|\xi_2(p)\rangle\langle\xi_2(p)| + \bar{q}\,|\xi_2(\bar{p})\rangle\langle\xi_2(\bar{p})|\,, \tag{10.3.3b}$$

$$\kappa_3(p,q) = q\,|\xi_3(p)\rangle\langle\xi_3(p)| + \bar{q}\,|\xi_3(\bar{p})\rangle\langle\xi_3(\bar{p})|\,, \tag{10.3.3c}$$

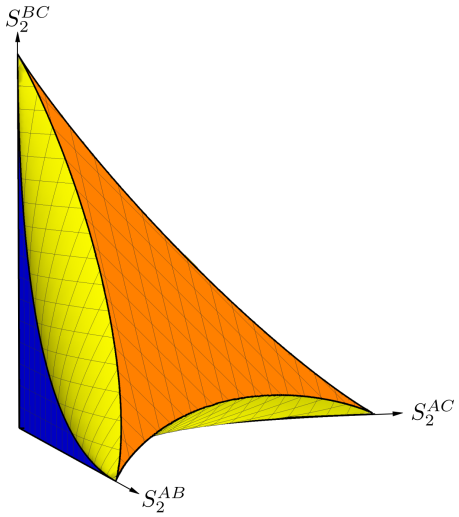

Figure 10.2: The state space in $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ of three qubits under two-body sector lengths. This is a conjecture in Eq. (10.3.2). This figure is taken from Ref. [11].

where $\bar{q} = 1 - q$, $\bar{p} = 1 - p$ and $|\xi_1(p)\rangle, |\xi_2(p)\rangle, |\xi_3(p)\rangle$ are respectively defined in Eqs. (10.2.2a, 10.2.2b, 10.2.2c). That is, together with $S_2 \leq 3$ they would completely characterize the set of points $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ attainable by three-qubit states.

10.3.2 Full separability

A mixed state is called fully separable if it can be written in the form

$$\varrho_{\text{fs}} = \sum_k p_k \varrho_k^A \otimes \varrho_k^B \otimes \varrho_k^C, \tag{10.3.4}$$

with $p_k \in [0,1]$ and $\sum_k p_k = 1$. For example, the maximally mixed state $\mathbb{1}_8/8$ sits at the origin $(0,0,0)$. Intuitively, a fully separable state should have small two-body correlations, and thus the set $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ attainable by fully separable states may be expected to sit close to the origin. Indeed, we present the following inequalities:

Result 44. *Any fully separable three-qubit state obeys*

$$S_2^{AB} + S_2^{BC} - S_2^{CA} \leq 1, \tag{10.3.5a}$$
$$S_2^{AB} - S_2^{BC} + S_2^{CA} \leq 1, \tag{10.3.5b}$$
$$-S_2^{AB} + S_2^{BC} + S_2^{CA} \leq 1. \tag{10.3.5c}$$

These criteria are optimal, the fully separable states fill the whole set defined by those inequalities.

Remark 58. The proof is given below. The set defined formed by the fully separable states is displayed in Fig. 10.3, the inequalities in Eqs. (10.3.5a)-(10.3.5c) are respectively represented by the Blue, Green, and Pink facets.

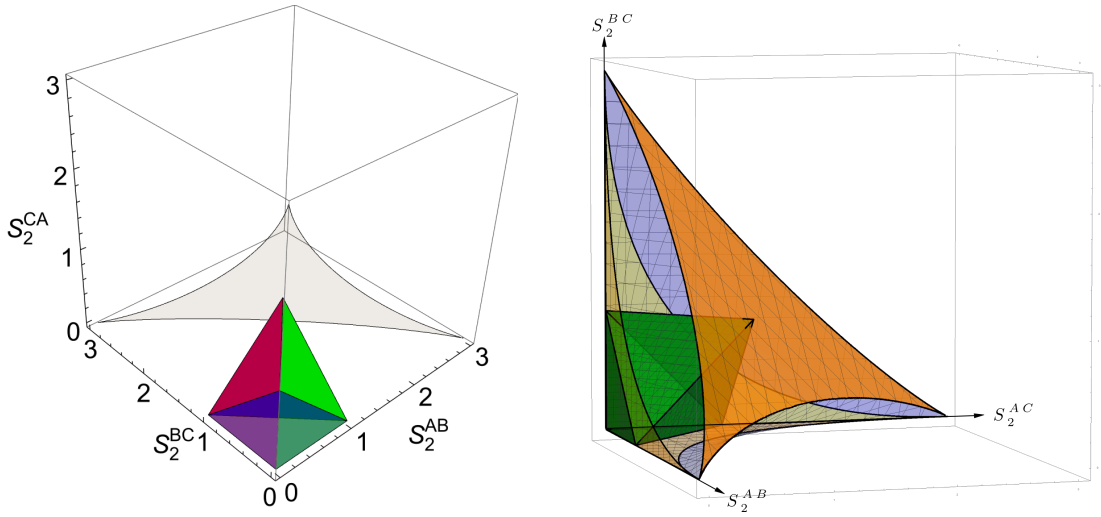

Figure 10.3: The space of the fully separable three-qubit states in the coordinates given by Result 44 is presented in this Chapter, along with the pure state in the background. The transparent yellow region specifies the pure state space while the blue is the fully separable region. The green, pink, and blue surface areas correspond to Eqs. (10.3.12a, 10.3.12b, 10.3.12c). This figure is taken from Ref. [11].

Proof. Let us recall the fully separable state:

$$\varrho_{\text{fs}} = \sum_k p_k \varrho_k^A \otimes \varrho_k^B \otimes \varrho_k^C, \tag{10.3.6}$$

with $p_k \in [0,1]$ and $\sum_k p_k = 1$. Here we note that any separable state has positive eigenvalues under partial transposition [194]: $\varrho_{XY} \in \text{SEP} \to \varrho_{XY}^{\top_X} \geq 0$, where $(\cdot)^{\top_X}$ denotes the partial transposition on subsystem X.

In the case where $X = A$ and $Y = BC$, we consider the following ϱ_1 for the fully separable state

$$\varrho_1 \equiv \sigma_y^{(A)} \varrho_{\text{fs}}^{\top_A} \sigma_y^{(A)} \geq 0, \tag{10.3.7}$$

where $\sigma_y^{(A)}$ denotes a Pauli-Y matrix, which is unitary, acting on the subsystem A. This corresponds to the local spin flip in Eq. (1.1.56) in Sec 1.1. Now, ϱ_1 is a quantum state since it is a positive density matrix. Similarly, in the case where $X = BC$ and $Y = A$, we have that

$$\varrho_2 \equiv \sigma_y^{(B)} \sigma_y^{(C)} \varrho_{\text{fs}}^{\top_{BC}} \sigma_y^{(B)} \sigma_y^{(C)} \geq 0. \tag{10.3.8}$$

Using the inequality $\text{tr}(AB) \geq 0$ for positive matrices A, B, we can arrive at

$$\text{tr}(\varrho_{\text{fs}} \varrho_1) \geq 0 \implies 1 - S_1^A + S_1^B + S_1^C - S_2^{AB} - S_2^{CA} + S_2^{BC} - S_3^{ABC} \geq 0, \tag{10.3.9}$$

$$\text{tr}(\varrho_{\text{fs}} \varrho_2) \geq 0 \implies 1 + S_1^A - S_1^B - S_1^C - S_2^{AB} - S_2^{CA} + S_2^{BC} + S_3^{ABC} \geq 0. \tag{10.3.10}$$

Adding the above two equations, we obtain

$$S_2^{AB} - S_2^{BC} + S_2^{CA} \leq 1, \tag{10.3.11}$$

which leads us to Eq. (10.3.5b). Similarly, choosing the appropriate bipartitions can derive Eqs. (10.3.5a),(10.3.5c).

Concerning the optimality, we find that these inequalities are saturated by the states

$$\varrho_{++-}(p,\theta) = p\,|000\rangle\langle 000| + (1-p)\,|01\theta\rangle\langle 01\theta|\,, \tag{10.3.12a}$$
$$\varrho_{+-+}(p,\theta) = p\,|000\rangle\langle 000| + (1-p)\,|0\theta1\rangle\langle 0\theta1|\,, \tag{10.3.12b}$$
$$\varrho_{-++}(p,\theta) = p\,|000\rangle\langle 000| + (1-p)\,|\theta01\rangle\langle \theta01|\,, \tag{10.3.12c}$$

where $|\theta\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle$. Thus we can complete the proof of Result 44. □

We can indeed find stronger criteria from Eqs. (10.3.9, 10.3.10). For that, we note that

$$\min(a,b) = \frac{a+b}{2} - \frac{|a-b|}{2}. \tag{10.3.13}$$

Then, taking the minimization over both sides leads to the stronger criteria for full separability:

$$S_2^{AB} + S_2^{CA} - S_2^{BC} + |S_3^{ABC} + S_1^{A} - S_1^{B} - S_1^{C}| \leq 1, \tag{10.3.14a}$$
$$S_2^{AB} - S_2^{CA} + S_2^{BC} + |S_3^{ABC} - S_1^{A} + S_1^{B} - S_1^{C}| \leq 1, \tag{10.3.14b}$$
$$-S_2^{AB} + S_2^{CA} + S_2^{BC} + |S_3^{ABC} - S_1^{A} - S_1^{B} + S_1^{C}| \leq 1. \tag{10.3.14c}$$

10.3.3 Biseparability

A state is called biseparable for the bipartition $A|BC$ if it can be written as

$$\varrho_{A|BC} = \sum_k q_k \varrho_k^A \otimes \varrho_k^{BC}, \tag{10.3.15}$$

with $q_k \in [0,1]$ and $\sum_k q_k = 1$. Let us propose the following criteria:

Result 45. *Any three-qubit state which is separable for a bipartition $X|YZ$ obeys*

$$S_2^{XY} + S_2^{ZX} - S_2^{YZ} \leq 1, \tag{10.3.16a}$$
$$S_2^{XY}, S_2^{ZX} \leq 1, \tag{10.3.16b}$$
$$3S_2^{XY} - S_2^{ZX} + S_2^{YZ} \leq 3, \tag{10.3.16c}$$
$$-S_2^{XY} + 3S_2^{ZX} + S_2^{YZ} \leq 3. \tag{10.3.16d}$$

Remark 59. The proof is given below and the sets defined by these inequalities are displayed in Fig. 10.4.

Proof. Without loss of generality, it is sufficient to prove the one of the bipartitions. In this proof, we take the case where a state is separable with respect to

partition $A|BC$, which obeys

$$S_2^{AB} + S_2^{CA} - S_2^{BC} \leq 1, \tag{10.3.17a}$$
$$S_2^{AB}, S_2^{CA} \leq 1, \tag{10.3.17b}$$
$$3S_2^{AB} - S_2^{CA} + S_2^{BC} \leq 3, \tag{10.3.17c}$$
$$-S_2^{AB} + 3S_2^{CA} + S_2^{BC} \leq 3. \tag{10.3.17d}$$

Note that the inequality (10.3.17a) was already proven in Result 44. Also the inequality (10.3.17b) is a trivial extension of the pure state criterion, due to the convexity of our coordinates. In the following, we will then show the inequalities (10.3.17c, 10.3.17d).

We begin by observing the case for pure states. The biseparability condition for $A|BC$ then leads to the condition $S_2^{AB} = S_2^{CA}$, which we already discussed. This implies that the left-hand sides in both Eqs. (10.3.17c, 10.3.17d) become,

$$3S_2^{AB} - S_2^{CA} + S_2^{BC} = 2S_2^{AB} + S_2^{BC} = S_2^{AB} + S_2^{CA} + S_2^{BC} = 3. \tag{10.3.18}$$

That is, the inequalities (10.3.17c, 10.3.17d) are clearly saturated by all rank-one three-qubit states that are biseparable for $A|BC$. Based on this fact, we will proceed with our proof.

Let us note that any biseparable state for $A|BC$ can be written as

$$\varrho_{A|BC} = \sum_i p_i \left|\psi^i_{A|BC}\right\rangle\!\left\langle\psi^i_{A|BC}\right|. \tag{10.3.19}$$

The squared coefficient of a two-body Bloch component $\sigma_a^{(m)} \otimes \sigma_b^{(n)}$ for the qubit indices $m, n = A, B, C$ and Pauli indices $a, b = 1, 2, 3$ are given by

$$\langle \sigma_a^{(m)} \otimes \sigma_b^{(n)} \rangle^2_{\varrho_{A|BC}} = \sum_i p_i^2 \left(\alpha^{m,n}_{i:a,b}\right)^2 + 2\sum_{i<j} p_i p_j \alpha^{m,n}_{i:a,b} \alpha^{m,n}_{j:a,b}, \tag{10.3.20}$$

where $\alpha^{m,n}_{i:a,b} = \langle \psi^i_{A|BC} | \sigma_a^{(m)} \otimes \sigma_b^{(n)} | \psi^i_{A|BC} \rangle$. Note this also holds for any general state. With this expression and the condition in Eq. (10.3.18), we can rewrite the left-hand side in Eq. (10.3.17c) as

$$3S_2^{AB} - S_2^{CA} + S_2^{BC} = 3\sum_i p_i^2 + \sum_{i<j} p_i p_j g_{ij}, \tag{10.3.21}$$

where the function g_{ij} contains the cross-terms given by

$$g_{ij} = \sum_{a,b=1}^{3} 3\alpha^{A,B}_{i:a,b}\alpha^{A,B}_{j:a,b} - \alpha^{C,A}_{i:a,b}\alpha^{C,A}_{j:a,b} + \alpha^{B,C}_{i:a,b}\alpha^{B,C}_{j:a,b}. \tag{10.3.22}$$

Using numerical optimization (explained below), one can observe that for any two pure states that are separable in the $A|BC$ bipartition, it holds that

$$g_{ij} \leq 3, \qquad \forall \left|\psi^i_{A|BC}\right\rangle, \left|\psi^j_{A|BC}\right\rangle \in \mathrm{SEP}\left(A|BC\right), \tag{10.3.23}$$

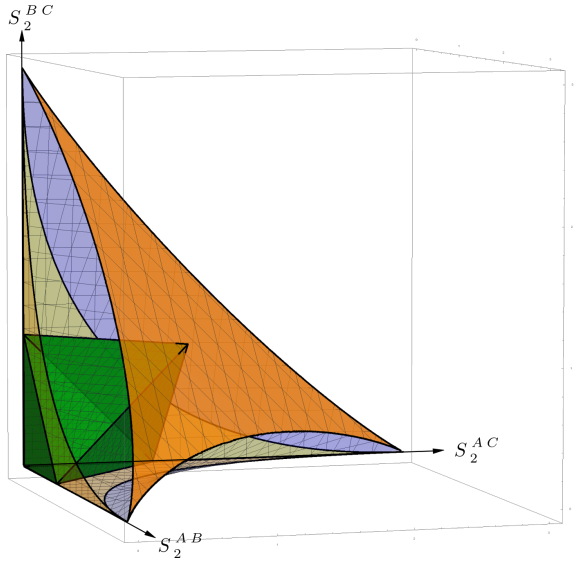

Figure 10.4: The state space of states that are biseparable along some fixed bipartition, according to Result 45 presented in this Chapter. The Green, Orange, and Red regions correspond to states biseparable in the $AC|B$,$AB|C$, and $BC|A$ bipartitions. This figure is taken from Ref. [11].

which results in that Eq. (10.3.21) can be bounded by 3. To be more precise, we consider the most general pure quantum state that is separable in the $A|BC$ bipartition:

$$|\psi(\boldsymbol{\theta},\boldsymbol{\phi})\rangle = \big[\cos(\theta_1)|0\rangle + e^{i\phi_1}\sin(\theta_1)|1\rangle\big] \otimes \big[\cos(\theta_2)|00\rangle + e^{i\phi_2}\sin(\theta_2)\cos(\theta_3)|01\rangle + e^{i\phi_3}\sin(\theta_2)\sin(\theta_3)\cos(\theta_4)|10\rangle + e^{i\phi_4}\sin(\theta_2)\sin(\theta_3)\sin(\theta_4)|11\rangle\big]. \tag{10.3.24}$$

Thus, by plugging Eq (10.3.24) into Eq. (10.3.22), we convert the problem of maximizing g into an unconstrained maximization problem over parameters. Implementing the optimization over these parameters, we thus can complete the proof of Result 45. □

The biseparability inequalities can also be written in terms of the purity of total and reduced density matrices of the three-qubit state. More precisely, the purity of two-qubit and single-qubit reduced density matrix takes the following forms:

$$\mathrm{tr}(\varrho_X^2) = \frac{1}{2}\left[1 + S_1^X\right], \tag{10.3.25}$$

$$\mathrm{tr}(\varrho_{XY}^2) = \frac{1}{4}\left[1 + S_1^X + S_1^Y + S_2^{XY}\right]. \tag{10.3.26}$$

Using the Eqs.(10.3.25) and (10.3.26), and with a bit of algebra, one can re-write the Eqs. (10.3.17c) and (10.3.17d) as

$$3\mathrm{tr}(\varrho_{AB}^2) + \mathrm{tr}(\varrho_{BC}^2) \leq \mathrm{tr}(\varrho_{AC}^2) + \mathrm{tr}(\varrho_A^2) + 2\mathrm{tr}(\varrho_B^2), \tag{10.3.27a}$$

$$3\mathrm{tr}(\varrho_{AC}^2) + \mathrm{tr}(\varrho_{BC}^2) \leq \mathrm{tr}(\varrho_{AB}^2) + \mathrm{tr}(\varrho_A^2) + 2\mathrm{tr}(\varrho_C^2). \tag{10.3.27b}$$

A state violating inequality (10.3.16c) cannot be written in the form (10.3.15) and therefore is entangled across the bipartition $A|BC$. Similarly, we can detect entanglement for the partitions $B|CA$ and $C|AB$. Combining this, any state mapping outside of the union of the three sets defined by Eqs. (10.3.16c)-(10.3.16d) can not be separable with respect to a given partition. However, this does not imply that the state is genuinely multipartite entangled (for details, see Sec. 1.2). There is the possibility that our inequalities are violated by a mixture of biseparable states. Such states have the form

$$\varrho_{\text{bisep}} = p_A \varrho_{A|BC} + p_B \varrho_{B|CA} + p_C \varrho_{C|AB}, \tag{10.3.28}$$

where p_A, p_B, p_C are probability distributions.

Let us explicitly provide a biseparable state that does not lie in the union of the three different partition biseparability. The general biseparable states that are biseparable along different bipartitions, do not satisfy the bounds given in Result 45. A non-trivial example is given by

$$\varrho_{12} = 0.65\,|\psi_1\rangle\langle\psi_1| + 0.35\,|\psi_2\rangle\langle\psi_2|\,, \tag{10.3.29}$$

$$|\psi_1\rangle = \sqrt{0.97}\,|000\rangle + \sqrt{0.03}\,|011\rangle\,, \tag{10.3.30}$$

$$|\psi_2\rangle = -0.97\,|000\rangle - 0.127\,|100\rangle + 0.2\,|110\rangle\,. \tag{10.3.31}$$

The above state is a mixture of states biseparable in the $A|BC$ and $C|AB$ bipartition. However, this can violate our criteria:

$$\min_{X\neq Y\neq Z\in\{A,B,C\}} 2|S_2^{XY} - S_2^{YZ}| + S_2^{XY} + S_2^{YZ} + S_2^{XZ} = 3.02684. \tag{10.3.32}$$

Remark 60. For pure biseparable states we recover the previous results, thus states of the form of Eq. (10.3.28) saturate the inequalities (10.3.16c)-(10.3.16d). However, it is not clear if the inequalities are also tight for mixed states. If Conjecture 10.3.2 holds, parts of the biseparable sets would lie outside of the region attainable by quantum states. Therefore the global tightness of the inequalities (10.3.16c)-(10.3.16d) stands in conflict with Conjecture 10.3.2.

10.4 Rank bounds

In this section, we look at restrictions of the two-body correlations $(S_2^{AB}, S_2^{BC}, S_2^{CA})$ depending on the matrix rank of a quantum state, that is, the number of eigenvalues. Here we formulate the following:

Result 46. *Any rank-two three-qubit state obeys $S_2 \geq 1$ and any rank-three three-qubit state obeys $S_2 \geq 1/3$. There is no non-trivial necessary condition for rank-k for $k \geq 4$ three-qubit states in terms of the coordinates $(S_2^{AB}, S_2^{BC}, S_2^{CA})$.*

Remark 61. The proof is given below. For both rank two and three there exists states that saturate the inequality. For rank wto, one family of states that saturate the bound are the ones in Eq. (10.3.12) with $p = \frac{1}{2}$. However, we do not expect these bounds to be optimal, i.e. the tightest bounds in terms of $(S_2^{AB}, S_2^{BC}, S_2^{CA})$, and believe that there exists better non-linear bounds.

Proof. Consider a rank-l density matrix. Suppose its purity is lower bounded by l. Then, using $\mathrm{tr}\left(\varrho^2\right) = \frac{1}{8}\left(1 + S_1 + S_2 + S_3\right)$,

$$S_1 + S_2 + S_3 \geq 8l - 1. \tag{10.4.1}$$

Furthermore, any three-qubit state obeys the following inequality in Ref [352]:

$$1 - S_1 + S_2 - S_3 \geq 0. \tag{10.4.2}$$

Using Eqs. (10.4.1 and 10.4.2), we arrive at

$$S_2 \geq 4l - 1. \tag{10.4.3}$$

The proof is completed by noting that for rank-two states, $l = \frac{1}{2}$ and for rank-three states, $l = \frac{1}{3}$. □

Concerning the nonexistence of non-trivial necessary conditions for states of rank-four and higher, we note that the trivial one is $S_2 \geq 0$. That is, rank-four states have just a high enough rank to cover the whole set of two-body correlations. For instance, the separable state

$$\eta = \frac{1}{4}(|000\rangle\langle 000| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110|) \tag{10.4.4}$$

has rank four but $S_2 = 0$. That is, this state is indistinguishable from the maximally mixed state in our coordinates. The same can even hold for entangled states. The three-qubit state ϱ_θ discussed in Eq. (F1) in Ref. [256], has no two-body correlation, that is $S_2 = 0$. This state is separable for all bipartitions but not fully separable, which contains a very weak form of entanglement in three qubits, called bound entanglement [166].

10.5 Discussions

This Chapter developed methods to characterize three-qubit quantum states with two-body marginal correlations that are invariant under local unitaries. For pure states, we have found tight nonlinear bounds and given their analytical proofs. For mixed states, we have proposed criteria for different forms of multipartite entanglement, which are expressed as nontrivial linear combinations.

There are several directions for further research. First, it would be interesting to extend this approach to many particles or higher dimensions. To advance our understanding of the geometry of quantum systems, it is interesting to develop a systematic approach to finding the set of admissible states. Second, different types of marginal local unitary invariants may be employed as other coordinates. This may lead to new criteria to detect multipartite entanglement from marginals information. Finally, since our entanglement criteria can detect entanglement in which the two-body correlations are not equally distributed, our results may encourage the characterization of multipartite entanglement without symmetric properties.

Chapter 11

Quantum speed limit for perturbed open systems

This Chapter deals with the analysis of open quantum dynamics in terms of perturbation. This Chapter presents quantum speed limits describing the divergence of a perturbed open system from its unperturbed trajectory in state space. This Chapter is based on Ref. [9].

11.1 Introduction

The concept of time-energy uncertainty in quantum mechanics was formally established in 1945 by Mandelstam and Tamm [591]. They demonstrated the limitation on the time required for a quantum state to evolve to an orthogonal state based on its energy uncertainty. Subsequently, this idea has been extended and generalized, notably by Margolus and Levitin [97], who introduced a bound involving mean energy, leading to what is now known as the quantum speed limit. Over time, numerous extensions to mixed states and driven and open quantum systems have been derived [592–596], along with an understanding of the connection to the geometry of quantum state spaces [91, 597, 598].

Quantum speed limits have found applications in various fields, including information processing rates [599, 600] and maximum physically allowable rates of communication [601]. Additionally, they have been utilized in quantum thermodynamics to bound entropy production rates [602], analyze heat engine efficiency and power [603, 604], and study battery charging rates [465, 466]. Furthermore, speed limits are closely related to metrology, where the precision of parameter estimation encoded in a quantum state depends on the rate of state change with respect to the parameter [605, 606].

The quantum Fisher information (QFI) [91, 92] plays a crucial role in metrology, as it not only represents a (squared) speed in state space but also quantifies various important properties of quantum states. For example, a sufficiently large QFI indicates many-body entanglement [176, 320, 607, 608]. Additionally, the QFI can be used as a measure of coherence in a given basis [609, 610], macro-

scopic quantumness of a system [611], and Glauber-Sudarshan nonclassicality in optics [612, 613]. Moreover, the QFI serves as a witness of general quantum resources [614]. Due to these applications, it is often desirable to experimentally measure lower bounds on the QFI. One common approach is to adopt speed limits to estimate the QFI from the distance between an initial state and a state evolved for a short time [615, 616].

In this Chapter, we introduce a novel type of speed limit that characterizes the response of a Markovian open quantum system to a perturbation in its dynamics. The derived inequality upper bounds the distance between the perturbed and unperturbed trajectories in state space in terms of the QFI of the system with respect to the perturbation. Importantly, this result holds under minimal assumptions and without detailed knowledge of the dynamics. For a system weakly coupled to its environment, we demonstrate that the speed limit can be expressed in terms of the QFI with respect to a perturbing Hamiltonian, up to an error bounded in terms of the relevant physical timescales. We then show how this speed limit can be used to experimentally determine a lower bound on the QFI. Finally, we apply this formalism to the thermodynamics of systems perturbed out of equilibrium, revealing that quantum fluctuations in the work performed during a sudden quench are necessary for rapid departure from the initial state.

11.2 Quantum speed limits

We begin by recalling the original Mandelstam-Tamm quantum speed limit [591]:

$$\tau \geq \frac{\pi}{2\sqrt{\mathrm{Var}(\psi, H)}}, \qquad \mathrm{Var}(\psi, H) = \langle \psi | H^2 | \psi \rangle - \langle \psi | H | \psi \rangle^2, \tag{11.2.1}$$

where $\mathrm{Var}(\psi, H)$ is the energy variance of a pure state $|\psi\rangle$ at time τ, and we take $\hbar = 1$. This bound implies that a large energy variance is necessary for a quantum state to evolve quickly to an orthogonal state under the influence of the Hamiltonian H.

The quantum speed limit has been extended to mixed states by considering the nonzero overlap between the initial and final states. In Ref. [597], Uhlmann introduced a speed limit involving the fidelity between the initial state ϱ_0 and the final state $\varrho_t = e^{-itH}\varrho_0 e^{itH}$ as follows:

$$F(\varrho_0, \varrho_t) = \mathrm{tr}\sqrt{\sqrt{\varrho_0}\varrho_t\sqrt{\varrho_0}}, \tag{11.2.2}$$

where ϱ_0 and ϱ_t represent the initial and final states, respectively. Instead of the energy variance, we employ the Quantum Fisher Information (QFI) to characterize the system's sensitivity to changes in time.

The QFI measures the sensitivity of a continuously parameterized family of states to small changes in a parameter [92]. In this chapter, we focus on the sensitivity to time evolution, so the QFI becomes a function of the state ϱ_t

and its instantaneous time derivative $\frac{d\varrho_t}{dt}$. We consider evolutions generated by Gorini-Kossakowski-Sudarshan-Lindblad (GKSL) superoperators [40, 41]:

$$\frac{d\varrho_t}{dt} = \mathcal{L}_t(\varrho_t), \tag{11.2.3}$$

where the QFI $\mathcal{F}(\varrho_t, \mathcal{L}_t)$ can be defined as a function of ϱ_t and $\mathcal{L}_t$. One definition of the QFI is expressed in terms of the spectral decomposition $\varrho_t = \sum_i \lambda_i(t) \, |\psi_i(t)\rangle\langle\psi_i(t)|$:

$$\mathcal{F}(\varrho_t, \mathcal{L}_t) = 2 \sum_{i,j:\, \lambda_i(t)+\lambda_j(t)>0} \frac{|\, \langle\psi_i(t)|\mathcal{L}_t(\varrho_t)|\psi_j(t)\rangle \,|^2}{\lambda_i(t) + \lambda_j(t)}. \tag{11.2.4}$$

With these concepts in place, the Uhlmann speed limit can be written as

$$\theta_B(\varrho_0, \varrho_t) \leq \frac{1}{2} \int_0^t ds \, \sqrt{\mathcal{F}(\varrho_s, \mathcal{H}_s)}, \quad \forall\, t \geq 0, \tag{11.2.5}$$

where $\mathcal{H}_t$ is the generator of time evolution under the time-dependent Hamiltonian H_t:

$$\mathcal{H}_t(\cdot) = -i[H_t, \cdot]. \tag{11.2.6}$$

This bound is derived from the infinitesimal expansion of the Bures angle as a metric on state space:

$$\theta_B(\varrho_t, \varrho_{t+dt})^2 = \frac{1}{4}\mathcal{F}(\varrho_t, \mathcal{L}_t)dt^2, \tag{11.2.7}$$

where the finite Bures angle represents the length of a geodesic between two points [91].

To understand how Eq. (11.2.1) can be derived from Eq. (11.2.5), we first note that the QFI under a Hamiltonian is bounded by four times the energy variance:

$$\mathcal{F}(\varrho, \mathcal{H}) \leq 4\mathrm{Var}(\varrho, H), \tag{11.2.8}$$

with equality holding when ϱ is a pure state [170]. Furthermore, in the case of a time-independent Hamiltonian H, the QFI remains constant over time. From these observations, the Mandelstam-Tamm inequality follows, considering that $\theta_B(\varrho_0, \varrho_t) = \pi/2$ for orthogonal initial and final states. Hence, the square root of the QFI can be interpreted as a "statistical speed" [92, 605].

In the case of a Hamiltonian, the QFI has an alternative interpretation as a quantum contribution to the variance (notably, $\mathcal{F}(\varrho, \mathcal{H}) = 0$ if and only if $[\varrho, H] = 0$) [170]. Moreover, it can be rigorously justified as a measure of coherence in the eigenbasis of H [609, 617].

11.3 Perturbation speed limit

In this section, we present the main result, which applies to a system undergoing arbitrary Markovian dynamics with a perturbation. We adopt the common definition that equates Markovianity with divisibility. According to this definition, the mapping $\mathcal{N}_{t_1,t_0}$ of states between any times t_0 and $t_1 \geq t_0$ is completely positive and trace-preserving, and it satisfies the composition property:

$$\mathcal{N}_{t_2,t_0} = \mathcal{N}_{t_2,t_1}\mathcal{N}_{t_1,t_0}, \quad \forall\, t_0 \leq t_1 \leq t_2. \tag{11.3.1}$$

This condition is equivalent to the dynamics being governed by the GKSL generator $\mathcal{L}_t$ [618].

Next, we present one of the main results in this chapter:

Result 47. *Consider a system starting in state ϱ_0 that can evolve along one of two trajectories:*

(i) Free evolution, given by

$$\frac{d\varrho_t}{dt} = \mathcal{L}_t(\varrho_t), \tag{11.3.2}$$

where $\mathcal{L}_t$ is a GKSL generator.

(ii) Perturbed evolution, given by

$$\frac{d\sigma_t}{dt} = \mathcal{L}'_t(\sigma_t) = \mathcal{L}_t(\sigma_t) + \mathcal{P}_t(\sigma_t), \tag{11.3.3}$$

which satisfies the same initial condition $\sigma_0 = \varrho_0$.

The Bures angle measuring the divergence between the trajectories is bounded by

$$\theta_B(\varrho_t, \sigma_t) \leq \frac{1}{2}\int_0^t ds\, \sqrt{\mathcal{F}(\sigma_s, \mathcal{P}_s)}, \quad \forall\, t \geq 0. \tag{11.3.4}$$

Remark 62. The proof is given below. In the case of $\mathcal{L}_t = 0$, the system remains stationary, and the bound reduces to a previously known result [619]. For the closed-system case, we consider Hamiltonian dynamics:

$$\mathcal{L}_t = \mathcal{H}_t, \qquad \mathcal{P}_t(\cdot) = v\mathcal{V}_t(\cdot) = -iv[V_t, \cdot]. \tag{11.3.5}$$

Notably, in this case, our bound (11.3.4) is equivalent to Uhlmann's speed limit in Eq. (11.2.5), and it can be derived from the latter by moving to the interaction picture. Therefore, our bound (11.3.4) generalizes previous speed limits. The relevant statistical speed measures the sensitivity of the system to the perturbation.

Proof. We make use of three main facts about the Bures angle:

(A) It obeys the triangle inequality.

(B) It is contractive under quantum channels [19].

(C) Its infinitesimal expansion is related to the QFI, as stated above.

At time t, consider the states ϱ_t and σ_t, as well as their corresponding time-evolved states $\varrho_{t+\delta t}$ and $\sigma_{t+\delta t}$, a short time δt later. Additionally, we consider the evolution of σ_t under the *unperturbed* dynamics for time δt, resulting in the state $\sigma'_{t+\delta t}$. The situation is illustrated in Fig. 11.1.

For the lowest order, we have:

$$\varrho_{t+\delta t} = \varrho_t + \delta t \mathcal{L}_t(\varrho_t) + \mathcal{O}(\delta t^2), \tag{11.3.6}$$

$$\sigma_{t+\delta t} = \sigma_t + \delta t \mathcal{L}_t(\sigma_t) + \delta t \mathcal{P}_t(\sigma_t) + \mathcal{O}(\delta t^2), \tag{11.3.7}$$

$$\sigma'_{t+\delta t} = \sigma_t + \delta t \mathcal{L}_t(\sigma_t) + \mathcal{O}(\delta t^2). \tag{11.3.8}$$

The triangle inequality (A) first gives us:

$$\theta_B(\varrho_{t+\delta t}, \sigma_{t+\delta t}) \leq \theta_B(\varrho_{t+\delta t}, \sigma'_{t+\delta t}) + \theta_B(\sigma'_{t+\delta t}, \sigma_{t+\delta t}). \tag{11.3.9}$$

For the first term on the right-hand side of Eq. (11.3.9), we use the fact that $\varrho_{t+\delta t}$ and $\sigma'_{t+\delta t}$ have both been evolved for time δt under the same dynamics resulting in the same channel $\mathcal{N}_{t+\delta t,t}$. The contractivity of the Bures angle (B) then implies:

$$\theta_B(\varrho_{t+\delta t}, \sigma'_{t+\delta t}) = \theta_B(\mathcal{N}_{t+\delta t,t}(\varrho_t), \mathcal{N}_{t+\delta t,t}(\sigma_t)) \leq \theta_B(\varrho_t, \sigma_t). \tag{11.3.10}$$

For the second term in Eq. (11.3.9), we use the infinitesimal form of the Bures angle (C) and the fact that $\sigma_{t+\delta t} - \sigma'_{t+\delta t} = \delta t \mathcal{P}_t(\sigma_t) + \mathcal{O}(\delta t^2)$, to write:

$$\theta_B(\sigma'_{t+\delta t}, \sigma_{t+\delta t}) = \frac{\delta t}{2} \sqrt{\mathcal{F}(\sigma_{t+\delta t}, \mathcal{P}_t)} + \mathcal{O}(\delta t^2). \tag{11.3.11}$$

Putting these into Eq. (11.3.9), we have:

$$\theta_B(\varrho_{t+\delta t}, \sigma_{t+\delta t}) \leq \theta_B(\varrho_t, \sigma_t) + \frac{\delta t}{2} \sqrt{\mathcal{F}(\sigma_{t+\delta t}, \mathcal{P}_t)} + \mathcal{O}(\delta t^2). \tag{11.3.12}$$

Subtracting the first term on the right and dividing by δt gives:

$$\frac{\theta_B(\varrho_{t+\delta t}, \sigma_{t+\delta t}) - \theta_B(\varrho_t, \sigma_t)}{\delta t} \leq \frac{1}{2} \sqrt{\mathcal{F}(\sigma_{t+\delta t}, \mathcal{P}_t)} + \mathcal{O}(\delta t). \tag{11.3.13}$$

Taking the limit as $\delta t \to 0$, we get:

$$\frac{d\theta_B(\varrho_t, \sigma_t)}{dt} \leq \frac{1}{2} \sqrt{\mathcal{F}(\sigma_t, \mathcal{P}_t)}. \tag{11.3.14}$$

The limit on the right-hand side makes use of the continuity of the QFI [620]. Integrating therefore gives the claimed result. □

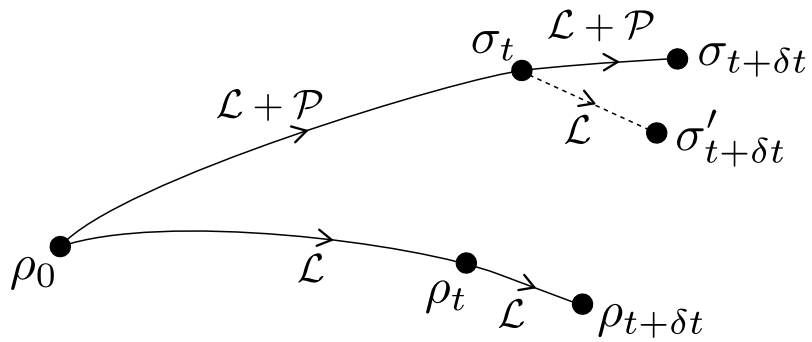

Figure 11.1: Illustration of the trajectories used in the proof of the main speed limit result (11.3.4). This figure is taken from Ref. [9].

The power of this bound comes from its minimal requirement of detailed information about the unperturbed dynamics $\mathcal{L}_t$ – only that they are Markovian. For the remainder of this chapter, we assume (as is typically true in quantum control) that the perturbation arises from a controlled change to the system's Hamiltonian. The free Hamiltonian is denoted as H_t, and the perturbed one is $H_t + vV_t$, where we include the constant v to later study variations in the size of the perturbation. While for many applications (see later sections), one is interested in the QFI with respect to V_t, the resulting perturbation to the master equation $\mathcal{P}_t$ could contain additional terms.

The identification of $\mathcal{P}_t$ with $v\mathcal{V}_t$ may be justified in the singular coupling limit [43] and in collision models of open system dynamics [621]. However, in the weak coupling regime, a change to the system's Hamiltonian will generally introduce an additional change to the generator of the dynamics. Therefore, we now investigate the error incurred by the approximation $\mathcal{P}_t \approx v\mathcal{V}_t$ and, correspondingly, the use of QFI with respect to V_t in the right-hand side of Eq. (11.3.4). From now on, we also consider time-independent dynamics for simplicity.

11.4 Weak coupling

To address the above issue, in this section, we consider a system weakly coupled to a Markovian environment and derive the error incurred by approximating the true perturbed trajectory with one in which the dissipative part of the dynamics is approximated as unchanged. Such situations are ubiquitous in experiments and encompass discrete [622] and continuous-variable [623] systems.

We assume the standard form of a weak coupling master equation with sec-

ular approximation [44]:

$$\frac{d\varrho_t}{dt} = \mathcal{L}(\varrho_t) = -i[H + H_{\mathrm{LS}}, \varrho_t] + \mathcal{D}(\varrho_t), \tag{11.4.1}$$

$$H_{\mathrm{LS}} = \lambda^2 \sum_{\omega,\alpha,\beta} S_{\alpha\beta}(\omega) A_\alpha^\dagger(\omega) A_\beta(\omega),$$

$$\mathcal{D}(\varrho) = \lambda^2 \sum_{\omega,\alpha,\beta} \gamma_{\alpha\beta}(\omega) \left[A_\beta(\omega) \varrho A_\alpha^\dagger(\omega) - \frac{\{A_\alpha^\dagger(\omega) A_\beta(\omega), \varrho\}}{2} \right], \tag{11.4.2}$$

where H_{LS} is the Lamb shift Hamiltonian and $\mathcal{D}$ is the dissipator. In this context, the interaction Hamiltonian with the bath $H_I = \lambda \sum_\alpha A_\alpha \otimes B_\alpha$ (where each appearing operator is Hermitian) has been decomposed into components $A_\alpha = \sum_\omega A_\alpha(\omega)$ with Bohr frequencies ω (i.e., gaps in the spectrum of the system Hamiltonian H), such that $[H, A_\alpha(\omega)] = \omega A_\alpha(\omega)$. The coefficients are real and imaginary parts of the Fourier-transformed (stationary) bath correlation functions:

$$\Gamma_{\alpha\beta}(\omega) = \int_0^\infty ds\, e^{i\omega s} \langle B_\alpha^\dagger(s) B_\beta(0) \rangle = \frac{1}{2}\gamma_{\alpha\beta}(\omega) + iS_{\alpha\beta}(\omega), \tag{11.4.3}$$

$$B_\alpha(s) = e^{isH_B} B_\alpha e^{-isH_B}, \tag{11.4.4}$$

where the bath Hamiltonian H_B is used, and angled brackets denote expectation value. We factor out the coupling strength λ such that A_α, $B_\alpha = \mathcal{O}(1)$ (meaning independent of λ).

We denote the size of the free system Hamiltonian H by h (measuring the size of the smallest energy gap and not to be confused with the Planck constant) and the size of the perturbing Hamiltonian by v (taking $V = \mathcal{O}(1)$). The important timescales are given by:

- The intrinsic system dynamics: $\tau_S \sim h^{-1}$,
- The perturbation: $\tau_V \sim v^{-1}$,
- The system relaxation: $\tau_R \sim \lambda^{-2}\gamma^{-1}$,
- The bath correlation decay: τ_B.

We make the following assumptions:

(i) Born-Markov approximation: $\tau_B \ll \tau_R$,

(ii) Rotating wave approximation [43, 44]: $\tau_S \ll \tau_R$,

(iii) Small perturbation relative to the bath: $\tau_B \ll \tau_V$,

(iv) Small perturbation relative to the system: $\tau_S \ll \tau_V$.

The need for assumption (iii) is not obvious but will become apparent later; it is essentially required so we can approximate the bath correlation function as flat in the frequency domain.

Now we find the following:

Result 48. *Consider a perturbation: $H \to H' = H + vV$. Then we can replace $H_{\mathrm{LS}} \to H'_{\mathrm{LS}} = H_{\mathrm{LS}} + vH^{(1)}_{\mathrm{LS}}$ and $\mathcal{D} \to \mathcal{D}' = \mathcal{D} + v\mathcal{D}^{(1)}$ to first order in v. This has the effect of changing the Bohr frequencies ω and the components $A_\alpha(\omega)$. The size of the perturbation terms $H^{(1)}_{\mathrm{LS}}$, $\mathcal{D}^{(1)}$ is given by:*

$$\epsilon = \max_{\psi} \|\mathcal{H}^{(1)}_{\mathrm{LS}}(\psi) + \mathcal{D}^{(1)}(\psi)\| = \mathcal{O}\left(\frac{\tau_S}{\tau_R}\right) + \mathcal{O}\left(\frac{\tau_B}{\tau_R}\right), \tag{11.4.5}$$

where $\|X\|$ denotes the largest singular value of X. It follows from assumptions (i)-(iv) that these terms are small compared to other terms in the master equation.

Proof. First, we expand the perturbed dissipator $\mathcal{D}'$ and Lamb shift H'_{LS} to first order in v using standard perturbation theory [18]. Note that we assume both are non-degenerate:

$$H = \sum_n E_n |n\rangle\langle n|, \qquad H' = \sum_n E'_n |n'\rangle\langle n'|. \tag{11.4.6}$$

To the lowest order, the perturbed energy eigenvalues and eigenvectors are

$$E'_n = E_n + vE^{(1)}_n + \mathcal{O}(v^2), \qquad |n'\rangle = |n\rangle + v|n^{(1)}\rangle + \mathcal{O}(v^2), \tag{11.4.7}$$

with

$$E^{(1)}_n = \langle n|V|n\rangle, \quad |n^{(1)}\rangle = \sum_{m\neq n} \frac{\langle m|V|n\rangle}{E_n - E_m}|m\rangle = \sum_{m\neq n} C_{nm}|m\rangle. \tag{11.4.8}$$

The perturbed Bohr frequencies are of the form $\omega' \approx \omega + \delta\omega$ with $\delta\omega = \mathcal{O}(v)$. It is possible for some ω to be degenerate, meaning that several transitions may have the same gap (for example, with the energies $\{-1, 0, 1\}$). We initially assume that the pattern of Bohr frequency degeneracies is unchanged under the perturbation, showing below how to handle a breaking of degeneracy. Recall that the RWA neglects terms in the master equation where $A_\alpha(\omega_1)$ and $A^\dagger_\beta(\omega_2)$ occur with $|\omega_1 - \omega_2| \gg \tau_R^{-1}$ [44]. On the other hand, if $|\omega_1 - \omega_2| \ll \tau_R^{-1}$, then we should treat these frequencies as effectively degenerate so that the RWA does not remove such off-diagonal terms, and we can include $A_\alpha(\omega_1)$ and $A_\alpha(\omega_2)$ in the same frequency component of A_α.

Supposing that the perturbed frequencies ω' have the same pattern of degeneracies as the ω, the perturbed jump operators are

$$\begin{aligned}
A'_\alpha(\omega') &= \sum_{m,n:\, E'_m - E'_n \approx \omega'} \Pi'_m A_\alpha \Pi'_n \\
&= \sum_{m,n:\, E_m - E_n \approx \omega} \Pi'_m A_\alpha \Pi'_n \\
&= \sum_{m,n:\, E_m - E_n \approx \omega} \Pi_m A_\alpha \Pi_n + v\left(Q_m A_\alpha \Pi_n + \Pi_m A_\alpha Q_n\right) + \mathcal{O}(v^2) \\
&= A_\alpha(\omega) + vA^{(1)}_\alpha(\omega) + \mathcal{O}(v^2),
\end{aligned} \tag{11.4.9}$$

where the $\approx$ sign is shorthand for equality up to an error much less than τ_R^{-1}, i.e., $|E_m - E_n - \omega| \ll \tau_R^{-1}$, and

$$\Pi_n' = \Pi_n + vQ_n + \mathcal{O}(v^2), \qquad Q_n = \sum_{m\neq n} C_{nm}\,|m\rangle\langle n| + C_{nm}^*\,|n\rangle\langle m|\,. \tag{11.4.10}$$

For the bath correlation coefficients, we write

$$\gamma_{\alpha\beta}(\omega') = \gamma_{\alpha\beta}(\omega) + \delta\omega\partial_\omega\gamma_{\alpha\beta}(\omega) + \mathcal{O}(v^2), \tag{11.4.11}$$

and similarly for $S_{\alpha\beta}(\omega')$. Inserting these into the expressions Eq. (11.4.1) to determine the perturbed Lamb shift and dissipator, we have the first-order terms:

$$\begin{aligned}
vH_{\mathrm{LS}}^{(1)} &= \lambda^2 \sum_\omega \sum_{\alpha,\beta} vS_{\alpha\beta}(\omega)\left[A_\alpha^{(1)\dagger}A_\beta(\omega) + A_\alpha^\dagger(\omega)A_\beta^{(1)}(\omega)\right] \\
&\quad + \delta\omega\partial_\omega S_{\alpha\beta}(\omega)A_\alpha^\dagger(\omega)A_\beta(\omega), \\
v\mathcal{D}^{(1)}(\varrho) &= \lambda^2 \sum_\omega \sum_{\alpha,\beta} v\gamma_{\alpha\beta}(\omega)\Bigg[A_\beta^{(1)}(\omega)\varrho A_\alpha^\dagger(\omega) + A_\beta(\omega)\varrho A_\alpha^{(1)\dagger}(\omega) \\
&\quad - \frac{1}{2}\left\{A_\alpha^{(1)\dagger}(\omega)A_\beta(\omega) + A_\alpha^\dagger(\omega)A_\beta^{(1)}(\omega), \varrho\right\}\Bigg] \\
&\quad + \delta\omega\partial_\omega\gamma_{\alpha\beta}(\omega)\left[A_\beta(\omega)\varrho A_\alpha^\dagger(\omega) - \frac{1}{2}\left\{A_\alpha^\dagger(\omega)A_\beta(\omega), \varrho\right\}\right].
\end{aligned} \tag{11.4.12}$$

To analyze the size of these terms, we first estimate $\lambda^2|\gamma_{\alpha\beta}(\omega)| \sim \tau_R^{-1}$ for all ω of interest. The first derivative can be found by observing that

$$\Gamma_{\alpha\beta}(\omega) = \int_0^\infty ds\; e^{i\omega s}\langle B_\alpha^\dagger(s)B_\beta(0)\rangle \tag{11.4.13}$$

implies

$$|\partial_\omega\Gamma_{\alpha\beta}(\omega)| = \left|\int_0^\infty ds\; se^{i\omega s}\langle B_\alpha^\dagger(s)B_\beta(0)\rangle\right| \sim \tau_B|\Gamma_{\alpha\beta}(\omega)|, \tag{11.4.14}$$

given that τ_B is the characteristic decay timescale of the correlation function. Therefore, we can estimate $\lambda^2|\partial_\omega\gamma_{\alpha\beta}(\omega)| \sim \tau_B\tau_R^{-1}$, and similarly for $S_{\alpha\beta}(\omega)$. From the perturbation theory expressions above and the fact that $A_\alpha(\omega) = \mathcal{O}(1)$, we further have $A_\alpha^{(1)}(\omega) \sim h^{-1} \sim \tau_S$. Hence, we see that

$$v\mathcal{H}_{\mathrm{LS}}^{(1)}(\varrho) + v\mathcal{D}^{(1)}(\varrho) = \mathcal{O}\left(\frac{\tau_S}{\tau_V\tau_R}\right) + \mathcal{O}\left(\frac{\tau_B}{\tau_V\tau_R}\right), \tag{11.4.15}$$

We want to ensure that this term is negligible compared with the other terms in the master equation. It is small compared with v as long as $\tau_S \ll \tau_R$ and $\tau_B \ll \tau_R$ – exactly the RWA and Born-Markov conditions, assumptions (ii) and (i) above. Furthermore, it is small compared with $\mathcal{D}$ and H_{LS} when $\tau_S \ll \tau_V$ and $\tau_B \ll \tau_V$, corresponding to the small perturbation assumptions (iv) and (iii). □

Remark 63. We comment on what happens when a degeneracy in the Bohr frequencies is broken by the perturbation. (The simplest example is a three-level system with energies $E_0 = 0$, $E_1 = \Delta$, and $E_2 = 2\Delta$, with a perturbation shifting the middle level E_1.) Suppose that $|\omega_1 - \omega_2| \ll \tau_R^{-1}$ but $|\omega_1' - \omega_2'| \gg \tau_R^{-1}$. This means the RWA now gets applied to remove the relevant off-diagonal term in the perturbed master equation. Then the error term contains a part of order τ_R^{-1} – of the same magnitude as $\mathcal{D}$ and thus non-negligible. In order to prevent this from happening, in such a situation we, therefore, need the additional condition $\tau_R \ll \tau_V$ – i.e., the perturbation must be weaker than the decoherence term. This is stricter than the small perturbation conditions (iii) and (iv) assumed above.

Now applying our bound (11.3.4) to this setting, we identify

- The *true* perturbed trajectory:

$$\frac{d\eta_t}{dt} = \mathcal{L}'(\eta_t), \tag{11.4.16}$$

- The *approximate* perturbed trajectory:

$$\frac{d\sigma_t}{dt} = \mathcal{L}(\sigma_t) + v\mathcal{V}(\sigma_t). \tag{11.4.17}$$

In the latter, we only perturb the Hamiltonian term and ignore the additional terms of size ϵ. All trajectories have the same initial state ϱ_0. Now we have the error estimation:

Result 49. *For an open system in the weak coupling regime perturbed by the Hamiltonian vV, we have the speed limit*

$$\theta_B(\varrho_t, \eta_t) \leq \frac{1}{2}\int_0^t ds\, v\sqrt{\mathcal{F}(\eta_s, \mathcal{V})} + \Delta(t), \tag{11.4.18}$$

where the error term is bounded by the estimate

$$|\Delta(t)| \lesssim \Delta_{\text{est}}(t) = \frac{4\sqrt{2}}{3}\|V\|\epsilon^{\frac{1}{2}}(vt)^{\frac{3}{2}} + \epsilon vt. \tag{11.4.19}$$

Remark 64. The proof is given below. For short times, the QFI term in Eq. (11.4.18) is roughly $vt\sqrt{\mathcal{F}(\varrho_0, \mathcal{V})}$ – hence, we expect the error term to be negligible when $\sqrt{\mathcal{F}(\varrho_0, \mathcal{V})} \gg \max\{\sqrt{\epsilon vt}, \epsilon\}$.

Proof. The triangle inequality for θ_B and an application of Result 47 implies

$$\begin{aligned}\theta_B(\varrho_t, \eta_t) &\leq \theta_B(\varrho_t, \sigma_t) + \theta_B(\sigma_t, \eta_t)\\ &\leq \frac{1}{2}\int_0^t ds\, v\sqrt{\mathcal{F}(\sigma_s, \mathcal{V})} + \theta_B(\sigma_t, \eta_t)\\ &\leq \frac{1}{2}\int_0^t ds\, v\sqrt{\mathcal{F}(\eta_s, \mathcal{V})} + \Delta_1(t) + \Delta_2(t),\end{aligned} \tag{11.4.20}$$

where the error terms are

$$\Delta_1(t) = \frac{1}{2}\left|\int_0^t ds\, v\sqrt{\mathcal{F}(\sigma_s,\mathcal{V})} - \int_0^t ds\, v\sqrt{\mathcal{F}(\eta_s,\mathcal{V})}\right|,$$
$$\Delta_2(t) = \theta_B(\sigma_t,\eta_t). \tag{11.4.21}$$

In order to bound these errors, we start by showing that Δ_1 can be related to Δ_2. Firstly, using the fact that

$$(\sqrt{x}-\sqrt{y})^2 = x+y-2\sqrt{xy} \leq x+y-2\min\{x,y\} = |x-y|, \tag{11.4.22}$$

we have

$$\Delta_1(t) \leq \frac{v}{2}\int_0^t ds\left|\sqrt{\mathcal{F}(\sigma_s,\mathcal{V})}-\sqrt{\mathcal{F}(\eta_s,\mathcal{V})}\right| \leq \frac{v}{2}\int_0^t ds\sqrt{|\mathcal{F}(\sigma_s,\mathcal{V})-\mathcal{F}(\eta_s,\mathcal{V})|}. \tag{11.4.23}$$

Now we use the QFI continuity result Eq. (A6) from Ref. [620]:

$$|\mathcal{F}(\sigma,\mathcal{V})-\mathcal{F}(\eta,\mathcal{V})| \leq 32 D_B(\sigma,\eta)\|V\|^2, \tag{11.4.24}$$

in terms of the Bures distance $D_B = \sqrt{2(1-F)}$ which satisfies $D_B \leq \theta_B$ (where F is the Uhlmann). Inserting this into Eq. (11.4.23) gives

$$\Delta_1(t) \leq 2\sqrt{2}v\|V\| \int_0^t ds\, \sqrt{\Delta_2(s)}. \tag{11.4.25}$$

Now we bound Δ_2 using another application of the speed limit in Result 47, now comparing σ_s and η_s under the error term $\mathcal{H}_{\text{LS}}^{(1)} + \mathcal{D}^{(1)}$. To lowest order in v,

$$\Delta_2(t) \leq \frac{v}{2}\int_0^t ds\, \sqrt{\mathcal{F}(\eta_s, \mathcal{H}_{\text{LS}}^{(1)} + \mathcal{D}^{(1)})}. \tag{11.4.26}$$

To proceed, let us use Lemma in Ref. [9]: It states that for any state ϱ and generator $\mathcal{L}$, we have

$$\mathcal{F}(\varrho,\mathcal{L}) \leq 4\max_{\psi}\|\mathcal{L}(\psi)\|^2, \tag{11.4.27}$$

with the maximization being over pure states ψ. Then we find that the size of the integrand is bounded as

$$\Delta_2(t) \leq vt \max_{\psi}\|\mathcal{H}_{\text{LS}}^{(1)}(\psi) + \mathcal{D}^{(1)}(\psi)\| = vt\epsilon. \tag{11.4.28}$$

The right-hand side of Eq. (11.4.28) measures the size of the generator $\mathcal{H}_{\text{LS}}^{(1)} + \mathcal{D}^{(1)}$ in terms of its greatest effect on any pure state. In specific examples (see Sec. 11.6) this norm can be calculated explicitly; from Eq. (11.4.15), we can generally estimate

$$\epsilon = \mathcal{O}\left(\frac{\tau_S}{\tau_R}\right) + \mathcal{O}\left(\frac{\tau_B}{\tau_R}\right). \tag{11.4.29}$$

Inserting into Eq. (11.4.25), we have

$$\Delta_1(t) \leq 2\sqrt{2}v\|V\| \int_0^t ds\, \sqrt{v\epsilon s} = \frac{4\sqrt{2}}{3}\|V\|\epsilon^{\frac{1}{2}}(vt)^{\frac{3}{2}}. \tag{11.4.30}$$

□

11.5 Quantum resource witnessing

There are numerous applications in which one aims to experimentally demonstrate a large QFI of a system with respect to some Hamiltonian V. Apart from establishing the system's usefulness for probing the strength of V, a suitable choice of Hamiltonian allows the observation of various quantum resources, such as many-body entanglement [169, 176, 320, 624], optical nonclassicality [612, 613], and quantum steering [625]. In all of these scenarios, the resource is witnessed when the QFI $\mathcal{F}(\varrho, \mathcal{V})$ exceeds a certain threshold value $\mathcal{F}_*$. Uhlmann's bound can be used in the absence of decoherence. However, in the presence of decoherence, an experimental lower bound for $\theta_B(\varrho_0, \varrho_t)$ can be obtained by performing measurements on the system either at time zero or time t in each experimental run. These measurements yield probability distributions of outcomes $p_i(0)$, $p_i(t)$.

The closeness between these distributions as measured by the Bhattacharyya coefficient [626] $B(\boldsymbol{p}(0), \boldsymbol{p}(t)) = \sum_i \sqrt{p_i(0) p_i(t)}$ is an upper bound to the quantum fidelity: $B(\boldsymbol{p}(0), \boldsymbol{p}(t)) \geq F(\varrho_0, \varrho_t)$, hence $\arccos B(\boldsymbol{p}(0), \boldsymbol{p}(t)) \leq \theta_B(\varrho_0, \varrho_t)$. This bound holds for any chosen measurement and can be saturated with an optimal measurement. The presence of the resource is therefore witnessed when $\frac{2}{tv} \arccos B(\boldsymbol{p}(0), \boldsymbol{p}(t)) > \sqrt{\mathcal{F}_*}$.

In practice, decoherence cannot always be neglected, which calls for a different protocol. We propose a new approach, exploiting the bound given in Eq. (11.3.4). The experiment is carried out in two ways: one allows the system to evolve under the dynamics generated by $\mathcal{L}$, while the other involves adding the perturbation $v\mathcal{V}$. In both cases, the same measurement is performed at time t, yielding the statistics $p_i(t)$ and $q_i(t)$ respectively. Assuming that the perturbation is exactly $\mathcal{P} = v\mathcal{V}$, the right-hand side of Eq. (11.3.4) equals $\frac{tv}{2}$ times the time-averaged value of $\sqrt{\mathcal{F}(\sigma_s, \mathcal{V})}$. Consequently, the presence of the resource at some time $s \in [0, t]$ within the perturbed trajectory is established whenever

$$\frac{2 \arccos B(\boldsymbol{p}(t), \boldsymbol{q}(t))}{tv} > \sqrt{\mathcal{F}_*}. \tag{11.5.1}$$

This criterion can be easily generalized to cases when the coefficient v_t varies with time (e.g., following a known pulse shape). The Cauchy-Schwarz inequality applied to the right-hand side of Eq. (11.3.4) gives

$$\begin{aligned} \int_0^t ds\, \sqrt{\mathcal{F}(\sigma_s, v_s \mathcal{V})} &= \int_0^t ds\, |v_s| \sqrt{\mathcal{F}(\sigma_s, \mathcal{V})} \\ &\leq \left(\int_0^t ds\, v_s^2 \right)^{\frac{1}{2}} \left(\int_0^t ds\, \mathcal{F}(\sigma_s, \mathcal{V}) \right)^{\frac{1}{2}} \\ &= t \langle v_s^2 \rangle_t^{\frac{1}{2}} \langle \mathcal{F}(\sigma_s, \mathcal{V}) \rangle_t^{\frac{1}{2}}, \end{aligned} \tag{11.5.2}$$

where angled brackets $\langle \cdot \rangle_t$ denote a time average over $s \in [0, t]$. Thus, the witness criterion in Eq. (11.5.1) is modified by replacing v with the root-mean-square $\langle v_s^2 \rangle_t^{\frac{1}{2}}$.

In a weak coupling setting, one can employ the error $\Delta_{\text{est}}(t)$ from Eq. (11.4.18) to tighten the threshold value in Eq. (11.5.1) to $\sqrt{\mathcal{F}_*} + \frac{2\Delta_{\text{est}}(t)}{vt}$. The change in this threshold is roughly

$$\frac{2\Delta_{\text{est}}(t)}{vt} = \mathcal{O}(\sqrt{\epsilon vt}) + \mathcal{O}(\epsilon). \tag{11.5.3}$$

11.6 Example: dephasing model

11.6.1 Single-qubit system

First, let us consider a single-qubit system in which it dephases by interacting independently with a bath of harmonic oscillators – see, for example, Ref. [43]. We take:

- System Hamiltonian: $H = \frac{h}{2}\sigma_z$,
- Pertubation Hamiltonian: $V = \frac{1}{2}\sigma_x$,
- Bath Hamiltonian: $H_B = \sum_k \omega_k b_k^\dagger b_k$, with b_k being the bosonic annihilation operator for mode k, satisfying $[b_k, b_k^\dagger] = \mathbb{1}$,
- Interaction Hamiltonian: $H_I = \lambda\sigma_z \otimes \sum_k g_k(b_k + b_k^\dagger)$, with g_k being dimensionless coupling coefficients,
- Continuum limit with an Ohmic bath, replacing g_k^2 by a spectral density function: $J(\omega) = \eta\omega e^{-\omega/\omega_c}$, with η being a constant with dimensions of time squared and ω_c being a cut-off frequency that we take to be large compared with all other relevant frequency scales.

Given that the bath is in a thermal state at inverse temperature β, one can derive [43]

$$\gamma(\omega) = \frac{2\pi\eta e^{-|\omega|/\omega_c}}{1 - e^{-\beta\omega}}. \tag{11.6.1}$$

In this case, we find the following:

Result 50. *The single-qubit error parameter ϵ_1 is therefore bounded by*

$$\epsilon_1 \leq \frac{2\lambda^2\gamma(0)}{h}. \tag{11.6.2}$$

Proof. Since there is a single jump operator in the master equation, $A = A(0) = \sigma_z$, from the proof in Result 48, we find $A^{(1)}(0) = \sigma_x$ and thus

$$H_{\text{LS}}^{(1)} = 0, \qquad \mathcal{D}^{(1)}(\varrho) = \frac{\lambda^2\gamma(0)}{h}\left(\sigma_z\varrho\sigma_x + \sigma_x\varrho\sigma_z\right). \tag{11.6.3}$$

Then $\gamma(0) = 2\pi\eta/\beta$ and $\tau_B \sim \beta$. In this case, note that the derivative $\partial_\omega\gamma(\omega)$ does not appear. However, for large ω_c one finds

$$\lim_{\omega\to 0^+} \partial_\omega\gamma(\omega) \approx \lim_{\omega\to 0^-} \partial_\omega\gamma(\omega) \approx \pi\eta \sim \gamma(0)\tau_B, \tag{11.6.4}$$

which is consistent with the claim in Eq. (11.4.14). The error terms are easily bounded using

$$\|\sigma_z\psi\sigma_x + \sigma_x\psi\sigma_z\| \leq 2\|\sigma_z\psi\sigma_x\| \leq 2\|\sigma_z\|\|\psi\|\|\sigma_x\| = 2. \tag{11.6.5}$$

□

11.6.2 Two-qubit system

For a two-qubit system , consider $H = \frac{h}{2}(\sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z)$, $V = \frac{1}{2}(\sigma_x \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_x)$, and an independent coupling of each qubit to a bath of the form $\lambda\sigma_z \otimes \sum_k g_k(b_k + b_k^\dagger)$, with g_k being dimensionless coupling coefficients. This gives local dephasing dynamics

$$\mathcal{D}(\varrho) = \lambda^2\gamma\left[(\sigma_z \otimes \mathbb{1})\varrho(\sigma_z \otimes \mathbb{1}) + (\mathbb{1} \otimes \sigma_z)\varrho(\mathbb{1} \otimes \sigma_z) - 2\varrho\right], \tag{11.6.6}$$

writing $\gamma = \gamma(0)$. Then we find

$$\epsilon \leq 2\epsilon_1 \leq 4\lambda^2\frac{\gamma}{h}. \tag{11.6.7}$$

Note that an extension of this model to N qubits would have an error term scaling with N; a similar analysis could also be performed for a collective decoherence model where all qubits couple to the same bath [627].

Remark 65. The validity and tightness of the estimates in Result 49 are shown in Fig. 11.2.

Remark 66. A simulation of this protocol is shown in Fig. 11.3 for the two-qubit dephasing model described above. A measurement in the Bell basis

$$\{\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}\} \tag{11.6.8}$$

is used for the Bhattacharrya coefficient. For any separable state ϱ_{sep} of two qubits, we have the inequality $\mathcal{F}(\varrho_{\text{sep}}, \mathcal{V}) \leq \mathcal{F}_* = 2$ [169, 176, 320]. Using the parameters $h = 1$ and $\lambda = \gamma = v = 0.1$, this threshold is broken by the exact QFI for $t \lessapprox 1.41$, while entanglement is witnessed taking into account the error estimate for $t \lessapprox 1.26$.

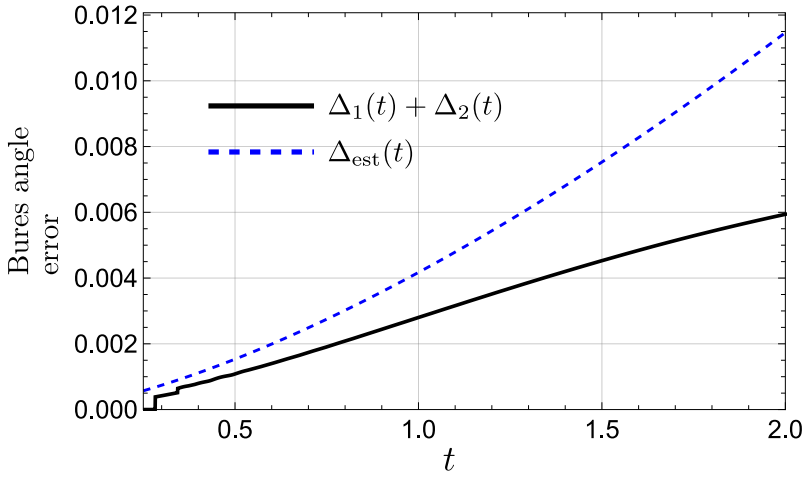

Figure 11.2: Demonstration of error bound for the two-qubit example, taking the same parameters as in Fig. 11.3. The error being shown is that on the right-hand side of the weak coupling speed limit Eq. (11.4.18): both the sum of the terms $\Delta_1(t) + \Delta_2(t)$ from Eq. (11.4.21) (which in this case is dominated by Δ_2) and the upper bound estimate $\Delta_{\rm est}(t)$ from Eqs. (11.4.25), (11.4.28). This figure is taken from Ref. [9].

11.7 Quantum work fluctuations

Finally, we show the implications of our speed limit for fluctuations in work performed during a sudden quench driving a system out of equilibrium. Consider a system with Hamiltonian H which is initially in thermal equilibrium at inverse temperature β, in the Gibbs state $\varrho_{\rm th} = \frac{e^{-\beta H}}{{\rm tr}e^{-\beta H}}$. At time 0, the Hamiltonian is quickly changed to H', involving fluctuating work w done on the system. The mean and variance of the work are computed from the change in the Hamiltonian ΔH:

$$\Delta H = H' - H, \quad \langle w \rangle = {\rm tr}[\varrho_{\rm th} \Delta H], \quad {\rm Var}_w = {\rm Var}(\varrho_{\rm th}, \Delta H). \tag{11.7.1}$$

If the system is subsequently left to thermalise to the new Gibbs state $\varrho'_{\rm th} = \frac{e^{-\beta H'}}{{\rm tr}e^{-\beta H'}}$, then its Helmholtz free energy $F_{H,\beta}$ will decrease. This is defined by

$$F_{H,\beta} = {\rm tr}[\varrho_{\rm th} H] - \beta^{-1} S(\varrho_{\rm th}), \tag{11.7.2}$$

where $S(\varrho_{\rm th}) = -{\rm tr}[\varrho_{\rm th} \ln \varrho_{\rm th}]$ is the von Neumann entropy [450]. The second law of thermodynamics implies that the change

$$\Delta F = F_{H',\beta} - F_{H,\beta} \leq \langle w \rangle, \tag{11.7.3}$$

which is equivalent to saying that the dissipated work [450]:

$$W_{\rm diss} = \langle w \rangle - \Delta F \geq 0. \tag{11.7.4}$$

This is thus associated with nonequilibrium entropy production.

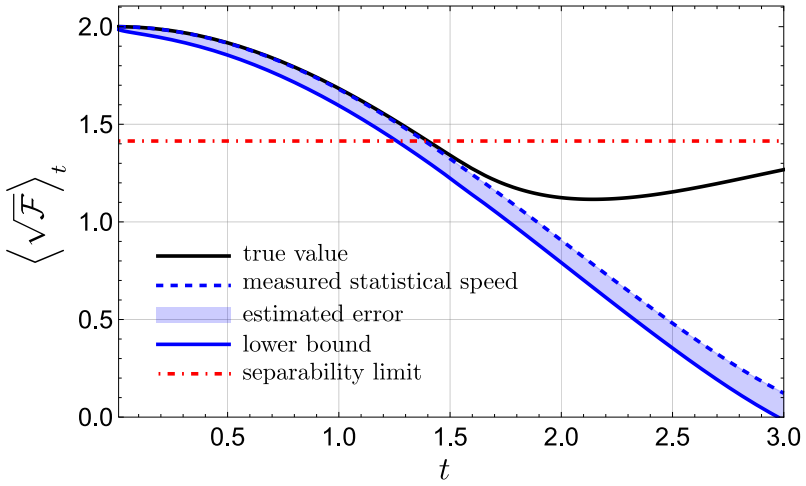

Figure 11.3: Two-qubit example with local dephasing noise, showing how the time-averaged value of $\sqrt{\mathcal{F}(\eta_s, \mathcal{V})}$ from $s = 0$ to t can be lower-bounded using the speed limit Eq. (11.4.18). The initial state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is maximally entangled. In units of $h = 1$, we take $\lambda = \gamma = v = 0.1$ and $\epsilon \leq 4\lambda^2\gamma/h = 0.004$. The measured statistical speed is the left-hand side of Eq. (11.5.1), taking a measurement in the Bell basis $\{\frac{|00\rangle\pm|11\rangle}{\sqrt{2}}, \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}\}$. The estimated error $\frac{2\Delta_{\text{est}}(t)}{vt}$ (indicated by the shaded area) is subtracted to give the lower bound. This figure is taken from Ref. [9].

In order to study small deviations from equilibrium, we follow the paradigm of, for instance, Refs. [628, 629], in which ΔH is taken as small. One then finds a fluctuation-dissipation relation [629]

$$\frac{\beta}{2}\text{Var}_w = W_{\text{diss}} + Q_w. \tag{11.7.5}$$

Here, $Q_w \geq 0$ is a quantum correction to the usual relation for classical systems [630, 631], thus Eq. (11.7.5) represents a modification of a classical statistical law near equilibrium that takes into account coherent quantum effects. It also implies a barrier to finding coherent protocols that simultaneously minimise work fluctuations and dissipation [629].

The relation Eq. (11.7.5) holds for a range of slow driving settings; in our case with a single small quench, Q_w is determined by a quantity closely related to the QFI:

$$\begin{aligned} Q_w &= \frac{\beta}{2}\bar{I}(\varrho_{\text{th}}, \Delta H), \\ \bar{I}(\varrho, A) &:= \int_0^1 dk\, \frac{1}{2}\text{tr}\left([\varrho^k, A][A, \varrho^{1-k}]\right). \end{aligned} \tag{11.7.6}$$

The details of this result from Ref. [629] are recalled in Sec. 11.8. Here, $\bar{I}$ belongs to a family of generalized quantum Fisher information quantities [632].

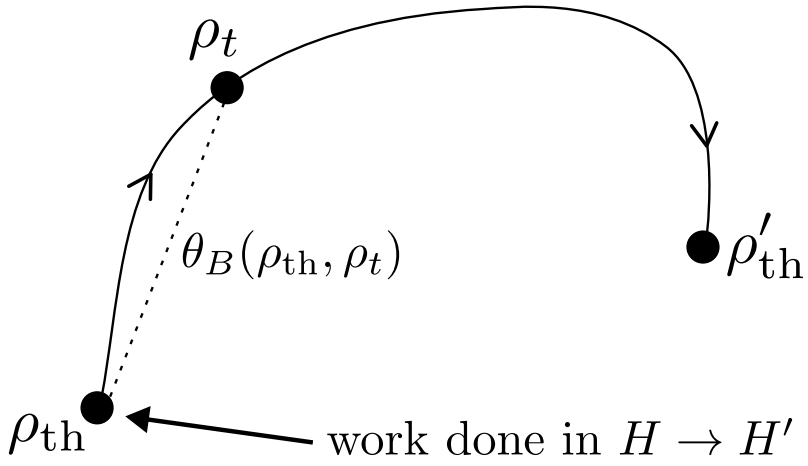

Figure 11.4: Driving out of equilibrium: work is performed during a sudden quench $H \to H'$. The system moves away from its initial Gibbs state $\varrho_{\rm th}$ to the new one $\varrho'_{\rm th}$. The speed limit Eq. (11.7.7) bounds the distance between $\varrho_{\rm th}$ and the state ϱ_t after time t in terms of quantum fluctuations in the work. This figure is taken from Ref. [9].

Members of this family are interpreted as measures of quantum coherence (also known as asymmetry in this context): $\bar{I}(\varrho, H)$ and $\mathcal{F}(\varrho, \mathcal{H})$, among others, quantify the coherence of a state ϱ with respect to a Hamiltonian H [606, 609, 617, 633]. Moreover, they can be regarded as quantum contributions to the variance of H [634–636]. Applied to $\bar{I}$, some of the key properties justifying this interpretation are that $\bar{I}(\varrho, H) \leq \mathrm{Var}(\varrho, H)$, with equality for pure states, and $\bar{I}(\varrho, H) = 0$ when ϱ commutes with H. Therefore, as required of a measure of quantum work fluctuations, $2Q_w/\beta = \bar{I}(\varrho_{\rm th}, \Delta H)$ vanishes exactly when $[H, \Delta H] = 0$.

We now use our speed limit to derive the following bound on how fast the state ϱ_t can evolve away from the initial Gibbs state (illustrated in Fig. 11.4).

Result 51. *Quantum work fluctuations are necessary for fast departure from equilibrium. For a system weakly coupled to a thermal environment, at all times $t > 0$ following the quench $H \to H'$, the distance between the initial Gibbs state $\varrho_{\rm th}$ and the system's state ϱ_t is limited by*

$$\theta_B(\varrho_{\rm th}, \varrho_t) \leq t\sqrt{3\bar{I}(\varrho_{\rm th}, \Delta H)} + \Delta(t), \tag{11.7.7}$$

where $\Delta(t)$ is the weak coupling error term from Eq. (11.4.19).

Proof. This can be proven by using Result 49 with initial state $\varrho_{\rm th}$, but instead reversing the roles of the perturbed and unperturbed trajectories. So now the unperturbed trajectory involves the Hamiltonian H' and its dynamics are generated by $\mathcal{L}'$, while the perturbation is $vV = -\Delta H$. Doing it this way around, the QFI appearing on the right-hand side of the speed limit is $\mathcal{F}(\varrho_{\rm th}, \Delta\mathcal{H})$, which is constant in time since the perturbed state $\varrho_t = \varrho_{\rm th}\, \forall\, t \geq 0$ is a steady state under $\mathcal{L}$. The relevant Bures angle is then $\theta_B(\varrho'_t, \varrho_t) = \theta_B(\varrho'_t, \varrho_{\rm th})$. We show in Sec. 11.8

that the QFI and $\bar{I}$ never differ by more than a constant factor: $4\bar{I} \leq \mathcal{F} \leq 12\bar{I}$. Finally using the the latter inequality, we have $\mathcal{F}(\varrho_{\text{th}}, \Delta\mathcal{H}) \leq 12\bar{I}(\varrho_{\text{th}}, \Delta H)$. □

A fast departure from ϱ_{th} thus requires a large value of quantum work fluctuations as measured by $\bar{I}(\varrho_{\text{th}}, \Delta H)$ – equivalently, ϱ_{th} must have a high degree of quantum coherence with respect to ΔH.

The physical importance of the correction $\Delta(t)$ is seen in the "classical" case where $[H, \Delta H] = 0$ (i.e., the energy levels are changed but not the energy eigenstates). Then $\bar{I} = 0$ but the system must deviate from ϱ_{th} in order to reach the new steady state ϱ'_{th}. From our earlier discussion of the weak coupling error and Eq. (11.4.19), by identifying v with $\|\Delta H\|$, we therefore see that the *quantum driving regime* – i.e., when the term with $\bar{I}$ dominates on the right-hand side of Eq. (11.7.7) – corresponds to

$$\frac{\sqrt{\bar{I}(\varrho_{\text{th}}, \Delta H)}}{\|\Delta H\|} \gg \max\{\sqrt{\epsilon \|\Delta H\| t}, \epsilon\}. \tag{11.7.8}$$

The left-hand side of this inequality measures the quantum work fluctuations relative to the size of ΔH. In the quantum driving regime, coherent evolution resulting from the change in Hamiltonian happens faster than thermalisation.

11.8 Detailed discussions about Result 51

Here, we first recall the derivation in Ref. [629] of Eq. (11.7.5). It starts from writing the dissipated work in terms of relative entropy as $\beta W_{\text{diss}} = S(\varrho_{\text{th}} || \varrho'_{\text{th}}) = \text{tr}[(\varrho_{\text{th}} - \varrho'_{\text{th}}) \ln \varrho'_{\text{th}}]$. For small ΔH, this can be approximated to lowest order as

$$W_{\text{diss}} \approx \frac{\beta}{2} \text{Var}^{\text{K}}(\varrho_{\text{th}}, \Delta H), \tag{11.8.1}$$

where Var^{K} is the so-called Kubo-Mori generalised variance [632]. This can be expressed using a superoperator $\mathbb{J}_\varrho$ which depends on a given state ϱ:

$$\mathbb{J}_\varrho(A) = \sum_{i,j} \frac{\lambda_i - \lambda_j}{\ln \lambda_i - \ln \lambda_j} \langle \psi_i | A | \psi_j \rangle \, |\psi_i\rangle\langle\psi_j| \,, \tag{11.8.2}$$

where λ_i and $|\psi_i\rangle$ are the eigenvalues and eigenvectors of ϱ. Then we have

$$\text{Var}^{\text{K}}(\varrho, A) = \text{tr}\left[\bar{A} \mathbb{J}_\varrho(\bar{A})\right], \quad \bar{A} = A - \text{tr}[\varrho A]\mathbb{1}. \tag{11.8.3}$$

The crucial property is the splitting of the variance of ΔH into two terms:

$$\text{Var}(\varrho_{\text{th}}, \Delta H) = \text{Var}^{\text{K}}(\varrho_{\text{th}}, \Delta H) + \bar{I}(\varrho_{\text{th}}, \Delta H), \tag{11.8.4}$$

interpreted as classical and quantum components respectively (see also Ref. [636]).

We also require the connection between $\bar{I}$ and the QFI proved in Lemma 52 below. This makes use of the theory of generalised QFI quantities – see Ref. [632]

for details. Every generalised "skew information" I^f corresponds to a function $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ fulfilling the conditions $f(1) = 1$, $xf(x^{-1}) = f(x)$, and being a matrix monotone. If $f(0) \neq 0$, it is possible to normalise I^f to be "metric-adjusted" [637], such that $I^f(|\psi\rangle\langle\psi|, H) = \mathrm{Var}(|\psi\rangle\langle\psi|, H)$ for all pure states. Explicitly, we have

$$I^f(\varrho, H) = \frac{f(0)}{2} \sum_{i,j} \frac{(\lambda_i - \lambda_j)^2}{\lambda_j f(\lambda_i/\lambda_j)} |\langle i|H|j\rangle|^2. \tag{11.8.5}$$

The case $f(x) = \frac{x+1}{2}$ is often denoted by I^{SLD} (standing for "symmetric logarithmic derivative") and recovers the standard QFI under evolution generated by H: $4I^{\mathrm{SLD}}(\varrho, H) = \mathcal{F}(\varrho, \mathcal{H})$.

Result 52. *For all states ϱ and observables H,*

$$4\bar{I}(\varrho, H) \leq \mathcal{F}(\varrho, \mathcal{H}) \leq 12\bar{I}(\varrho, H). \tag{11.8.6}$$

Proof. We start from the definition $I^{(k)}(\varrho, H) = \frac{1}{2}\mathrm{tr}\left([\varrho^k, H][H, \varrho^{1-k}]\right)$, such that $\bar{I} = \int_0^1 dk\ I^{(k)}$. We can rewrite $I^{(k)}$ in terms of the matrix elements $H_{ij} = \langle\psi_i|H|\psi_j\rangle$ in the eigenbasis of $\varrho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$:

$$\begin{aligned}
I^{(k)}(\varrho, H) &= \mathrm{tr}\left(\varrho H^2 - \varrho^k H \varrho^{1-k} H\right) \\
&= \sum_{i,j} (\lambda_i - \lambda_i^k \lambda_j^{1-k}) H_{ij} H_{ji} \\
&= \sum_{i,j} \frac{1}{2} (\lambda_i + \lambda_j - \lambda_i^k \lambda_j^{1-k} - \lambda_i^{1-k} \lambda_j^k) |H_{ij}|^2 \\
&= \sum_{i,j} \frac{1}{2} (\lambda_i^k - \lambda_j^k)(\lambda_i^{1-k} - \lambda_j^{1-k}) |H_{ij}|^2 \\
&= \frac{f^{(k)}(0)}{2} \sum_{i,j} \frac{(\lambda_i - \lambda_j)^2}{\lambda_j f^{(k)}(\lambda_i/\lambda_j)} |H_{ij}|^2,
\end{aligned} \tag{11.8.7}$$

where $f^{(k)}$ is the matrix monotone function corresponding to $I^{(k)}$. We must therefore have

$$f^{(k)}(x) \propto \frac{(x-1)^2}{(x^k - 1)(x^{1-k} - 1)}. \tag{11.8.8}$$

In order to be normalized in the standard way, we require $f^{(k)}(1) = 1$; taking the limit $x \to 1$ in the above shows that

$$f^{(k)}(x) = \frac{k(1-k)(x-1)^2}{(x^k - 1)(x^{1-k} - 1)} \tag{11.8.9}$$

and $f^{(k)}(0) = k(1-k)$. For all metric-adjusted skew informations we have the inequality $I^f \leq I^{\mathrm{SLD}} \leq \frac{I^f}{2f(0)}$ [635]. It is immediate from its definition that $I^{(k)}$

is metric-adjusted. Thus, the lower bound on $\mathcal{F} = 4I^{\mathrm{SLD}}$ is immediate, and we also have

$$I^{(k)}(\varrho, H) \geq 2f^{(k)}(0)I^{\mathrm{SLD}}(\varrho, H) = \frac{f^{(k)}(0)}{2}\mathcal{F}(\varrho, \mathcal{H}) = \frac{k(1-k)}{2}\mathcal{F}(\varrho, \mathcal{H}). \quad (11.8.10)$$

Finally,

$$\bar{I}(\varrho, H) \geq \int_0^1 dk\, \frac{k(1-k)}{2}\mathcal{F}(\varrho, \mathcal{H}) = \frac{1}{12}\mathcal{F}(\varrho, \mathcal{H}). \quad (11.8.11)$$

□

11.9 Discussions

This Chapter demonstrated the extension of the well-known Mandelstam-Tamm quantum speed limit to describe the rate of divergence of a perturbed open quantum system from its unperturbed trajectory. We have found that this speed limit holds to a high degree of approximation when a system is weakly coupled to an environment, assuming only a small perturbing Hamiltonian and the standard Born-Markov and secular approximations and that the error may be bounded with knowledge of the relevant timescales. This results in a practically useful method for experimentally lower-bounding quantum Fisher information, where the error need not be neglected but can be estimated and taken into account. Finally, we used the speed limit to prove that quantum work fluctuations are necessary to have a fast departure from equilibrium in a perturbed system weakly coupled to a thermal environment.

It is worth noting that we can derive a similar speed limit by replacing the Bures angle with the quantity $\tilde{\theta}(\varrho, \sigma) = \arccos \mathrm{tr}(\sqrt{\varrho}\sqrt{\sigma})$ and the Quantum Fisher Information (QFI) with four times the Wigner-Yanase skew information [638], given by $I^{\mathrm{WY}}(\varrho, \mathcal{V}) = -\frac{1}{2}\mathrm{tr}([\sqrt{\varrho}, V]^2)$ in the Hamiltonian case. Future work may explore the extension of the speed limit to different distance measures or generalized QFI quantities [632].

In the weak coupling regime, an interesting direction for further investigation is to determine the error term for slow continuous changes in the perturbation, using the theory of adiabatic master equations [639]. This could lead to a generalization of Result 51 to account for continuous driving. Additionally, it would be valuable to explore whether this has implications for thermodynamic uncertainty relations, which connect current fluctuations to entropy production [640].

Finally, since our speed limit holds under the assumption of Markovian dynamics, a violation of the inequality could be used as a witness of non-Markovianity. For this purpose, one would need an independent method to estimate (upper-bound) the QFI, for example via the variance of the perturbing Hamiltonian. This would contribute to a library of witnesses of non-Markovianity, including those based on the contractivity of QFI over time [618, 628].

Chapter 12

Multipartite entanglement under partial classicalization

This thesis has discussed several approaches to analyzing quantum systems under limited control over them. This Chapter addresses the question of the extent to which multipartite entanglement changes when one particle is destructed by a measurement but the information obtained is still available. This Chapter is based on Ref. [5].

12.1 Introduction

Different types of quantum resources [101] are essential for quantum information tasks, like quantum computation [641], quantum key distribution [642], and quantum metrology [286], where they can provide a decisive advantage over the classical regime. One main problem for many quantum resources is their sensitivity to the disturbance from the environment. Their protection with tools like quantum error correction [643] is usually expensive, especially if larger systems are considered. In practice, some fraction of the particles of a larger quantum system can inevitably become classical, e.g., caused by a measurement or decoherence process. In fact, the particles may even be completely lost.

It is a natural question to ask how multiparticle entanglement [17, 120] is affected by such processes. Many works have considered the influence of decoherence on multiparticle entanglement [644–649].

Other works considered the robustness of multiparticle entanglement under particle loss [142, 650–652]. Moreover, the sharp change of bipartite entanglement caused by the complete loss of one particle in one party has been studied as the concept of lockable entanglement [281, 282, 653, 654]. There can, however, still be information left in the environment after the loss of particles. For example, in the case of the Stern-Gerlach experiment, the left information is given by the location of the spots on the screen.

As another example, one can consider the decay of particles due to decoherence. Then it may be reasonable to gather some information from the particles

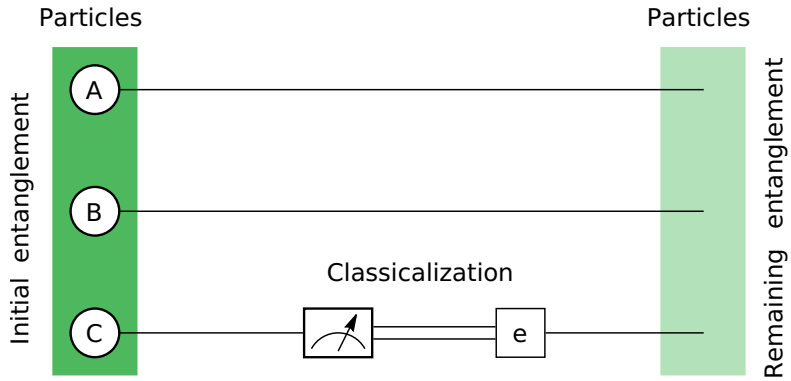

Figure 12.1: The change of multiparticle entanglement if the particle C becomes classical. In this process of classicalization the particle C is first destroyed by the measurement and then the measurement information is encoded in a new register. This Chapter asks for which classicalization procedure the change of entanglement is minimal. This figure is taken from Ref. [5].

before their complete decay. The usefulness of this classical information has been extensively explored in the form of the entanglement of assistance [655]. There a third party (Charly) optimizes the measurement and the resulting information to assist the two original parties (Alice and Bob) to reveal as much quantum entanglement as possible. Most research on the entanglement of assistance has focused on the case where the global state is pure [656–658]. As it turns out [655], the entanglement of assistance depends only on the reduced state for Alice and Bob, and the exact three-partite initial state is not important.

In this Chapter, we consider a different scenario: One or more particles in a multiparticle system are destructed by a measurement. The gained classical information is then encoded in a quantum state. Our question is how much the multiparticle entanglement is affected in this process of classicalization, see also Fig. 12.1. This scenario is practically relevant, as one may not have the perfect 'assistance' when the size and performance of the register system are limited. Consequently, our approach can provide guidance for the storage of quantum entanglement robust to particle loss. It also gives suggestions for finding the optimal strategy of entanglement recovery with the gained classical information and a small register system. In comparison with the concept of quantum assistance, we consider mixed quantum states where the entanglement is stored and it is not the aim of the measured party to increase the bipartite entanglement between the remaining ones.

Most importantly, the initial quantum state plays a major role in the change of entanglement due to classicalization. We stress that there are further related concepts. The so-called hidden entanglement [659] has been introduced as the difference between the entanglement without the decomposition information of a mixed state and the one with the decomposition information. Besides, the role of one particle in the change of entanglement has also been considered in distributed entanglement [660, 661]. There, the particle is transferred from one

party to another one rather than it is destroyed.

12.2 Notations and definitions

We focus on tripartite systems in this Chapter, other multipartite systems can be analyzed similarly. We denote the initial state as ϱ_{ABC}. First, suppose that one party of this state is measured in a process that completely destroys the measured party, such as the detection of the photon polarization.

Without loss of generality, we here assume that the destructive measurement $M = \{m_i\}$ acts on the party C. After the measurement, the particles belonging to party C vanish, but the post-measurement information from the associated outcome is available. That is, each classical outcome i can be encoded into a new register system E as associated post-measurement states τ_i. We say that this encoding is perfect, if $\tau_i = |i\rangle\langle i|$ for an orthogonal basis $\{|i\rangle\}$. In practice, of course, the encoding may not be perfect due to the interaction with the environment.

We can write the above process as the operation

$$\Phi_C(\varrho_{ABC}) = \sum_i p_i \sigma_i \otimes \tau_i, \quad p_i = \mathrm{tr}(\varrho_{ABC} m_i), \quad \sigma_i = \mathrm{tr}_C(\varrho_{ABC} m_i)/p_i, \tag{12.2.1}$$

where τ_i is the register state related to the outcome i. We say that this encoding is perfect, if $\tau_i = |i\rangle\langle i|$ for an orthogonal basis $\{|i\rangle\}$. In practice, of course, the encoding may not be perfect due to the interaction with the environment or the limited memory of the register.

We denote by $\mathcal{N}_C$ the set of all possible operations in the form in Eq. (12.2.1) on the party C. We stress that the set $\mathcal{N}_C$ is equivalent to the set of entanglement breaking channels [662] acting on the party C. So far, we have not imposed any assumption on the destructive measurements and the encoding, but in practice, there can be extra limitations on them.

Our central question is how much the global entanglement in ϱ_{ABC} is changed by the operation Φ_C. The maximal change happens usually when there is no classical information left or it has not been employed, that is, the τ_i are the same for all outcomes i's, a similar question has been explored already under the concept of lockable entanglement [282], see more details in Sec. 12.5. Here we are particularly interested in the minimal amount of entanglement change with remaining classical information, which corresponds to the optimal operation Φ_C to keep as much entanglement as possible.

For this purpose, we define the quantity $\Delta_{\mathcal{E}}(\varrho_{ABC})$ as

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) = \min_{\Phi_C \in \mathcal{N}_C} \{\mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\Phi_C(\varrho_{ABC})]\}, \tag{12.2.2}$$

where $\mathcal{E}$ is a tripartite entanglement measure. The practical choice of $\mathcal{E}$ may depend on the quantum information task under consideration. For the choice of entanglement measures, it is necessary to require that $\mathcal{E}$ does not increase under local operations and classical communication (LOCC) [55], called monotonicity under LOCC. In this case, $\Delta_{\mathcal{E}}(\varrho_{ABC})$ is always non-negative.

Remark 67. Two further remarks are in order. First, if $\mathcal{E}$ is a measure of genuine multipartite entanglement, then $\Delta_{\mathcal{E}}(\varrho_{ABC}) = \mathcal{E}[\varrho_{ABC}]$, since $\Phi_C(\varrho_{ABC})$ is always separable with respect to the bipatition $AB|C$ for any Φ_C and ϱ_{ABC}. Second, if we restrict the set $\mathcal{N}_C$ with limitations on measurements and register states, the amount of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ can be affected. One example is to consider the operations which keep the dimension of the system.

12.3 Simplification

In general, it is difficult to calculate $\Delta_{\mathcal{E}}(\varrho_{ABC})$, due to the complexity of characterizing the set $\mathcal{N}_C$. Here we provide a method to simplify the calculation. By default, we assume the entanglement measure $\mathcal{E}$ is monotonic under LOCC. Then we have:

Result 53. *If the entanglement measure $\mathcal{E}$ is convex, we only need to consider $M = \{m_i\}$ as an extremal point in the considered measurement set $\mathcal{M}$. More precisely:*

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) = \min_{M \in \partial\mathcal{M}} \left\{ \mathcal{E}[\varrho_{ABC}] - \sum_i p_i \mathcal{E}[\sigma_i \otimes |0\rangle\langle 0|] \right\}, \tag{12.3.1}$$

where $p_i = \mathrm{tr}(\varrho_{ABC} m_i)$, $\sigma_i = \mathrm{tr}_C(\varrho_{ABC} m_i)/p_i$, and $\partial\mathcal{M}$ is the set of extremal points in $\mathcal{M}$.

Proof. For any entanglement-breaking channel Φ_C, we have the decomposition:

$$\Phi_C(\varrho_{ABC}) = \sum_i p_i \sigma_i \otimes \tau_i, \quad p_i = \mathrm{tr}(\varrho_{ABC} m_i), \quad \sigma_i = \mathrm{tr}_C(\varrho_{ABC} m_i)/p_i \tag{12.3.2}$$

where $M = \{m_i\}$ is a measurement acting on C and τ_i is the state encoding the measurement outcome i. Since the set $\mathcal{M}$ of all POVMs acting on C is convex, any POVM $M = \{m_i\}$ can be decomposed into the convex combinations of extreme points of $\mathcal{M}$. That is, we have

$$m_i = \sum_k c_k m_i^{(k)}, \forall i, \tag{12.3.3}$$

where $M^{(k)} = \{m_i^{(k)}\}$ is an extreme point in the set $\mathcal{M}$ and $0 < c_k \leq 1$ with $\sum_k c_k = 1$. Consequently, the operation Φ_C can be rewritten as

$$\Phi_C(\varrho_{ABC}) = \sum_k c_k \Phi_C^{(k)}(\varrho_{ABC}), \quad \Phi_C^{(k)}(\varrho_{ABC}) = \sum_i \mathrm{tr}_C\left(\varrho_{ABC} m_i^{(k)}\right) \otimes \tau_i. \tag{12.3.4}$$

In the case that the entanglement measure $\mathcal{E}$ is convex, we have

$$\mathcal{E}[\Phi_C(\varrho_{ABC})] \leq \sum_k c_k \mathcal{E}\left[\Phi_C^{(k)}(\varrho_{ABC})\right] \leq \max_k \mathcal{E}\left[\Phi_C^{(k)}(\varrho_{ABC})\right]. \tag{12.3.5}$$

This implies that the maximal value of $\mathcal{E}[\Phi_C(\varrho_{ABC})]$, or equivalently, the value of $\Delta_{\mathcal{E}}(\varrho_{ABC})$, can always be achieved by extreme POVMs. That is,

$$\max_{\Phi_C \in \mathcal{N}_C} \mathcal{E}\left[\Phi_C(\varrho_{ABC})\right] = \max_{M \in \partial\mathcal{M}, \{\tau_i\}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes \tau_i\right), \tag{12.3.6}$$

where $\partial\mathcal{M}$ is the set of all extreme POVMs.

Note that, any imperfect encoding can be generated from the perfect one by local operations. Since the entanglement measure $\mathcal{E}$ is LOCC monotonic, we have $\mathcal{E}\left(\sum_i p_i \sigma_i \otimes \tau_i\right) \leq \mathcal{E}\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|_C\right)$. This implies that,

$$\max_{M \in \partial\mathcal{M}, \{\tau_i\}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes \tau_i\right) \leq \max_{M \in \partial\mathcal{M}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|_C\right). \tag{12.3.7}$$

Since $\{\tau_i = |i\rangle\langle i|\}$ is just a special encoding, we have

$$\max_{M \in \partial\mathcal{M}, \{\tau_i\}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes \tau_i\right) \geq \max_{M \in \partial\mathcal{M}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|_C\right). \tag{12.3.8}$$

In total, we know that

$$\max_{M \in \partial\mathcal{M}, \{\tau_i\}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes \tau_i\right) = \max_{M \in \partial\mathcal{M}} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|_C\right). \tag{12.3.9}$$

Besides, we have

$$\begin{aligned} \mathcal{E}\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|_C\right) &= \mathcal{E}\left(\sum_i p_i \sigma_i \otimes (|0\rangle\langle 0| \otimes |i\rangle\langle i|)_C\right) \\ &= \sum_i p_i \mathcal{E}[\sigma_i \otimes |0\rangle\langle 0|_C], \end{aligned} \tag{12.3.10}$$

where the equalities in the first line holds since $\{|i\rangle\langle i|\}$ and $\{|0\rangle\langle 0| \otimes |i\rangle\langle i|\}$ can be converted to each other by LOCC, the equality in the second line is from the flag condition satisfied by any entanglement measure which is monotonic under LOCC, see Theorem 2 in Ref. [277]. By putting Eq. (12.3.6), Eq. (12.3.9) and Eq. (12.3.10) together, we complete the proof. □

This Result shows that the actual calculation of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ can be reduced to the set of extremal points in $\mathcal{M}$, which has been well characterized in Ref. [663]. In the following, we will address this problem in two special cases.

The first case is that the party C is a qubit and the measurement information from the outcomes is also registered in a qubit system E [664]. For convenience, we denote by $\mathcal{N}_1$ the set of those operations, which is equivalent to the set of all entanglement breaking channels mapping qubit to qubit. The second case is that the measurement M is a dichotomic POVM [663], where C is not necessarily a qubit. We denote this set as $\mathcal{N}_2$.

Now we can present the following observation:

Result 54. *For a convex entanglement measure $\mathcal{E}$, if we replace $\mathcal{N}_C$ by $\mathcal{N}_1$ or $\mathcal{N}_2$ in the definition of $\Delta_{\mathcal{E}}$, then the value of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ can be achieved with projective measurements.*

Remark 68. Result 53 and Result 54 make the numerical calculation possible with only a few parameters as in the following examples.

Proof. From Result 53, we know that for a convex entanglement measure $\mathcal{E}$ that satisfies the monotonicity condition, the optimal value of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ can always be obtained by the extreme points of destructive measurements in the sets $\mathcal{N}_1$ and $\mathcal{N}_2$. Then it is sufficient to show that these extreme points are given by projective measurements.

First, we consider the case of $\mathcal{N}_1$. As proven in Ref. [664], any entanglement breaking channel from qubit to qubit, i.e., any channel in $\mathcal{N}_1$, can be decomposed as a convex combination of classical-quantum channels. Here recall that a channel Φ_C is called a classical-quantum channel if

$$\Phi_C(\varrho) = \sum_i \langle x_i|\varrho|x_i\rangle \otimes \tau_i, \tag{12.3.11}$$

where $\{|x_i\rangle\}$ is an orthonormal basis. By definition, the classical-quantum channel is written in the composition of projective measurements and local state preparation. That is, the extreme point in $\mathcal{N}_1$ is obtained by projective measurements.

Next, we consider the case of $\mathcal{N}_2$. It is known that a POVM $\{m_1, \ldots, m_k\}$ is extreme if m_i, m_j have disjoint supports for any $i \neq j$ [663]. In the dichotomic case, $m_1 = \mathbb{1} - m_2$, thus, m_1, m_2 can be diagonalized simultaneously. Then, there is no overlap between the supports of m_1, m_2 if and only if they are orthogonal projectors. Hence, the extremal points in $\mathcal{N}_2$ are also obtained by projective measurements. □

12.3.1 Example: three-qubit systems

Here we look at three-qubit systems and analyze $\Delta_{\mathcal{E}}(\varrho_{ABC})$ with $\mathcal{N}_1$ and $\mathcal{N}_2$. Important examples of multipartite entanglement measures that satisfy convexity and monotonicity under LOCC are the multipartite negativity [665] and multipartite squashed entanglement [280, 281]:

$$N_{ABC}(\varrho_{ABC}) = N_{AB|C} + N_{BC|A} + N_{AC|B}, \tag{12.3.12}$$

$$E_{sq}(\varrho_{ABC}) = \min_{\gamma_{ABCX}} \frac{1}{2} I(A:B:C|X). \tag{12.3.13}$$

Here, $N_{X|Y} = \left|\sum_{\lambda_i<0} \lambda_i\right|$ is the negativity for a bipatition $X|Y$ with eigenvalues λ_i of the partial transposed state ϱ^{T_Y} with respect to the subsystem Y, where $Y = A, B, C$. Also, $I(A:B:C|X) = S(AX) + S(BX) + S(CX) - S(ABCX) - 2S(X)$ is the quantum conditional mutual information, where γ_{ABCX} is any extension of ϱ_{ABC}, i.e., $\varrho_{ABC} = \mathrm{tr}_X[\gamma_{ABCX}]$, and $S(M)$ is the von Neumann entropy of system

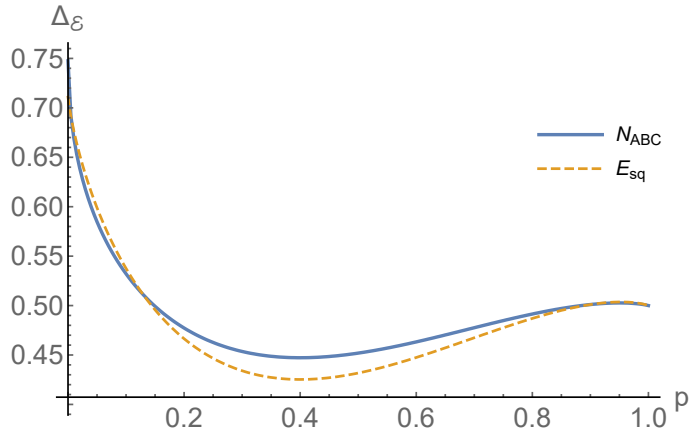

Figure 12.2: $\Delta_{\mathcal{E}}$ with N_{ABC} and E_{sq} for $|\psi(p)\rangle = \sqrt{p}\,|\mathrm{GHZ}\rangle + \sqrt{1-p}\,|\mathrm{W}\rangle$. This figure is taken from Ref. [5].

M. For a pure state ϱ_{ABC}, the quantum conditional mutual information can be simplified as $I(A:B:C|X) = S(A) + S(B) + S(C)$, which is independent of the system X.

As the first example, we consider the superposition of Greenberger-Horne-Zeilinger (GHZ) states and W states:

$$|\psi(p)\rangle = \sqrt{p}\,|\mathrm{GHZ}\rangle + \sqrt{1-p}\,|\mathrm{W}\rangle\,, \tag{12.3.14}$$

where $0 \leq p \leq 1$, $|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$, and $|\mathrm{W}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$. The numerical relation between $\Delta_{\mathcal{E}}$ and p is presented in Fig. 12.2 for $\mathcal{E} = N_{ABC}$, E_{sq}, details about the optimization method are given below. Interestingly, we find that the maximal value of $\Delta_{\mathcal{E}}(|\psi\rangle)$ is given by the W state, while the minimal value is not achieved by the GHZ state but the state at $p = 0.4$. We remark that both of $N_{ABC}(|\psi(p)\rangle)$ and $E_{sq}(|\psi(p)\rangle)$ are minimized when $p = 0.4$. However, it is an open problem to understand why this state should also have minimal entanglement change.

Moreover, let us consider a three-qutrit case and compute the tuple of $\Delta_{\mathcal{E}}$ for $\mathcal{E} = (N_{ABC}, E_{sq})$. The GHZ state $\sum_{i=0}^{2} |iii\rangle / \sqrt{3}$ has (1.667, 0.792489), while the state $(|012\rangle + |120\rangle + |201\rangle + |021\rangle + |210\rangle + |102\rangle)/\sqrt{6}$ has (1.86747, 0.971332). More details are given below.

12.3.2 Details of computation in figures

Since we consider the set of entanglement breaking channels from qubit to qubit in the examples, we only need to focus on dichromatic projective measurements $M = \{m_0, m_1\}$ and perfect encoding of the outcomes according to Result 53 and Result 54. In this case, we have

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) = \mathcal{E}[\varrho_{ABC}] - \max_{M\in\mathcal{P}} \sum_{i=0,1} p_i \mathcal{E}[\sigma_i \otimes |0\rangle\langle 0|], \tag{12.3.15}$$

where $\mathcal{P}$ is the set of all dichotomatic projective measurements on qubit C, $p_i = \mathrm{tr}(\varrho_{ABC} m_i)$, and $\sigma_i = \mathrm{tr}_C(\varrho_{ABC} m_i)/p_i$. Here, the entanglement measure $\mathcal{E}$ is taken to be either the multipartite negativity N_{ABC} or the multipartite squashed entanglement E_{sq}.

First, let us consider the case of the multipartite negativity N_{ABC}. Then we have

$$\begin{aligned} N_{ABC}(\sigma_i \otimes |0\rangle\langle 0|) &= N_{AB|C}(\sigma_i \otimes |0\rangle\langle 0|) + N_{BC|A}(\sigma_i \otimes |0\rangle\langle 0|) + N_{AC|B}(\sigma_i \otimes |0\rangle\langle 0|) \\ &= N_{B|A}(\sigma_i) + N_{A|B}(\sigma_i) \\ &= 2N_{A|B}(\sigma_i), \end{aligned} \tag{12.3.16}$$

where the second equality is from the fact that $\sigma_i^{T_A} \otimes |0\rangle\langle 0|$ has same non-zero eigenvalues as $\sigma_i^{T_A}$ as well as for the case B.

Second, let us consider the case of the multipartite squashed entanglement E_{sq}. Note that, for any 4-partite state η_{ABCX} such that $\mathrm{tr}_X(\eta_{ABCX}) = \sigma_i \otimes |0\rangle\langle 0|$, it can only be in the form $\gamma_{ABX} \otimes |0\rangle\langle 0|$, where $\mathrm{tr}_X(\gamma_{ABX}) = \sigma_i$. Thus,

$$\begin{aligned} E_{sq}(\sigma_i \otimes |0\rangle\langle 0|) &= \min_{\gamma_{ABX} \otimes |0\rangle\langle 0|} \frac{1}{2} I(A:B:C|X) \\ &= \min_{\gamma_{ABX} \otimes |0\rangle\langle 0|} \frac{1}{2} [S(AX) + S(BX) + S(CX) - S(ABCX) - 2S(X)] \\ &= \min_{\gamma_{ABX} \otimes |0\rangle\langle 0|} \frac{1}{2} [S(AX) + S(BX) + S(X) - S(ABX) - 2S(X)] \\ &= \min_{\gamma_{ABX}} \frac{1}{2} [S(AX) + S(BX) - S(ABX) - S(X)] \\ &= E_{sq}^{(2)}(\sigma_i), \end{aligned} \tag{12.3.17}$$

where in the third line we employ the additivity of the von Neumann entropy, and we denote $E_{sq}^{(2)}$ the bipartite squashed entanglement [280]. In the case that ϱ_{ABC} is a pure state, each σ_i is also a pure state. From the result of Ref. [280], we have

$$E_{sq}^{(2)}(\sigma_i) = S(A) + S(B). \tag{12.3.18}$$

Therefore, once we have parameterized the 2-dimensional projective measurement M, the numerical calculation of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ can be easily performed by brute force optimization in each example. To be more explicitly, each 2-dimensional rank-1 projective measurement M corresponds to a vector which can be parameterized as $\langle v| = (\cos x, e^{it} \sin x)$ such that $M = \{|v\rangle\langle v|, \mathbb{1} - |v\rangle\langle v|\}$. In the calculation, we have taken x in the discrete set $\{\pi k/300\}_{k=0}^{300}$ and t in the set $\{\pi j/50\}_{j=0}^{50}$. For each measurement direction defined by the pair (x,t), the poset-selected bipartite states and their entanglement can be computed directly by the definition of the entanglement measure. By choosing the maximal entanglement of the post-measurement state over all pairs (x,t), we obtain the numerical approximation of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ for $\mathcal{E}$ either to be N_{ABC} or E_{sq}.

We remark that the three-dimensional non-trivial projective measurements can also be parameterized by $M = \{|v\rangle\langle v|, \mathbb{1} - |v\rangle\langle v|\}$, where $|v\rangle$ is a three-dimensional complex vector $(\cos x_1, e^{it_1} \sin x_1 \cos x_2, e^{it_2} \sin x_1 \sin x_2)$. Note that for the sake of simplicity, we considered the case of only real parameters to obtain the result of three-qutrit states.

12.4 General bounds

12.4.1 Lower bound

In general, it may be hard to obtain the exact value of $\Delta_{\mathcal{E}}(\varrho_{ABC})$ for some entanglement measure $\mathcal{E}$. To address this situation, we now derive upper and lower bounds that can be useful for the estimation. First, we present a general lower bound.

Result 55. *For a convex entanglement measure $\mathcal{E}$, and for the set $\mathcal{N}_C$, we have*

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) \geq \min_{|x\rangle} \left\{ \mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\sigma_{|x\rangle} \otimes |0\rangle\langle 0|] \right\}, \tag{12.4.1}$$

where $|x\rangle$ is a measurement direction on the party C and $\sigma_{|x\rangle} \propto \langle x|\varrho_{ABC}|x\rangle$ is a normalized state.

Remark 69. This lower bound can be used to characterize the complete entanglement loss, as we will see later in Sec. 12.6.

Proof. For a given entanglement breaking channel Φ_C, it can be equivalently characterized [662] by a POVM with $M = \{q_i|x_i\rangle\langle x_i|\}$ and a preparation $\{|\psi_i\rangle\langle\psi_i|\}$. That is,

$$\Phi_C(\varrho_{ABC}) = \sum_i q_i \langle x_i|\varrho_{ABC}|x_i\rangle \otimes |\psi_i\rangle\langle\psi_i| = \sum_i q_i p_i \sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|, \tag{12.4.2}$$

where $p_i = \mathrm{tr}(\langle x_i|\varrho_{ABC}|x_i\rangle)$, $\sigma_{|x_i\rangle}$ is the normalized state of $\langle x_i|\varrho_{ABC}|x_i\rangle$, and $\sum_i q_i p_i = 1$.

For any convex entanglement measure $\mathcal{E}$, we then have

$$\begin{aligned} \mathcal{E}[\Phi_C(\varrho_{ABC})] &\leq \sum_i q_i p_i \mathcal{E}[\sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|] \\ &\leq \max_i \mathcal{E}[\sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|] \\ &\leq \max_{|x\rangle} \mathcal{E}[\sigma_{|x\rangle} \otimes |0\rangle\langle 0|], \end{aligned} \tag{12.4.3}$$

where in the last line we apply local unitary operations on the party C to rotate the states to $|0\rangle$ and maximize over a more general range of measurement directions. □

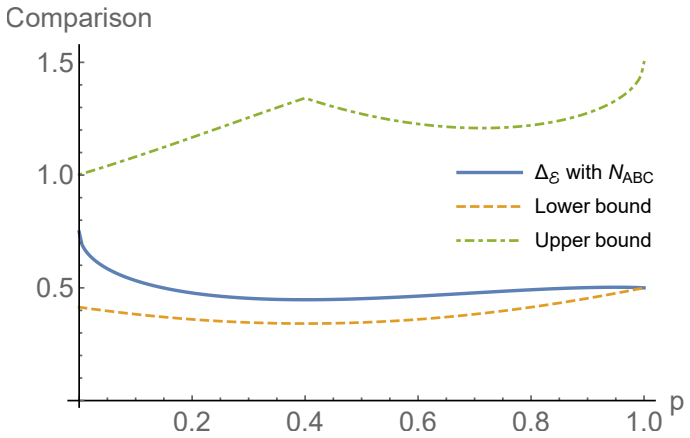

Figure 12.3: Comparison between $\Delta_{\mathcal{E}}$ with N_{ABC} and its lower and upper bounds for the state $|\psi(p)\rangle = \sqrt{p}\,|\mathrm{GHZ}\rangle + \sqrt{1-p}\,|\mathrm{W}\rangle$. This figure is taken from Ref. [5].

Remark 70. In principle, the optimization can be done similarly as in Sec. 12.3.2. As for the application of Result 55 in Result 59, we only need to show that $\sigma_{|x\rangle}$ is separable for each $|x\rangle$, which can be checked by the PPT condition in the case that A and B are two-dimensional subsystems with symbolic calculations. For this purpose, we do not need to specify the values of parameters in $|x\rangle$.

Furthermore, suppose that we remove all the classical information of the measurement outcomes, that is, we encode all the measurement outcomes into the same state $|0\rangle$. Then we find an upper bound:

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) \leq \tilde{\Delta}_{\mathcal{E}}(\varrho_{ABC}), \tag{12.4.4}$$

for any convex entanglement measure $\mathcal{E}$, where

$$\tilde{\Delta}_{\mathcal{E}}(\varrho_{ABC}) = \mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\varrho_{AB} \otimes |0\rangle\langle 0|], \tag{12.4.5}$$

with $\varrho_{AB} = \mathrm{tr}_C(\varrho_{ABC})$. We remark that $\tilde{\Delta}_{\mathcal{E}}(\varrho_{ABC})$ is the maximal entanglement change, since we can always map any encoding into the state $|0\rangle\langle 0|$ with a local operation on the system C.

Let us compare $\Delta_{\mathcal{E}}$ with its lower and upper bounds using the tripartite negativity N_{ABC}. Figs. 12.3 and 12.4 illustrate the cases of the pure three-qubit state $|\psi(p)\rangle$ in Eq. (12.3.14) and the mixed three-qubit state $\varrho(q) = q\varrho_{\mathrm{GHZ}} + (1-q)\varrho_{\mathrm{W}}$, where $\varrho_{\mathrm{GHZ}} = |\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|$ and $\varrho_{\mathrm{W}} = |\mathrm{W}\rangle\langle\mathrm{W}|$. We find that the lower bound is relatively close to $\Delta_{\mathcal{E}}$, especially if the state approximates the GHZ state. The gap between $\Delta_{\mathcal{E}}$ and $\tilde{\Delta}_{\mathcal{E}}$ shows that the post-measurement information is more relevant for the GHZ state than for the W state.

12.4.2 Quantum discord

Next, let us connect entanglement change to quantum discord. For that, we consider the multipartite relative entropy of entanglement, which is the sum of

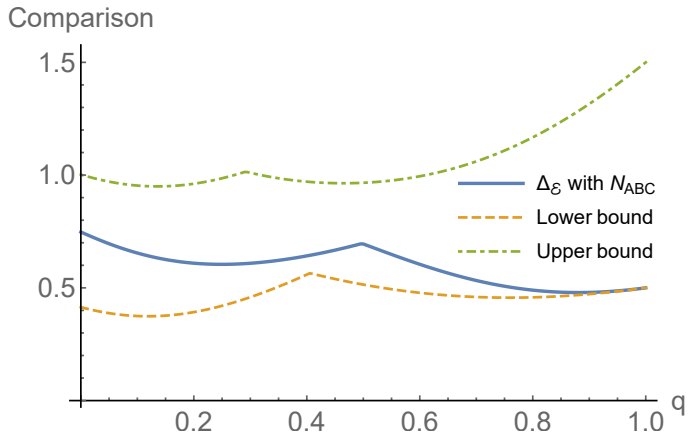

Figure 12.4: Comparison between $\Delta_{\mathcal{E}}$ with N_{ABC} and its lower and upper bounds presented for the state $\varrho(q) = q\varrho_{\mathrm{GHZ}} + (1-q)\varrho_{\mathrm{W}}$. This figure is taken from Ref. [5].

the relative entropies of entanglement [666] for all bipartitions, i.e.,

$$R_{ABC}(\varrho_{ABC}) = R_{AB|C} + R_{BC|A} + R_{AC|B}, \tag{12.4.6}$$

where $R_{X|Y} = \min_{\sigma\in\mathrm{SEP}} S(\varrho_{XY}||\sigma)$ is the relative entropy of entanglement for a bipatition $X|Y$, $S(\varrho||\sigma) = \mathrm{tr}[\varrho\,(\log\varrho - \log\sigma)]$ is the von Neumann relative entropy and SEP is the set of bipartite separable states.

Similarly, the amount of quantum discord [667] can be also measured by the relative entropy: $D_{XY}(\varrho_{XY}) = \min_{\varrho'\in\Lambda} S(\varrho_{XY}||\varrho')$, where Λ is the set of quantum-classical states $\varrho' = \sum_i p_i\sigma_i \otimes |i\rangle\langle i|$ with orthonormal basis $\{|i\rangle\}$. Now we can formulate the following two Results:

Result 56. *For the entanglement measure $\mathcal{E}$ being the tripartite relative entropy of entanglement R_{ABC}, we have*

$$R_{AB|C}(\varrho_{ABC}) \leq \Delta_{\mathcal{E}}(\varrho_{ABC}) \leq 3D_{AB|C}(\varrho_{ABC}). \tag{12.4.7}$$

Proof. We begin by noting that Lemma 1 in Ref. [660]: for a given tripartite state ϱ_{ABC}, it holds that

$$R_{BC|A}(\varrho_{ABC}) \leq D_{AB|C}(\varrho_{ABC}) + R_{BC|A}[\Phi_C(\varrho_{ABC})], \tag{12.4.8}$$

where $\Phi_C(\varrho_{ABC}) = \sum_i p_i\sigma_i^{AB} \otimes |i\rangle\langle i|^C$ where $\tau_i = |i\rangle\langle i|^C$. Exchanging A and B, we similarly have

$$R_{AC|B}(\varrho_{ABC}) \leq D_{AB|C}(\varrho_{ABC}) + R_{AC|B}[\Phi_C(\varrho_{ABC})]. \tag{12.4.9}$$

Summarizing both inequalities leads to

$$R_{BC|A}(\varrho_{ABC}) + R_{AC|B}(\varrho_{ABC}) \leq 2D_{AB|C}(\varrho_{ABC}) + R_{ABC}[\Phi_C(\varrho_{ABC})], \tag{12.4.10}$$

where we use the fact that $R_{AB|C}[\Phi_C(\varrho_{ABC})] = 0$ since $\Phi_C(\varrho_{ABC})$ is separable with respect to $AB|C$. Rewriting this left hand side as $R_{ABC}(\varrho_{ABC}) - R_{AB|C}(\varrho_{ABC})$, we have

$$R_{ABC}(\varrho_{ABC}) - R_{ABC}[\Phi_C(\varrho_{ABC})] \leq 2D_{AB|C}(\varrho_{ABC}) + R_{AB|C}(\varrho_{ABC}). \tag{12.4.11}$$

By definition, $\Delta_{\mathcal{E}}(\varrho_{ABC})$ is always no more than this left hand side, since Φ_C is just a special entanglement-breaking channel. Then we obtain

$$\Delta_{\mathcal{E}}(\varrho_{ABC}) \leq 2D_{AB|C}(\varrho_{ABC}) + R_{AB|C}(\varrho_{ABC}). \tag{12.4.12}$$

Finally, since $R_{AB|C}(\varrho_{ABC}) \leq D_{AB|C}(\varrho_{ABC})$, we find the upper bound.

Concerning the lower bound, we have

$$\begin{aligned}\Delta_{\mathcal{E}}(\varrho_{ABC}) &= \min_{\Phi_C \in \mathcal{N}_C} \{R_{ABC}(\varrho_{ABC}) - R_{ABC}[\Phi_C(\varrho_{ABC})]\} \\ &\geq R_{AB|C}(\varrho_{ABC}) + \min_{\Phi_C \in \mathcal{N}_C} \left\{R_{BC|A}(\varrho_{ABC}) - R_{BC|A}[\Phi_C(\varrho_{ABC})]\right\} \\ &+ \min_{\Phi_C \in \mathcal{N}_C} \left\{R_{AC|B}(\varrho_{ABC}) - R_{AC|B}[\Phi_C(\varrho_{ABC})]\right\},\end{aligned} \tag{12.4.13}$$

where we again use that $R_{AB|C}[\Phi_C(\varrho_{ABC})] = 0$. Since the relative entropy of entanglement satisfies the monotonicity condition, we have that $R_{BC|A}(\varrho_{ABC}) - R_{BC|A}[\Phi_C(\varrho_{ABC})] \geq 0$ and $R_{AC|B}(\varrho_{ABC}) - R_{AC|B}[\Phi_C(\varrho_{ABC})] \geq 0$. Then we arrive at the lower bound. □

Result 57. *More generally, if $D_{AB|C}(\varrho_{ABC}) = 0$, then we have $\Delta_{\mathcal{E}}(\varrho_{ABC}) = 0$ for any entanglement measure $\mathcal{E}$.*

Proof. We note that $D_{AB|C}(\varrho_{ABC}) = 0$ if and only if there exists an entanglement-breaking channel Φ_C such that $\Phi_C(\varrho_{ABC}) = \varrho_{ABC}$ (see Proposition 21 in Ref. [668] for more details). By definition,

$$\begin{aligned}\Delta_{\mathcal{E}}(\varrho_{ABC}) &= \min_{\Phi'_C \in \mathcal{N}_C} \left\{\mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\Phi'_C(\varrho_{ABC})]\right\}, \\ &\leq \mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\Phi_C(\varrho_{ABC})] \\ &= \mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\varrho_{ABC}] \\ &= 0.\end{aligned} \tag{12.4.14}$$

Since $\Delta_{\mathcal{E}}(\varrho_{ABC})$ is nonnegative for any entanglement measure $\mathcal{E}$ which is monotonic under LOCC, this eventually implies that $\Delta_{\mathcal{E}}(\varrho_{ABC}) = 0$ for any entanglement measure $\mathcal{E}$ which is assumed to be monotonic under LOCC. □

From Result 57, the condition $D_{AB|C}(\varrho_{ABC}) = 0$ is a sufficient condition for $\Delta_{\mathcal{E}}(\varrho_{ABC}) = 0$ for any measure $\mathcal{E}$. On the other hand, this is not a necessary condition. For instance, if the initial state ϱ_{ABC} is fully separable, clearly $\Delta_{\mathcal{E}}(\varrho_{ABC}) = 0$, but this does not mean $D_{AB|C}(\varrho_{ABC}) = 0$. From the conceptional perspective, quantum discord is the difference of quantum correlation before and after a projective measurement, whereas $\Delta_{\mathcal{E}}(\varrho_{ABC})$ quantifies the difference of entanglement, which is only one sort of quantum correlations.

12.5 Lockability

Previous works [282, 653, 654] have studied a similar issue under the name of lockability of entanglement measures. There, one asks for the quantitative change of entanglement by the loss of one particle, (e.g., one qubit) *within* one party. For example, in the bipartite scenario, one considers the situation where Alice and Bob have both five qubits and then one asks how the entanglement changes if Alice loses one of her qubits. If the entanglement change can be arbitrarily large, the entanglement measure is called lockable. For instance, all convex entanglement measures are known to be lockable, while the relative entropy of entanglement is not lockable, see Ref. [282].

The lockable entanglement is related to our consideration in the following sense. For a given tripartite state ϱ_{ABC}, if we choose the convex entanglement measure $\mathcal{E}$ to only measure the entanglement between the bipartition $A|BC$ (or $AC|B$), then $\tilde{\Delta}_{\mathcal{E}}$ defined in Eq. (12.4.5) is the quantity considered in lockable entanglement. More precisely, for any convex entanglement measure $\mathcal{E}$ for the bipartition $A|BC$, we have

$$\tilde{\Delta}_{\mathcal{E}}(\varrho_{ABC}) = \mathcal{E}[\varrho_{ABC}] - \mathcal{E}[\varrho_{AB}], \tag{12.5.1}$$

where we used that $\mathcal{E}[\varrho_{AB} \otimes |0\rangle\langle 0|] = \mathcal{E}[\varrho_{AB}]$, see Theorem 2 in Ref. [277].

In order to understand the difference between the behavior of entanglement under classicalization and the lockability problem, one has to analyze the role of the information coming from the measurement results. We know already from Fig. 12.3 and 12.4 that this information makes some difference for the entanglement change. In the following, we will show that this difference can be arbitrarily large.

12.5.1 Flower state

First, let us consider the so-called flower state on $d \otimes d \otimes 2$-dimensional systems [653]:

$$\omega_{ABC} = \frac{2}{d(d+1)} P_{AB}^{(+)} \otimes \frac{d+1}{2d} |0\rangle\langle 0|_C + \frac{2}{d(d-1)} P_{AB}^{(-)} \otimes \frac{d-1}{2d} |1\rangle\langle 1|_C, \tag{12.5.2}$$

where $P_{AB}^{(\pm)}$ are the projections onto the symmetric and anti-symmetric subspaces, that is $P_{AB}^{(\pm)} = (\mathbb{1}_{AB} \pm \mathbb{S}_{AB})/2$ with the SWAP operator $\mathbb{S}_{AB}$, acting as $\mathbb{S}_{AB} |v_A\rangle \otimes |v_B\rangle = |v_B\rangle \otimes |v_A\rangle$.

Notice that, the quantum discord of ω_{ABC} for the bipartition $AB|C$ is 0, i.e., $D_{AB|C}(\omega_{ABC}) = 0$. From Result 57, we conclude that $\Delta_{\mathcal{E}}(\omega_{ABC}) = 0$ for any entanglement measure $\mathcal{E}$. However, we have $\tilde{\Delta}_{\mathcal{E}}(\omega_{ABC}) = \mathcal{E}(\omega_{ABC}) > 0$, because $\mathrm{tr}_C(\omega_{ABC}) \otimes |0\rangle\langle 0|$ is fully separable. In fact, if the entanglement measure $\mathcal{E}$ is taken as the squashed entanglement, then $\mathcal{E}(\omega_{ABC})$ can be arbitrarily large [653]. This directly implies that the difference $\tilde{\Delta}_{\mathcal{E}} - \Delta_{\mathcal{E}}$ can be arbitrarily large by choosing d properly. Hence, although the information from the measurement at the

flower state is only one bit, a large amount of entanglement can be saved by collecting it.

12.5.2 Many pairs of Bell states

On the other hand, we will see that the entanglement change $\Delta_{\mathcal{E}}$ can also be arbitrarily large even if only one qubit has become classical. As example, let us consider a pure state made of n pairs of Bell state $|\Psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. We label the i-th pair of particles with a_i, b_i. Suppose that the party A owns the particles $\{a_i\}_{i=1}^n$, the party B owns the particles $\{b_i\}_{i=1}^{n-1}$, and the party C owns the particle b_n. We denote this state as $\beta_{ABC} = |\Psi^+\rangle\langle\Psi^+|^{\otimes n}$. Now we can present the following observation:

Result 58. *For the entanglement measure $\mathcal{E}$ to be the tripartite negativity N_{ABC}, we have*

$$\Delta_{\mathcal{E}}(\beta_{ABC}) = 2^{n-2} + 1/2. \tag{12.5.3}$$

Thus, $\Delta_{\mathcal{E}}(\beta_{ABC})$ can be arbitrary large by choosing n properly.

Proof. To prove this, we first show that for a $d \times d$-dimensional bipartite state, its negativity is no more than $(d-1)/2$. Since the negativity is a convex function, we only need to prove it for pure states. Let us write a pure state $|\psi\rangle$ as

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |a_i b_i\rangle \,,\ \sum_i \lambda_i^2 = 1,\ \lambda_i \geq 0. \tag{12.5.4}$$

Then direct calculation yields that

$$N(|\psi\rangle) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j \leq \frac{d-1}{2} \sum_{i=1}^{d} \lambda_i^2 = \frac{d-1}{2}. \tag{12.5.5}$$

Here the maximal value $(d-1)/2$ can be saturated by the maximally entangled state $|\Psi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.

Next, let us recall the n-copy of Bell state $\beta_{ABC} = |\Psi^+\rangle\langle\Psi^+|^{\otimes n}$. We remark that this n-copy state can be represented by the maximally entangled state in $(2^n \times 2^n)$-dimensional systems $|\Psi_{2^n}^+\rangle$. This leads to

$$N_{BC|A}(\beta_{ABC}) = (2^n - 1)/2. \tag{12.5.6}$$

Suppose that an entanglement breaking channel Φ_C acts on the n-th particle of the last party b_n, equivalently, on the party C. Since all entanglement breaking channels can be decomposed into measure and prepare operations, we again write the measure process for Φ_C as the form of the POVM with $M = \{q_i |x_i\rangle\langle x_i|\}$ and the preparation process as $\{|\psi_i\rangle\langle\psi_i|\}$, i.e.,

$$\Phi_C(\beta_{ABC}) = \sum_i q_i p_i \sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|, \tag{12.5.7}$$

where $p_i = \mathrm{tr}(\langle x_i|\beta_{ABC}|x_i\rangle)$, $\sigma_{|x_i\rangle}$ is the normalized pure state of $\langle x_i|\beta_{ABC}|x_i\rangle$, and $\sum_i q_i p_i = 1$. Then we have

$$\begin{aligned} N_{BC|A}[\Phi_C(\beta_{ABC})] &= N_{BC|A}\left(\sum_i q_i p_i \sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|\right) \\ &\leq \sum_i q_i p_i N_{BC|A}\left(\sigma_{|x_i\rangle} \otimes |\psi_i\rangle\langle\psi_i|\right) \\ &= \sum_i q_i p_i N_{BC|A}\left(\sigma_{|x_i\rangle} \otimes |0\rangle\langle 0|\right) \\ &= \sum_i q_i p_i N_{AB}(\sigma_{|x_i\rangle}) \\ &\leq \sum_i q_i p_i (2^{n-1}-1)/2 \\ &= (2^{n-1}-1)/2, \end{aligned} \tag{12.5.8}$$

where in the second line we employ the convexity of negativity. In the third line we apply local untary operations on the party C to rotate the states $|\psi_i\rangle$'s to $|0\rangle$. In the fourth line, we use fact that negativity is invariant under local unitaries and adding local ancillas, see [277]. In the fifth line, we apply the upper bound given in Eq. (12.5.5).

On the other hand, we obtain

$$\begin{aligned} N_{BC|A}[\Phi_C(\beta_{ABC})] &\geq N_{BC|A}[\mathrm{tr}_C(\Phi_C(\beta_{ABC})) \otimes |0\rangle\langle 0|_C] \\ &= N_{B|A}[\mathrm{tr}_C(\beta_{ABC})] \\ &= N_{B|A}[(|\Psi^+\rangle\langle\Psi^+|_{AB})^{\otimes(n-1)} \otimes \mathrm{tr}_C(|\Psi^+\rangle\langle\Psi^+|_{AC})] \\ &= N_{B|A}[(|\Psi^+\rangle\langle\Psi^+|_{AB})^{\otimes(n-1)}] \\ &= (2^{n-1}-1)/2. \end{aligned} \tag{12.5.9}$$

In the first line we use the LOCC monotonicity, and in the second line we make use of the fact that $\mathrm{tr}_C \circ \Phi_C = \mathrm{tr}_C$. In the fourth line, we use fact that negativity is invariant under adding local ancillas, see [277].

Thus, independently of the entanglement breaking channel Φ_C, we show

$$N_{BC|A}[\Phi_C(\beta_{ABC})] = (2^{n-1}-1)/2. \tag{12.5.10}$$

This result directly leads to

$$N_{BC|A}(\beta_{ABC}) - N_{BC|A}\left[\Phi_C(\beta_{ABC})\right] = 2^{n-2}. \tag{12.5.11}$$

Also, since negativity is invariant under adding local ancillas, we have

$$N_{B|CA}(\beta_{ABC}) = N_{B|CA}\left[\Phi_C(\beta_{ABC})\right] = N_{B|A}\left[(|\Psi^+\rangle\langle\Psi^+|_{AB})^{\otimes(n-1)}\right] = (2^{n-1}-1)/2, \tag{12.5.12}$$

which implies

$$N_{B|CA}(\beta_{ABC}) - N_{B|CA}\left[\Phi_C(\beta_{ABC})\right] = 0. \tag{12.5.13}$$

Similarly, we have

$$N_{AB|C}(\beta_{ABC}) = N_{A|C}\left[|\Psi^+\rangle\langle\Psi^+|_{AC}\right] = 1/2. \tag{12.5.14}$$

The fact that Φ_C is an entanglement-breaking channel implies that

$$N_{AB|C}\left[\Phi_C(\beta_{ABC})\right] = 0. \tag{12.5.15}$$

Consequently, we have

$$N_{AB|C}(\beta_{ABC}) - N_{AB|C}\left[\Phi_C(\beta_{ABC})\right] = 1/2. \tag{12.5.16}$$

By definition of $\Delta_{\mathcal{E}}(\beta_{ABC})$ with N_{ABC} using Eqs. (12.5.11, 12.5.13, 12.5.16), we complete the proof:

$$\Delta_{\mathcal{E}}(\beta_{ABC}) = 2^{n-2} + 1/2. \tag{12.5.17}$$

We have one remark. From Eq. (12.5.6), Eq. (12.5.12) and Eq. (12.5.14), we know that the original tripartite negativity is

$$N_{ABC}(\beta_{ABC}) = 2^{n-1} + 2^{n-2} - 1/2, \tag{12.5.18}$$

which is strictly larger than $\Delta_{\mathcal{E}}(\beta_{ABC})$ whenever $n \geq 2$. Furthermore,

$$\frac{N_{ABC}(\beta_{ABC})}{\Delta_{\mathcal{E}}(\beta_{ABC})} \to 2, \quad n \gg 2. \tag{12.5.19}$$

□

Inspired by those two examples, an interesting question arises whether there exist entanglement measures $\mathcal{E}$ and states ϱ_{ABC} such that both $\Delta_{\mathcal{E}}(\varrho_{ABC})$ and $\tilde{\Delta}_{\mathcal{E}}(\varrho_{ABC}) - \Delta_{\mathcal{E}}(\varrho_{ABC})$ can be arbitrarily large in the sense that they are not limited by the size of C, even if C is only a qubit. We leave this question for further research.

12.6 Complete entanglement loss under classicalization

By definition, $\Delta_{\mathcal{E}}(\varrho_{ABC}) \leq \mathcal{E}[\varrho_{ABC}]$ always holds. We are now concerned about the case where this inequality is saturated, i.e., $\Delta_{\mathcal{E}}(\varrho_{ABC}) = \mathcal{E}[\varrho_{ABC}]$, or equivalently, $\max_{\Phi_C \in \mathcal{N}_C} \mathcal{E}[\Phi_C(\varrho_{ABC})] = 0$.

First of all, Result 55 implies a sufficient condition for complete entanglement loss under classicalization, which can be formulated as follows.

Result 59. *If, after a projective measurement in any direction $|x\rangle$ on C, the post-measurement state $\sigma_{|x\rangle} \propto \langle x|\varrho_{ABC}|x\rangle$ is always separable, then the entanglement is completely lost under classicalization.*

Clearly, Result 59 is stronger than the condition that the reduced state ϱ_{AB} is separable. For instance, let us consider the GHZ state. Its reduced state $\mathrm{tr}_C[\varrho_{\mathrm{GHZ}}]$ is separable, but its post-measurement state $\sigma_{|x\rangle}$ can be entangled if measurement bases are $\{|+\rangle, |-\rangle\}$.

The existence of genuine multipartite entangled states which satisfy Result 59, however, has already been reported in Ref. [587]. We will propose observations using Result 59 and provide more examples.

12.6.1 Results on complete entanglement loss under classicalization

In this section, we propose two results for the entangled states satisfying Result 59. A similar observation has been made for pure states in Ref. [651].

Result 60. *Suppose that a tripartite state ϱ_{ABC} satisfies Result 59. If ϱ_{ABC} is entangled for the bipartitions $A|BC$ and $B|AC$, then the reduced state $\varrho_{AB} = \mathrm{tr}_C(\varrho_{ABC})$ should have rank more than 2.*

Proof. First we denote that $p_x = \mathrm{tr}[\langle x|\varrho_{ABC}|x\rangle]$ and $\sigma_{|x\rangle} = \langle x|\varrho_{ABC}|x\rangle / p_x$. Let us begin by recalling that any tripartite quantum state can be written as

$$\varrho_{ABC} = \sum_{i,j} M_{ij} \otimes |i\rangle\langle j|, \tag{12.6.1}$$

where $M_{ij} = \mathrm{tr}_C[\varrho_{ABC}(\mathbb{1}_{AB} \otimes |j\rangle\langle i|)]$. For $i = j$, we have that $M_{ii} = p_i \sigma_{|i\rangle}$. For $i \neq j$, M_{ij} can be written as linear combinations of $p_x\sigma_{|x\rangle}$ for some $|x\rangle$, since any $|j\rangle\langle i|$ can be decomposed using some projectors $|x\rangle\langle x|$. The more explicit form will be given below.

In the following, we will show the contraposition of the observation, that is, if ϱ_{ABC} satisfies Result 59 and ϱ_{AB} has rank no more than 2, then ϱ_{ABC} is either separable for the bipartition $A|BC$ or separable for the bipartition $B|AC$. Since $\varrho_{AB} = \sum_i p_i \sigma_{|i\rangle}$ where $\{|i\rangle\}$ is the computational orthonormal basis, and $\sigma_{|i\rangle}$ is separable for any $|i\rangle$ according to Result 59, then ϱ_{AB} is also separable. If ϱ_{AB} has rank 1, it is easy to see that ϱ_{ABC} is a pure product state. Further, let us consider the case that the separable state ϱ_{AB} has exactly rank 2. Up to local unitary, we can assume the following decomposition:

$$\varrho_{AB} = \alpha(\lambda\,|00\rangle\langle 00| + (1-\lambda)\,|ab\rangle\langle ab|) + (1-\alpha)\sum_i \lambda_i |a_i b_i\rangle\langle a_i b_i|, \tag{12.6.2}$$

where $|ab\rangle \neq |00\rangle$, $\alpha, \lambda, \lambda_i \in [0,1]$.

Denote $|\psi_1\rangle, |\psi_2\rangle$ the eigenstates of ϱ_{AB} with non-zero eigenvalues. Then $|00\rangle$, $|ab\rangle$, $|a_i b_i\rangle$ should be superpositions of $|\psi_1\rangle, |\psi_2\rangle$. Since $|ab\rangle \neq |00\rangle$, $|\psi_1\rangle, |\psi_2\rangle$ can also be written as superpositions of $|00\rangle, |ab\rangle$. Consequently, any $|a_i b_i\rangle$ can be written as superpositions of $|00\rangle, |ab\rangle$.

In the case that $|a\rangle = |0\rangle$, we have $|a_i\rangle = |0\rangle$, which implies that

$$\varrho_A = \mathrm{tr}_{BC}(\varrho_{ABC}) = \mathrm{tr}_B(\varrho_{AB}) = |0\rangle\langle 0|. \tag{12.6.3}$$

Hence, $\varrho_{ABC} = |0\rangle\langle 0| \otimes \varrho_{BC}$, which contradicts the assumption that ϱ_{ABC} is entangled for the bipartition $A|BC$. Thus, $|a\rangle \neq |0\rangle$ should hold. Similarly, we have $|b\rangle \neq |0\rangle$.

Since $|a\rangle \neq |0\rangle$, $|b\rangle \neq |0\rangle$, then any non-trivial superposition of them is entangled. This leads to that $|a_i b_i\rangle$ should either be $|00\rangle$ or $|ab\rangle$ up to a phase.

Since the range of $\sigma_{|x\rangle}$ belongs to the range of ϱ_{AB} and $\sigma_{|x\rangle}$ is separable, we have

$$\sigma_{|x\rangle} = \lambda_x |00\rangle\langle 00| + (1-\lambda_x) |ab\rangle\langle ab|, \tag{12.6.4}$$

where $\sum_x p_x \lambda_x = \lambda$. Since M_{ij} is a combination of $\sigma_{|x\rangle}$, M_{ij} can be written as

$$M_{ij} = X_{ij} |00\rangle\langle 00| + Y_{ij} |ab\rangle\langle ab|, \tag{12.6.5}$$

where the coefficients X_{ij} and Y_{ij} are given by combinations of $p_x \lambda_x$ for some x. Accordingly, we can write

$$\varrho_{ABC} = |00\rangle\langle 00| \otimes \tau_x + |ab\rangle\langle ab| \otimes \tau_y, \tag{12.6.6}$$

where $\tau_x = \sum_{i,j} X_{ij} |i\rangle\langle j|$ and $\tau_y = \sum_{i,j} Y_{ij} |i\rangle\langle j|$.

To show that ϱ_{ABC} is fully separable, it is sufficient to prove that the matrices τ_x and τ_y are positive semidefinite. For that, we note that since $|ab\rangle \neq |00\rangle$, there exists a bipartite pure state $|\alpha\beta\rangle$ such that $\langle ab|\alpha\beta\rangle = 0$ and $\langle 00|\alpha\beta\rangle \neq 0$. Then it holds that

$$\langle \alpha\beta\gamma|\varrho_{ABC}|\alpha\beta\gamma\rangle = |\langle \alpha\beta|00\rangle|^2 \langle\gamma|\tau_x|\gamma\rangle \geq 0, \tag{12.6.7}$$

for any $|\gamma\rangle$. This implies that $\langle\gamma|\tau_x|\gamma\rangle \geq 0$, that is, τ_x is positive semidefinite. Similarly, we can show that τ_y is positive semidefinite. Hence, we conclude that ϱ_{ABC} is fully separable, which contradicts the assumption. □

In the case that the party C is not entangled with A and B, we have a similar requirement of the global state as in the following observation.

Result 61. *Suppose that a tripartite state ϱ_{ABC} satisfies Result 59. If ϱ_{ABC} is entangled for the bipartitions $A|BC$ and $B|AC$ separable for $AB|C$, then it should have rank more than* 2.

Proof. Here we prove the statement by contradiction. Let us assume ϱ_{ABC} satisfies Result 59 and has rank no more than 2. Since ϱ_{ABC} is separable for the bipartition $AB|C$, we have the decomposition

$$\varrho_{ABC} = \sum_i p_i |\psi_i\phi_i\rangle\langle\psi_i\phi_i|, \tag{12.6.8}$$

where $|\psi_i\rangle, |\phi_i\rangle$ are states for parties A, B and party C, respectively.

By assumption, the dimension of the space spanned by $\{|\psi_i\phi_i\rangle\}$ is no more than 2, this leads to that the dimension of the space spanned by $\{|\psi_i\rangle\}$ is no more than 2. Thus, $\varrho_{AB} = \mathrm{tr}_C(\varrho_{ABC}) = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ has rank no more than 2. By applying Result 60, we finish the proof. □

We have two remarks. First, one can indeed find tripartite entangled states satisfying Result 59 and separable for the bipartition $AB|C$. Especially, there exist tripartite entangled states which are separable for any bipartition [137, 267], which satisfy Result 59 automatically. We collect more such examples in Sec. 12.6.2. Second, Results 60, 61 may provide insight into a type of quantum marginal problem: whether a global state can be separable or entangled if its marginal systems are subjected to separability conditions and rank constraints.

12.6.2 Examples for three-qubit states

Here, we discuss three-qubit entangled states that satisfy Result 59 for the complete entanglement change. In this Section, we will first propose a nontrivial three-qubit state that is entangled $A|BC$ and $AC|B$ but separable for $AB|C$. Next, we will connect the complete entanglement change with bound entanglement.

Complete entanglement change with separability for $AB|C$

To find a nontrivial three-qubit entangled state that satisfies Result 59, we employ the method of entanglement witnesses: For a Hermitian operator W, it is called an entanglement witness if $\mathrm{tr}(W\varrho_s) \geq 0$ for all separable states ϱ_s, and $\mathrm{tr}(W\varrho_e) < 0$ for some entangled states ϱ_e. The latter allows us to detect entanglement. In particular, we adopt the entanglement witness that can have the negative eigenvalues of its partial transpose (NPT) state. This witness is described as follows: Suppose that a state ϱ_e is NPT. Then one can find a negative eigenvalue $\lambda < 0$ of $\varrho_e^{T_A}$ and the corresponding eigenvector $|\phi_C\rangle$. Hence the operator $|\phi_C\rangle\langle\phi_C|^{T_A}$ can be an witness to detect the entangled state ϱ_e.

In practice, entanglement witnesses can be implemented by semi-definite programming (SDP). For our purpose, we use the following conditions that are compatible with the SDP method. First, to impose the separability condition for the bipartition $AB|C$, we apply the fact that if a $2 \otimes N$ state ϱ_{XY} obeys $\varrho_{XY} = \varrho_{XY}^{T_X}$, then it is separable, see Theorem 2 in Ref. [669]. That is, we require that $\varrho_{ABC} = \varrho_{ABC}^{T_C}$. Second, for the separability condition of the two-qubit post-measurement state $\sigma_{|x\rangle}$, we employ the positive partial transpose (PPT) criterion, which is necessary and sufficient for two-qubit separability. Third, for the sake of simplicity, we suppose that the state ϱ_{ABC} is invariant under exchange between A and B using SWAP $\mathbb{S}$ operator $\mathbb{S}\,|a\rangle\,|b\rangle = |b\rangle\,|a\rangle$.

Since the set of NPT states is not convex, we use the see-saw method with entanglement witnesses. This is a numerical iteration technique for non-convex optimization, which allows us to find states with the (local) minimal value as a solution. From the numerical solution, we can find an analytical form of the state and verify that it satisfies Result 59 for any measurement direction. Our

finding is the following entangled state:

$$\tilde{\varrho} = \frac{1}{8}\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{12.6.9}$$

This state has the following properties. First, the matrix rank of $\tilde{\varrho}$ is 4. Second, one can show that the state $\sigma_{|x\rangle}$ with $|x\rangle = (\cos t, e^{ia}\sin t)$ is PPT and therefore separable for any t, a. Third, the minimum eigenvalue of $\tilde{\varrho}^{T_A}$ is equal to $-1/8$. Fourth, the party C is not entangled with the other two parties. Nevertheless, the discord $D_{AB|C}(\tilde{\varrho}) > 0$, which is necessary for complete entanglement change according to Result 57.

Complete entanglement change and bound entanglement

We have found the existence of state $\tilde{\varrho}$ that is entangled states for $A|BC$ and $AC|B$ but separable for $AB|C$ that can achieve the complete entanglement change. Now we are also interested in the case where the separability for $AB|C$ is replaced by bound entanglement. Such a state is already known as the $4 \otimes 2$ bound entangled state [239], denoted by ϱ_{HDK} in Eq. (1.2.96). Here the parties AB are in 4-dimensional systems and the party C is 2-dimensional systems. We remark that this state satisfies Result 59. Since this state is NPT entangled for $A|BC$ and $AC|B$ but PPT entangled for $AB|C$, we cannot apply Result 61. On the other hand, its reduced state ϱ_{AB} has rank 4, and therefore, it complies with Result 60.

To proceed further, we now present the following:

Result 62. *If a tripartite state ϱ_{ABC} is separable either for the bipartition $A|BC$ or the bipartition $B|AC$, then ϱ_{ABC} satisfies Result 59.*

Proof. If ϱ_{ABC} is separable either for $A|BC$ or $B|AC$, then the normalized state of $\langle x|\,\varrho_{ABC}\,|x\rangle$ is separable for any measurement direction $|x\rangle$ on C. Thus, Result 55 implies that the entanglement change must be complete. □

In the following, we collect entangled states for complete entanglement change which are even separable for any bipartition: $\varrho_{\text{UPB}}, \varrho_{\text{ADMA}}, \varrho_{AK}, \varrho_{PH}$ given in Sec. 1.2. Since their matrix ranks are, respectively, given by $\text{Rank}(\varrho_{\text{UPB}}) = 4$, $\text{Rank}(\varrho_{\text{ADMA}}) = 7$, $\text{Rank}(\varrho_{\text{AK}}) = 8$, $\text{Rank}(\varrho_{\text{PH}}) = 5$, this follows Result 61.

12.7 Discussions

This Chapter studied the change of multiparticle entanglement under the classicalization of one particle. Clearly, the results usually depend on the choice of the

entanglement quantifier, and the change of entanglement is difficult to compute. We provided simplifications for important special scenarios and upper and lower bounds for the general case. One crucial question is whether one small part like one qubit can change a lot of quantum resources like quantum entanglement or not. Our results show that the entanglement change can be still arbitrarily large even with complete measurement information left. Besides, the measurement information can also make an arbitrarily large difference. Finally, we provide conditions under which quantum entanglement is always completely lost under classicalization.

While we focused on the difference between the original quantum resource and the remaining resource if one party becomes classical, the behavior of quantum resources during the quantum to classical transition is also interesting, and it may have a richer theoretical structure. We believe that our work paves the way for the design of concepts for quantum resource storage and may help to develop a novel direction in the field of quantum resource theories.

Bibliography

[1] Satoya Imai, Nikolai Wyderka, Andreas Ketterer, and Otfried Gühne. "Bound entanglement from randomized measurements". *Phys. Rev. Lett.* 126.15 (2021), 150501.

[2] Andreas Ketterer, Satoya Imai, Nikolai Wyderka, and Otfried Gühne. "Statistically significant tests of multiparticle quantum correlations based on randomized measurements". *Phys. Rev. A* 106.1 (2022), L010402.

[3] Xiao-Dong Yu, Satoya Imai, and Otfried Gühne. "Optimal entanglement certification from moments of the partial transpose". *Phys. Rev. Lett.* 127.6 (2021), 060504.

[4] Satoya Imai, Otfried Gühne, and Stefan Nimmrichter. "Work fluctuations and entanglement in quantum batteries". *Phys. Rev. A* 107.2 (2023), 022215.

[5] Zhen-Peng Xu, Satoya Imai, and Otfried Gühne. "Fate of multiparticle entanglement when one particle becomes classical". *Phys. Rev. A* 107.4 (2023), L040401.

[6] Nikolai Wyderka, Andreas Ketterer, Satoya Imai, Jan Lennart Bönsel, Daniel E Jones, Brian T Kirby, Xiao-Dong Yu, and Otfried Gühne. "Complete characterization of quantum correlations by randomized measurements". *Phys. Rev. Lett.* 131.9 (2023), 090201.

[7] Paweł Cieśliński, Satoya Imai, Jan Dziewior, Otfried Gühne, Lukas Knips, Wiesław Laskowski, Jasmin Meinecke, Tomasz Paterek, and Tamás Vértesi. "Analysing quantum systems with randomised measurements". *arXiv preprint arXiv:2307.01251* (2023).

[8] Chao Zhang et al. "Experimental verification of bound and multiparticle entanglement with the randomized measurement toolbox". *arXiv preprint arXiv:2307.04382* (2023).

[9] Benjamin Yadin, Satoya Imai, and Otfried Gühne. "Quantum speed limit for perturbed open systems". *arXiv preprint arXiv:2307.09118* (2023).

[10] Satoya Imai, Géza Tóth, and Otfried Gühne. "Collective randomized measurements in quantum information processing". *arXiv preprint arXiv:2309.10745* (2023).

[11] Shravan Shravan, Simon Morelli, Otfried Gühne, and Satoya Imai. "Geometry of two-body correlations in three-qubit states". *arXiv preprint arXiv:2309.09549* (2023).

[12] Asher Peres. "What's wrong with these observables?" *Foundations of Physics* 33 (2003), 1543–1547.

[13] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.* 47.10 (1935), 777.

[14] Erwin Schrödinger. "Die gegenwärtige Situation in der Quantenmechanik". *Naturwissenschaften* 23.50 (1935), 844–849.

[15] John S Bell. "On the einstein podolsky rosen paradox". *Physics Physique Fizika* 1.3 (1964), 195.

[16] John S Bell. *The theory of local beables*. Tech. rep. 1975.

[17] Otfried Gühne and Géza Tóth. "Entanglement detection". *Phys. Rep.* 474.1-6 (2009), 1–75.

[18] Jun John Sakurai and Eugene D Commins. *Modern quantum mechanics, revised edition*. 1995.

[19] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002.

[20] Teiko Heinosaari and Mário Ziman. *The mathematical language of quantum theory: from uncertainty to entanglement*. Cambridge University Press, 2011.

[21] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[22] Masahito Hayashi. *Quantum information theory*. Springer, 2016.

[23] Ingemar Bengtsson and Karol Życzkowski. *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge university press, 2017.

[24] Osvaldo Simeone et al. "An introduction to quantum machine learning for engineers". *Foundations and Trends® in Signal Processing* 16.1-2 (2022), 1–223.

[25] Gen Kimura. "The Bloch vector for N-level systems". *Physics Letters A* 314.5-6 (2003), 339–349.

[26] Reinhold A Bertlmann and Philipp Krammer. "Bloch vectors for qudits". *J. Phys. A* 41.23 (2008), 235303.

[27] Christopher Eltschka and Jens Siewert. "Distribution of entanglement and correlations in all finite dimensions". *Quantum* 2 (2018), 64.

[28] Lu Wei, Zhian Jia, Dagomir Kaszlikowski, and Sheng Tan. "Antilinear superoperator and quantum geometric invariance for higher-dimensional quantum systems". *arXiv preprint arXiv:2202.10989* (2022).

[29] Carlton M Caves and Gerard J Milburn. "Qutrit entanglement". *Optics communications* 179.1-6 (2000), 439–446.

[30] Paweł Kurzyński, Adrian Kołodziejski, Wiesław Laskowski, and Marcin Markiewicz. "Three-dimensional visualization of a qutrit". *Phys. Rev. A* 93.6 (2016), 062126.

[31] Christopher Eltschka, Marcus Huber, Simon Morelli, and Jens Siewert. "The shape of higher-dimensional state space: Bloch-ball analog for a qutrit". *Quantum* 5 (2021), 485.

[32] Daniel T Larson. *How to Talk to a Physicist: Groups, Symmetry, and Topology*. 2005.

[33] Wolfgang Ziller. "Lie groups, representation theory and symmetric spaces". *Lecture Notes (preliminary version)* (2010).

[34] Ashok Das and Susumu Okubo. *Lie groups and Lie algebras for physicists*. World Scientific, 2014.

[35] Alistair Savage. "Introduction to Lie groups". *Course notes of MAT* 1411 (2015).

[36] William K Wootters. "Entanglement of formation of an arbitrary state of two qubits". *Phys. Rev. Lett.* 80.10 (1998), 2245.

[37] Michał Horodecki and Paweł Horodecki. "Reduction criterion of separability and limits for a class of distillation protocols". *Phys. Rev. A* 59.6 (1999), 4206.

[38] Pranaw Rungta, Vladimir Bužek, Carlton M Caves, Mark Hillery, and Gerard J Milburn. "Universal state inversion and concurrence in arbitrary dimensions". *Phys. Rev. A* 64.4 (2001), 042315.

[39] Noëlle Pottier. *Nonequilibrium statistical physics: linear irreversible processes*. Oxford University Press, 2009.

[40] Vittorio Gorini, Andrzej Kossakowski, and Ennackal Chandy George Sudarshan. "Completely positive dynamical semigroups of N-level systems". *Journal of Mathematical Physics* 17.5 (1976), 821–825.

[41] Goran Lindblad. "On the generators of quantum dynamical semigroups". *Communications in Mathematical Physics* 48 (1976), 119–130.

[42] Angel Rivas and Susana F Huelga. *Open quantum systems*. Vol. 10. Springer, 2012.

[43] Daniel A Lidar. "Lecture notes on the theory of open quantum systems". *arXiv preprint arXiv:1902.00967* (2019).

[44] Heinz-Peter Breuer, Francesco Petruccione, et al. *The theory of open quantum systems*. Oxford University Press on Demand, 2002.

[45] Paul Busch. "Unsharp reality and joint measurements for spin observables". *Phys. Rev. D* 33.8 (1986), 2253.

[46] Paul Busch, Pekka Lahti, Juha-Pekka Pellonpää, and Kari Ylinen. *Quantum measurement*. Vol. 23. Springer, 2016.

[47] Konstantin Beyer, Roope Uola, Kimmo Luoma, and Walter T Strunz. "Joint measurability in nonequilibrium quantum thermodynamics". *Phys. Rev. E* 106.2 (2022), L022101.

[48] Barbara Kraus and J Ignacio Cirac. "Optimal creation of entanglement using a two-qubit gate". *Phys. Rev. A* 63.6 (2001), 062309.

[49] Jun Zhang, Jiri Vala, Shankar Sastry, and K Birgitta Whaley. "Geometric theory of nonlocal two-qubit operations". *Phys. Rev. A* 67.4 (2003), 042313.

[50] Suhail Ahmad Rather, S Aravinda, and Arul Lakshminarayan. "Creating ensembles of dual unitary and maximally entangling quantum evolutions". *Phys. Rev. Lett.* 125.7 (2020), 070501.

[51] Bhargavi Jonnadula, Prabha Mandayam, Karol Życzkowski, and Arul Lakshminarayan. "Entanglement measures of bipartite quantum gates and their thermalization under arbitrary interaction strength". *Phys. Rev. Research* 2.4 (2020), 043126.

[52] Claude Cohen-Tannoudji, Bernard Diu, and Frank Laloe. "Quantum Mechanics, Volume 2". *Quantum Mechanics* 2 (1986), 626.

[53] Gennaro Auletta, Mauro Fortunato, and Giorgio Parisi. *Quantum mechanics*. Cambridge University Press, 2009.

[54] Martin Houde. "Lecture note in Physics 9203a, Quantum Mechanics, Fall 2016, Department of Physics and Astronomy, University of Western Ontario" (2016).

[55] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. "Everything you always wanted to know about LOCC (but were afraid to ask)". *Commun. Math. Phys.* 328.1 (2014), 303–326.

[56] Frank Verstraete, Jeroen Dehaene, and Bart DeMoor. "Local filtering operations on two qubits". *Phys. Rev. A* 64.1 (2001), 010101.

[57] Frank Verstraete, Jeroen Dehaene, and Bart De Moor. "Normal forms and entanglement measures for multipartite quantum states". *Phys. Rev. A* 68.1 (2003), 012103.

[58] Jon Magne Leinaas, Jan Myrheim, and Eirik Ovrum. "Geometrical aspects of entanglement". *Phys. Rev. A* 74.1 (2006), 012313.

[59] Otfried Gühne, Philipp Hyllus, Oleg Gittsovich, and Jens Eisert. "Covariance matrices and the separability problem". *Phys. Rev. Lett.* 99.13 (2007), 130504.

[60] Julio I de Vicente. "Further results on entanglement detection and quantification from the correlation matrix criterion". *J. Phys. A* 41.6 (2008), 065309.

[61] William Hall. "Multipartite reduction criteria for separability". *Phys. Rev. A* 72.2 (2005), 022311.

[62] William Hall. "A new criterion for indecomposability of positive maps". *Journal of Physics A: Mathematical and General* 39.45 (2006), 14119.

[63] Heinz-Peter Breuer. "Optimal entanglement criterion for mixed quantum states". *Phys. Rev. Lett.* 97.8 (2006), 080501.

[64] Ryszard Horodecki et al. "Information-theoretic aspects of inseparability of mixed states". *Phys. Rev. A* 54.3 (1996), 1838.

[65] Benoıt Collins and Piotr Śniady. "Integration with respect to the Haar measure on unitary, orthogonal and symplectic group". *Communications in Mathematical Physics* 264.3 (2006), 773–795.

[66] Zbigniew Puchała and Jarosław Adam Miszczak. "Symbolic integration with respect to the Haar measure on the unitary group". *arXiv preprint arXiv:1109.4244* (2011).

[67] Christoph Spengler, Marcus Huber, and Beatrix C Hiesmayr. "Composite parameterization and Haar measure for all unitary and special unitary groups". *Journal of mathematical physics* 53.1 (2012), 013501.

[68] Lin Zhang. "Matrix integrals over unitary groups: An application of Schur-Weyl duality". *arXiv preprint arXiv:1408.3782* (2014).

[69] Benoit Collins, Sho Matsumoto, and Jonathan Novak. "The weingarten calculus". *arXiv preprint arXiv:2109.14890* (2022).

[70] Todd Tilma and ECG Sudarshan. "Generalized Euler angle parametrization for SU (N)". *Journal of Physics A: Mathematical and General* 35.48 (2002), 10467.

[71] Reinhard F Werner. "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model". *Phys. Rev. A* 40.8 (1989), 4277.

[72] Hermann Weyl. *The classical groups: their invariants and representations*. 1. Princeton university press, 1946.

[73] Barry Simon. *Representations of finite and compact groups*. 10. American Mathematical Soc., 1996.

[74] Karl Gerd H Vollbrecht and Reinhard F Werner. "Entanglement measures under symmetry". *Phys. Rev. A* 64.6 (2001), 062307.

[75] Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Artur Ekert, Maciej Lewenstein, Chiara Macchiavello, and Anna Sanpera. "Detection of entanglement with few local measurements". *Phys. Rev. A* 66.6 (2002), 062305.

[76] Otfried Gühne and Philipp Hyllus. "Investigating three qubit entanglement with local measurements". *International Journal of Theoretical Physics* 42 (2003), 1001–1013.

[77] Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Artur Ekert, Maciej Lewenstein, Chiara Macchiavello, and Anna Sanpera. "Experimental detection of entanglement via witness operators and local measurements". *Journal of Modern Optics* 50.6-7 (2003), 1079–1102.

[78] Mohamed Bourennane et al. “Experimental detection of multipartite entanglement using witness operators”. *Phys. Rev. Lett.* 92.8 (2004), 087902.

[79] Otfried Gühne, Chao-Yang Lu, Wei-Bo Gao, and Jian-Wei Pan. “Toolbox for entanglement detection and fidelity estimation”. *Phys. Rev. A* 76.3 (2007), 030305.

[80] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. “Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity”. *IEEE Transactions on Information Theory* 54.6 (2008), 2604–2620.

[81] Thomas M Cover. *Elements of information theory*. John Wiley & Sons, 1999.

[82] Hossein Pishro-Nik. “Introduction to probability, statistics, and random processes” (2016).

[83] Oliver Schabenberger and Carol A Gotway. *Statistical methods for spatial data analysis*. CRC press, 2017.

[84] Roman Vershynin. *High-dimensional probability: An introduction with applications in data science*. Vol. 47. Cambridge university press, 2018.

[85] Daniel FV James, Paul G Kwiat, William J Munro, and Andrew G White. “Measurement of qubits”. *Phys. Rev. A* 64.5 (2001), 052312.

[86] G Mauro D’Ariano, Matteo GA Paris, and Massimiliano F Sacchi. “Quantum tomography”. *Advances in imaging and electron physics* 128 (2003), 206–309.

[87] Matteo Paris and Jaroslav Rehacek. *Quantum state estimation*. Vol. 649. Springer Science & Business Media, 2004.

[88] Christopher A Fuchs and Jeroen Van De Graaf. “Cryptographic distinguishability measures for quantum-mechanical states”. *IEEE Transactions on Information Theory* 45.4 (1999), 1216–1227.

[89] Jaroslaw Adam Miszczak, Zbigniew Puchała, Pawel Horodecki, Armin Uhlmann, and Karol Życzkowski. “Sub–and super–fidelity as bounds for quantum fidelity”. *arXiv preprint arXiv:0805.2037* (2008).

[90] Yeong-Cherng Liang, Yu-Hao Yeh, Paulo EMF Mendonça, Run Yan Teh, Margaret D Reid, and Peter D Drummond. “Quantum fidelity measures for mixed states”. *Reports on Progress in Physics* 82.7 (2019), 076001.

[91] Samuel L Braunstein and Carlton M Caves. “Statistical distance and the geometry of quantum states”. *Phys. Rev. Lett.* 72.22 (1994), 3439.

[92] Matteo GA Paris. “Quantum estimation for quantum technology”. *International Journal of Quantum Information* 7.supp01 (2009), 125–137.

[93] J Lambert and ES Sørensen. “From Classical to Quantum Information Geometry, an Introductory Guide”. *arXiv preprint arXiv:2302.13515* (2023).

[94] Jing Liu, Haidong Yuan, Xiao-Ming Lu, and Xiaoguang Wang. "Quantum Fisher information matrix and multiparameter estimation". *J. Phys. A* 53.2 (2020), 023001.

[95] Paul Busch, Pekka Lahti, and Reinhard F Werner. "Colloquium: Quantum root-mean-square error and measurement uncertainty relations". *Rev. Mod. Phys* 86.4 (2014), 1261.

[96] Leonid Mandelstam and Igor Tamm. "The uncertainty relation between energy and time in non-relativistic quantum mechanics". *Selected papers*. Springer, 1991, 115–123.

[97] Norman Margolus and Lev B Levitin. "The maximum speed of dynamical evolution". *Physica D: Nonlinear Phenomena* 120.1-2 (1998), 188–195.

[98] Sebastian Deffner and Steve Campbell. "Quantum speed limits: from Heisenberg's uncertainty principle to optimal quantum control". *J. Phys. A* 50.45 (2017), 453001.

[99] Debashis Sen. "The uncertainty relations in quantum mechanics". *Current Science* (2014), 203–218.

[100] Stephen D Bartlett, Terry Rudolph, and Robert W Spekkens. "Reference frames, superselection rules, and quantum information". *Rev. Mod. Phys* 79.2 (2007), 555.

[101] Eric Chitambar and Gilad Gour. "Quantum resource theories". *Rev. Mod. Phys.* 91.2 (2019), 025001.

[102] VI Borodulin, RN Rogalyov, and SR Slabospitsky. "Core 2.1 (compendium of relations, version 2.1)". *arXiv preprint hep-ph/9507456* (1995).

[103] Zdravko Cvetkovski. *Inequalities: theorems, techniques and selected problems*. Springer Science & Business Media, 2012.

[104] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[105] Andreas Elben et al. "Mixed-state entanglement from local randomized measurements". *Phys. Rev. Lett.* 125.20 (2020), 200501.

[106] Howard Haber. "Useful relations among the generators in the defining and adjoint representations of SU (N)". *SciPost Physics Lecture Notes* (2021), 021.

[107] Artur K Ekert, Carolina Moura Alves, Daniel KL Oi, Michał Horodecki, Paweł Horodecki, and Leong Chuan Kwek. "Direct estimations of linear and nonlinear functionals of a quantum state". *Phys. Rev. Lett.* 88.21 (2002), 217901.

[108] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum principal component analysis". *Nat. Phys.* 10.9 (2014), 631–633.

[109] Daniel A Roberts and Beni Yoshida. "Chaos and complexity by design". *Journal of High Energy Physics* 2017.4 (2017), 1–64.

[110] William J Huggins, Sam McArdle, Thomas E O'Brien, Joonho Lee, Nicholas C Rubin, Sergio Boixo, K Birgitta Whaley, Ryan Babbush, and Jarrod R McClean. "Virtual distillation for quantum error mitigation". *Phys. Rev. X* 11.4 (2021), 041036.

[111] Bálint Koczor. "Exponential error suppression for near-term quantum devices". *Phys. Rev. X* 11.3 (2021), 031057.

[112] You Zhou, Pei Zeng, and Zhenhuan Liu. "Single-copies estimation of entanglement negativity". *Phys. Rev. Lett.* 125.20 (2020), 200502.

[113] Paweł Horodecki and Artur Ekert. "Method for direct detection of quantum entanglement". *Phys. Rev. Lett.* 89.12 (2002), 127902.

[114] Aram W Harrow and Richard A Low. "Random quantum circuits are approximate 2-designs". *Communications in Mathematical Physics* 291 (2009), 257–302.

[115] Felix Huber. "Positive maps and trace polynomials from the symmetric group". *Journal of Mathematical Physics* 62.2 (2021), 022203.

[116] Géza Tóth and Otfried Gühne. "Entanglement detection in the stabilizer formalism". *Phys. Rev. A* 72.2 (2005), 022340.

[117] Howard E Haber. "Notes on the matrix exponential and logarithm". *Santa Cruz Institute for Particle Physics, University of California: Santa Cruz, CA, USA* (2018).

[118] Martin B Plenio and Shashank Virmani. "An introduction to entanglement measures." *Quantum Inf. Comput.* 7.1 (2007), 1–51.

[119] Dagmar Bruß and Gerd Leuchs. "Lectures on quantum information" (2007).

[120] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. "Quantum entanglement". *Rev. Mod. Phys.* 81.2 (2009), 865.

[121] Christopher Eltschka and Jens Siewert. "Quantifying entanglement resources". *J. Phys. A* 47.42 (2014), 424005.

[122] Michael Walter, David Gross, and Jens Eisert. "Multipartite entanglement". *Quantum Information: From Foundations to Quantum Technology Applications* (2016), 293–330.

[123] Nicolai Friis, Giuseppe Vitagliano, Mehul Malik, and Marcus Huber. "Entanglement certification from theory to experiment". *Nature Reviews Physics* 1.1 (2019), 72–87.

[124] Barbara M Terhal and Paweł Horodecki. "Schmidt number for density matrices". *Phys. Rev. A* 61.4 (2000), 040301.

[125] Michael A Nielsen. "Conditions for a class of entanglement transformations". *Phys. Rev. Lett.* 83.2 (1999), 436.

[126] Michael A Nielsen. "An introduction to majorization and its applications to quantum mechanics". *Lecture Notes, Department of Physics, University of Queensland, Australia* (2002), 53.

[127] 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". *Phys. Rev. Lett.* 70.13 (1993), 1895.

[128] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L Braunstein. "Advances in quantum teleportation". *Nat. Photonics* 9.10 (2015), 641–652.

[129] William K Wootters and Wojciech H Zurek. "A single quantum cannot be cloned". *Nature* 299.5886 (1982), 802–803.

[130] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acin. "Quantum cloning". *Rev. Mod. Phys* 77.4 (2005), 1225.

[131] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. "Quantum state merging and negative information". *Communications in Mathematical Physics* 269 (2007), 107–136.

[132] Danilo Boschi, Salvatore Branca, Francesco De Martini, Lucien Hardy, and Sandu Popescu. "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels". *Phys. Rev. Lett.* 80.6 (1998), 1121.

[133] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. "Experimental quantum teleportation". *Nature* 390.6660 (1997), 575–579.

[134] Ji-Gang Ren et al. "Ground-to-satellite quantum teleportation". *Nature* 549.7670 (2017), 70–73.

[135] Jaroslaw K Korbicz, Otfried Gühne, Maciej Lewenstein, Hartmut Häffner, Christian F Roos, and Rainer Blatt. "Generalized spin-squeezing inequalities in N-qubit systems: Theory and experiment". *Phys. Rev. A* 74.5 (2006), 052319.

[136] Wolfgang Dür, Guifre Vidal, and J Ignacio Cirac. "Three qubits can be entangled in two inequivalent ways". *Phys. Rev. A* 62.6 (2000), 062314.

[137] Antonio Acin, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera. "Classification of mixed three-qubit states". *Phys. Rev. Lett.* 87.4 (2001), 040401.

[138] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. "How to share a quantum secret". *Phys. Rev. Lett.* 83.3 (1999), 648.

[139] Robert Raussendorf and Hans J Briegel. "A one-way quantum computer". *Phys. Rev. Lett.* 86.22 (2001), 5188.

[140] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. "Optical quantum memory". *Nat. Photonics* 3.12 (2009), 706–714.

[141] Frank Verstraete, Jeroen Dehaene, Bart De Moor, and Henri Verschelde. "Four qubits can be entangled in nine different ways". *Phys. Rev. A* 65.5 (2002), 052112.

[142] Hans J Briegel and Robert Raussendorf. "Persistent entanglement in arrays of interacting particles". *Phys. Rev. Lett.* 86.5 (2001), 910.

[143] Marc Hein, Jens Eisert, and Hans J Briegel. "Multiparty entanglement in graph states". *Phys. Rev. A* 69.6 (2004), 062311.

[144] Matteo Rossi, Marcus Huber, Dagmar Bruß, and Chiara Macchiavello. "Quantum hypergraph states". *New J. Phys* 15.11 (2013), 113022.

[145] Wolfram Helwig, Wei Cui, José Ignacio Latorre, Arnau Riera, and Hoi-Kwong Lo. "Absolute maximal entanglement and quantum secret sharing". *Phys. Rev. A* 86.5 (2012), 052335.

[146] Felix Huber, Otfried Gühne, and Jens Siewert. "Absolutely maximally entangled states of seven qubits do not exist". *Phys. Rev. Lett.* 118.20 (2017), 200502.

[147] Philipp Krammer, Hermann Kampermann, Dagmar Bruß, Reinhold A Bertlmann, Leong Chuang Kwek, and Chiara Macchiavello. "Multipartite entanglement detection via structure factors". *Phys. Rev. Lett.* 103.10 (2009), 100502.

[148] A Chiuri, G Vallone, N Bruno, C Macchiavello, D Bruß, and P Mataloni. "Hyperentangled mixed phased Dicke states: optical design and detection". *Phys. Rev. Lett.* 105.25 (2010), 250501.

[149] Marcus Cramer, Martin B Plenio, and Harald Wunderlich. "Measuring entanglement in condensed matter systems". *Phys. Rev. Lett.* 106.2 (2011), 020401.

[150] Oliver Marty, Michael Epping, Hermann Kampermann, Dagmar Bruß, Martin B Plenio, and M Cramer. "Quantifying entanglement with scattering experiments". *Phys. Rev. B* 89.12 (2014), 125117.

[151] Massimo Borrelli, Matteo Rossi, Chiara Macchiavello, and Sabrina Maniscalco. "Witnessing entanglement in hybrid systems". *Phys. Rev. A* 90.2 (2014), 020301.

[152] Zihao Li, Yun-Guang Han, Hao-Feng Sun, Jiangwei Shang, and Huangjun Zhu. "Verification of phased Dicke states". *Phys. Rev. A* 103.2 (2021), 022601.

[153] Sevag Gharibian. "Strong NP-hardness of the quantum separability problem". *arXiv preprint arXiv:0810.4507* (2008).

[154] Maciej Lewenstein, Barabara Kraus, J Ignacio Cirac, and Pawel Horodecki. "Optimization of entanglement witnesses". *Phys. Rev. A* 62.5 (2000), 052310.

[155] Dagmar Bruß, J Ignacio Cirac, Pawel Horodecki, Florian Hulpke, Barbara Kraus, Maciej Lewenstein, and Anna Sanpera. "Reflections upon separability and distillability". *Journal of Modern Optics* 49.8 (2002), 1399–1418.

[156] Antonio Acin, Nicolas Gisin, and Lluis Masanes. "From Bell's theorem to secure quantum key distribution". *Phys. Rev. Lett.* 97.12 (2006), 120405.

[157] Jean-Daniel Bancal and Jean-Daniel Bancal. "Device-independent witnesses of genuine multipartite entanglement". *On the Device-Independent Approach to Quantum Physics: Advances in Quantum Nonlocality and Multipartite Entanglement Detection* (2014), 73–80.

[158] Károly F Pál, Tamás Vértesi, and Miguel Navascués. "Device-independent tomography of multipartite quantum states". *Phys. Rev. A* 90.4 (2014), 042340.

[159] Anders Sørensen, L-M Duan, Juan Ignacio Cirac, and Peter Zoller. "Many-particle entanglement with Bose–Einstein condensates". *Nature* 409.6816 (2001), 63–66.

[160] Géza Tóth, Christian Knapp, Otfried Gühne, and Hans J Briegel. "Optimal spin squeezing inequalities detect bound entanglement in spin models". *Phys. Rev. Lett.* 99.25 (2007), 250405.

[161] Jian Ma, Xiaoguang Wang, Chang-Pu Sun, and Franco Nori. "Quantum spin squeezing". *Physics Reports* 509.2-3 (2011), 89–165.

[162] Nicolas J Cerf and Chris Adami. "Negative entropy and information in quantum mechanics". *Phys. Rev. Lett.* 79.26 (1997), 5194.

[163] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. "Partial quantum information". *Nature* 436.7051 (2005), 673–676.

[164] Valerie Coffman, Joydip Kundu, and William K Wootters. "Distributed entanglement". *Phys. Rev. A* 61.5 (2000), 052306.

[165] Tobias J Osborne and Frank Verstraete. "General monogamy inequality for bipartite qubit entanglement". *Phys. Rev. Lett.* 96.22 (2006), 220503.

[166] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?" *Phys. Rev. Lett.* 80.24 (1998), 5239.

[167] David P DiVincenzo, Peter W Shor, John A Smolin, Barbara M Terhal, and Ashish V Thapliyal. "Evidence for bound entangled states with negative partial transpose". *Phys. Rev. A* 61.6 (2000), 062312.

[168] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. "Entanglement as a precondition for secure quantum key distribution". *Phys. Rev. Lett.* 92.21 (2004), 217903.

[169] Luca Pezzé and Augusto Smerzi. "Entanglement, nonlinear dynamics, and the Heisenberg limit". *Phys. Rev. Lett.* 102.10 (2009), 100401.

[170] Géza Tóth and Iagoba Apellaniz. "Quantum metrology from a quantum information science perspective". *J. Phys. A* 47.42 (2014), 424006.

[171] Luca Pezzè, Augusto Smerzi, Markus K Oberthaler, Roman Schmied, and Philipp Treutlein. "Quantum metrology with nonclassical states of atomic ensembles". *Rev. Mod. Phys* 90.3 (2018), 035005.

[172] Wolfgang Dür, J Ignacio Cirac, and Rolf Tarrach. "Separability and distillability of multiparticle quantum systems". *Phys. Rev. Lett.* 83.17 (1999), 3562.

[173] Wolfgang Dür and J Ignacio Cirac. "Classification of multiqubit mixed states: Separability and distillability properties". *Phys. Rev. A* 61.4 (2000), 042314.

[174] Otfried Gühne, Géza Tóth, and Hans J Briegel. "Multipartite entanglement in spin chains". *New J. Phys* 7.1 (2005), 229.

[175] Otfried Gühne and Géza Tóth. "Energy and multipartite entanglement in multidimensional and frustrated spin models". *Phys. Rev. A* 73.5 (2006), 052319.

[176] Philipp Hyllus, Wiesław Laskowski, Roland Krischek, Christian Schwemmer, Witlef Wieczorek, Harald Weinfurter, Luca Pezzé, and Augusto Smerzi. "Fisher information and multiparticle entanglement". *Phys. Rev. A* 85.2 (2012), 022321.

[177] Anders S Sørensen and Klaus Mølmer. "Entanglement and extreme spin squeezing". *Phys. Rev. Lett.* 86.20 (2001), 4431.

[178] Szilárd Szalay. "k-stretchability of entanglement, and the duality of k-separability and k-producibility". *Quantum* 3 (2019), 204.

[179] Géza Tóth. "Stretching the limits of multiparticle entanglement". *Quantum Views* 4 (2020), 30.

[180] Zhihong Ren, Weidong Li, Augusto Smerzi, and Manuel Gessner. "Metrological detection of multipartite entanglement from young diagrams". *Phys. Rev. Lett.* 126.8 (2021), 080502.

[181] Jens Eisert and Hans J Briegel. "Schmidt measure as a tool for quantifying multiparticle entanglement". *Phys. Rev. A* 64.2 (2001), 022306.

[182] Christoph Spengler, Marcus Huber, Andreas Gabriel, and Beatrix C Hiesmayr. "Examining the dimensionality of genuine multipartite entanglement". *Quantum information processing* 12 (2013), 269–278.

[183] Marcus Huber and Julio I De Vicente. "Structure of multidimensional entanglement in multipartite systems". *Phys. Rev. Lett.* 110.3 (2013), 030501.

[184] Tristan Kraft, Christina Ritz, Nicolas Brunner, Marcus Huber, and Otfried Gühne. "Characterizing genuine multilevel entanglement". *Phys. Rev. Lett.* 120.6 (2018), 060502.

[185] Miguel Navascues, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens. "Genuine network multipartite entanglement". *Phys. Rev. Lett.* 125.24 (2020), 240505.

[186] Armin Tavakoli, Alejandro Pozas-Kerstjens, Ming-Xing Luo, and Marc-Olivier Renou. "Bell nonlocality in networks". *Reports on Progress in Physics* 85.5 (2022), 056001.

[187] Kiara Hansenne, Zhen-Peng Xu, Tristan Kraft, and Otfried Gühne. "Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques". *Nat. Commun.* 13.1 (2022), 496.

[188] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. "Proposed experiment to test local hidden-variable theories". *Phys. Rev. Lett.* 23.15 (1969), 880.

[189] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". *Rev. Mod. Phys* 86.2 (2014), 419.

[190] Valerio Scarani. *Bell nonlocality*. Oxford University Press, 2019.

[191] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. "Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition". *Physics Letters A* 200.5 (1995), 340–344.

[192] Samuel L Braunstein, Ady Mann, and Michael Revzen. "Maximal violation of Bell inequalities for mixed states". *Phys. Rev. Lett.* 68.22 (1992), 3259.

[193] Frank Verstraete and Michael M Wolf. "Entanglement versus Bell violations and their behavior under local filtering operations". *Phys. Rev. Lett.* 89.17 (2002), 170401.

[194] Asher Peres. "Separability criterion for density matrices". *Phys. Rev. Lett.* 77.8 (1996), 1413.

[195] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps". *Physics Letters A* 283.1-2 (2001), 1–7.

[196] Anna Sanpera, Rolf Tarrach, and Guifré Vidal. "Local description of quantum inseparability". *Phys. Rev. A* 58.2 (1998), 826.

[197] Remigiusz Augusiak, Maciej Demianowicz, and Paweł Horodecki. "Universal observable detecting all two-qubit entanglement and determinant-based separability tests". *Phys. Rev. A* 77.3 (2008), 030301.

[198] Géza Tóth and Otfried Gühne. "Entanglement and permutational symmetry". *Phys. Rev. Lett.* 102.17 (2009), 170503.

[199] Fabian Bohnet-Waldraff, Daniel Braun, and Olivier Giraud. "Partial transpose criteria for symmetric states". *Phys. Rev. A* 94.4 (2016), 042343.

[200] Remigiusz Augusiak, Janusz Grabowski, Marek Kuś, and Maciej Lewenstein. "Searching for extremal PPT entangled states". *Optics Communications* 283.5 (2010), 805–813.

[201] J Tura, R Augusiak, P Hyllus, M Kuś, J Samsonowicz, and M Lewenstein. "Four-qubit entangled symmetric states with positive partial transpositions". *Phys. Rev. A* 85.6 (2012), 060302.

[202] R Augusiak, J Tura, J Samsonowicz, and M Lewenstein. "Entangled symmetric states of N qubits with all positive partial transpositions". *Phys. Rev. A* 86.4 (2012), 042316.

[203] Xiao-Dong Yu, Timo Simnacher, Nikolai Wyderka, H Chau Nguyen, and Otfried Gühne. "A complete hierarchy for the pure state marginal problem in quantum mechanics". *Nat. Commun.* 12.1 (2021), 1012.

[204] NJ Cerf, C Adami, and RM Gingrich. "Reduction criterion for separability". *Phys. Rev. A* 60.2 (1999), 898.

[205] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. "Quantum α-entropy inequalities: independent condition for local realism?" *Physics Letters A* 210.6 (1996), 377–381.

[206] Karl Gerd H Vollbrecht and Michael M Wolf. "Conditional entropies and their relation to entanglement criteria". *Journal of Mathematical Physics* 43.9 (2002), 4299–4306.

[207] Remigiusz Augusiak, Julia Stasińska, and Paweł Horodecki. "Beyond the standard entropic inequalities: Stronger scalar separability criteria and their applications". *Phys. Rev. A* 77.1 (2008), 012333.

[208] Remigiusz Augusiak and Julia Stasińska. "General scheme for construction of scalar separability criteria from positive maps". *Phys. Rev. A* 77.1 (2008), 010303.

[209] Michael A Nielsen and Julia Kempe. "Separable states are more disordered globally than locally". *Phys. Rev. Lett.* 86.22 (2001), 5184.

[210] Tohya Hiroshima. "Majorization criterion for distillability of a bipartite quantum state". *Phys. Rev. Lett.* 91.5 (2003), 057902.

[211] Albert Rico and Felix Huber. "Entanglement detection with trace polynomials". *arXiv preprint arXiv:2303.07761* (2023).

[212] John de Pillis. "Linear transformations which preserve hermitian and positive semidefinite operators". *Pacific Journal of Mathematics* 23.1 (1967), 129–137.

[213] Man-Duen Choi. "Completely positive linear maps on complex matrices". *Linear algebra and its applications* 10.3 (1975), 285–290.

[214] Andrzej Jamiołkowski. "Linear transformations which preserve trace and positive semidefiniteness of operators". *Reports on Mathematical Physics* 3.4 (1972), 275–278.

[215] Barbara M Terhal. "Bell inequalities and the separability criterion". *Physics Letters A* 271.5-6 (2000), 319–326.

[216] Mirjam Weilenmann, Benjamin Dive, David Trillo, Edgar A Aguilar, and Miguel Navascués. "Entanglement detection beyond measuring fidelities". *Phys. Rev. Lett.* 124.20 (2020), 200502.

[217] Pengyu Liu, Zhenhuan Liu, Shu Chen, and Xiongfeng Ma. "Fundamental limitation on the detectability of entanglement". *Phys. Rev. Lett.* 129.23 (2022), 230503.

[218] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "General teleportation channel, singlet fraction, and quasidistillation". *Phys. Rev. A* 60.3 (1999), 1888.

[219] Gernot Alber et al. "Mixed-state entanglement and quantum communication". *Quantum information: An introduction to basic theoretical concepts and experiments* (2001), 151–195.

[220] Otfried Gühne, Yuanyuan Mao, and Xiao-Dong Yu. "Geometry of faithful entanglement". *Phys. Rev. Lett.* 126.14 (2021), 140503.

[221] Gabriele Riccardi, Daniel E Jones, Xiao-Dong Yu, Otfried Gühne, and Brian T Kirby. "Exploring the relationship between the faithfulness and entanglement of two qubits". *Phys. Rev. A* 103.4 (2021), 042417.

[222] Lieven Clarisse. "Entanglement distillation; a discourse on bound entanglement in quantum information theory". *arXiv preprint quant-ph/0612072* (2006).

[223] Michael Gaida and Matthias Kleinmann. "Seven definitions of bipartite bound entanglement". *arXiv preprint arXiv:2212.11015* (2022).

[224] Paweł Horodecki, Łukasz Rudnicki, and Karol Życzkowski. "Five open problems in quantum information theory". *PRX Quantum* 3.1 (2022), 010101.

[225] Asher Peres. "All the Bell inequalities". *Foundations of Physics* 29.4 (1999), 589–614.

[226] W Dür. "Multipartite bound entangled states that violate Bell's inequality". *Phys. Rev. Lett.* 87.23 (2001), 230402.

[227] Tamás Vértesi and Nicolas Brunner. "Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement". *Nat. Commun.* 5.1 (2014), 5297.

[228] Matthew F Pusey. "Negativity and steering: A stronger Peres conjecture". *Phys. Rev. A* 88.3 (2013), 032313.

[229] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti. "Quantifying einstein-podolsky-rosen steering". *Phys. Rev. Lett.* 112.18 (2014), 180404.

[230] Tobias Moroder, Oleg Gittsovich, Marcus Huber, and Otfried Gühne. "Steering bound entangled states: a counterexample to the stronger Peres conjecture". *Phys. Rev. Lett.* 113.5 (2014), 050404.

[231] Pawel Horodecki, John A Smolin, Barbara M Terhal, and Ashish V Thapliyal. "Rank two bipartite bound entangled states do not exist". *Theoretical Computer Science* 292.3 (2003), 589–596.

[232] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "Secure key from bound entanglement". *Phys. Rev. Lett.* 94.16 (2005), 160502.

[233] Karol Horodecki, Lukasz Pankowski, Michal Horodecki, and Pawel Horodecki. "Low-dimensional bound entanglement with one-way distillable cryptographic key". *IEEE Transactions on Information Theory* 54.6 (2008), 2621–2625.

[234] Géza Tóth and Tamás Vértesi. "Quantum states with a positive partial transpose are useful for metrology". *Phys. Rev. Lett.* 120.2 (2018), 020506.

[235] Károly F Pál, Géza Tóth, Erika Bene, and Tamás Vértesi. "Bound entangled singlet-like states for quantum metrology". *Phys. Rev. Research* 3.2 (2021), 023101.

[236] Otfried Gühne. "Entanglement criteria and full separability of multi-qubit quantum states". *Phys. Lett. A* 375.3 (2011), 406–410.

[237] Koji Nagata. "Necessary and sufficient condition for Greenberger-Horne-Zeilinger diagonal states to be full N-partite entangled". *Int. J. Theor. Phys.* 48.12 (2009), 3358–3364.

[238] Kiara Hansenne et al. "Quantum Entanglement: a Study of Recent Separability Criteria" (2020).

[239] Pawel Horodecki. "Separability criterion and inseparable mixed states with positive partial transposition". *Phys. Lett. A* 232.5 (1997), 333–339.

[240] Oliver Rudolph. "A separability criterion for density operators". *Journal of Physics A: Mathematical and General* 33.21 (2000), 3951.

[241] Kai Chen and Ling-An Wu. "A matrix realignment method for recognizing entanglement". *arXiv preprint quant-ph/0205017* (2002).

[242] Oliver Rudolph. "Further results on the cross norm criterion for separability". *Quantum Information Processing* 4 (2005), 219–239.

[243] Cheng-Jie Zhang, Yong-Sheng Zhang, Shun Zhang, and Guang-Can Guo. "Entanglement detection beyond the computable cross-norm or realignment criterion". *Phys. Rev. A* 77.6 (2008), 060301.

[244] Julio I De Vicente. "Separability criteria based on the Bloch representation of density matrices". *arXiv preprint quant-ph/0607195* (2006).

[245] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "Separability of mixed quantum states: linear contractions and permutation criteria". *Open Systems & Information Dynamics* 13 (2006), 103–111.

[246] Holger F Hofmann and Shigeki Takeuchi. "Violation of local uncertainty relations as a signature of entanglement". *Phys. Rev. A* 68.3 (2003), 032103.

[247] Otfried Gühne. "Characterizing entanglement via uncertainty relations". *Phys. Rev. Lett.* 92.11 (2004), 117903.

[248] Carlos de Gois, Kiara Hansenne, and Otfried Gühne. "Uncertainty relations from graph theory". *Phys. Rev. A* 107.6 (2023), 062211.

[249] Oleg Gittsovich, Otfried Gühne, Philipp Hyllus, and Jens Eisert. "Unifying several separability conditions using the covariance matrix criterion". *Phys. Rev. A* 78.5 (2008), 052319.

[250] Jiangwei Shang, Ali Asadian, Huangjun Zhu, and Otfried Gühne. "Enhanced entanglement criterion via symmetric informationally complete measurements". *Phys. Rev. A* 98.2 (2018), 022309.

[251] Gniewomir Sarbicki, Giovanni Scala, and Dariusz Chruściński. "Family of multipartite separability criteria based on a correlation tensor". *Phys. Rev. A* 101.1 (2020), 012341.

[252] Sabine Wölk, Marcus Huber, and Otfried Gühne. "Unified approach to entanglement criteria using the Cauchy-Schwarz and Hölder inequalities". *Phys. Rev. A* 90.2 (2014), 022315.

[253] Y Akbari-Kourbolagh and M Azhdargalam. "Entanglement criterion for multipartite systems based on quantum Fisher information". *Phys. Rev. A* 99.1 (2019), 012304.

[254] Qing-Hua Zhang and Shao-Ming Fei. "A sufficient entanglement criterion based on quantum fisher information and variance". *Laser Physics Letters* 17.6 (2020), 065202.

[255] Zhenhuan Liu, Yifan Tang, Hao Dai, Pengyu Liu, Shu Chen, and Xiongfeng Ma. "Detecting entanglement in quantum many-body systems via permutation moments". *Phys. Rev. Lett.* 129.26 (2022), 260501.

[256] Ties-A Ohst, Xiao-Dong Yu, Otfried Gühne, and H Chau Nguyen. "Certifying Quantum Separability with Adaptive Polytopes". *arXiv preprint arXiv:2210.10054* (2022).

[257] Julio I de Vicente and Marcus Huber. "Multipartite entanglement detection from correlation tensors". *Phys. Rev. A* 84.6 (2011), 062306.

[258] Nikolai Wyderka and Andreas Ketterer. "Probing the geometry of correlation matrices with randomized measurements". *PRX Quantum* 4.2 (2023), 020325.

[259] Anna Sanpera, Dagmar Bruß, and Maciej Lewenstein. "Schmidt-number witnesses and bound entanglement". *Phys. Rev. A* 63.5 (2001), 050301.

[260] Marco Piani and Caterina E Mora. "Class of positive-partial-transpose bound entangled states associated with almost any set of pure entangled states". *Phys. Rev. A* 75.1 (2007), 012305.

[261] Łukasz Pankowski, Marco Piani, Michał Horodecki, and Paweł Horodecki. "A few steps more towards NPT bound entanglement". *IEEE Transactions on Information Theory* 56.8 (2010), 4085–4100.

[262] Sixia Yu and CH Oh. "Family of nonlocal bound entangled states". *Phys. Rev. A* 95.3 (2017), 032111.

[263] Satvik Singh. "Can entanglement hide behind triangle-free graphs?" *arXiv preprint arXiv:2010.11891* (2020).

[264] Joonwoo Bae, Anindita Bera, Dariusz Chruściński, Beatrix C Hiesmayr, and Daniel McNulty. "How many measurements are needed to detect bound entangled states?" *arXiv preprint arXiv:2108.01109* (2021).

[265] Joshua Lockhart, Otfried Gühne, and Simone Severini. "Entanglement properties of quantum grid states". *Phys. Rev. A* 97.6 (2018), 062340.

[266] Dagmar Bruß and Asher Peres. "Construction of quantum states with bound entanglement". *Phys. Rev. A* 61.3 (2000), 030301.

[267] Charles H Bennett, David P DiVincenzo, Tal Mor, Peter W Shor, John A Smolin, and Barbara M Terhal. "Unextendible product bases and bound entanglement". *Phys. Rev. Lett.* 82.26 (1999), 5385.

[268] Paweł Horodecki, Michał Horodecki, and Ryszard Horodecki. "Bound entanglement can be activated". *Phys. Rev. Lett.* 82.5 (1999), 1056.

[269] Beatrix C Hiesmayr. "Free versus Bound Entanglement: Machine learning tackling a NP-hard problem". *arXiv preprint arXiv:2106.03977* (2021).

[270] Marcin Wieśniak. "Two-Qutrit entanglement: 56-years old algorithm challenges machine learning". *arXiv preprint arXiv:2211.03213* (2022).

[271] Fabio Benatti, Roberto Floreanini, and Marco Piani. "Non-decomposable quantum dynamical semigroups and bound entangled states". *Open Systems & Information Dynamics* 11.04 (2004), 325–338.

[272] Alastair Kay. "Optimal detection of entanglement in Greenberger-Horne-Zeilinger states". *Phys. Rev. A* 83.2 (2011), 020303.

[273] Philipp Hyllus. "Witnessing entanglement in qudit systems". PhD thesis. Hannover: Universität, 2005.

[274] Otfried Gühne and Michael Seevinck. "Separability criteria for genuine multiparticle entanglement". *New J. Phys* 12.5 (2010), 053002.

[275] Tilo Eggeling and Reinhard F Werner. "Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry". *Phys. Rev. A* 63.4 (2001), 042111.

[276] Géza Tóth, Christian Knapp, Otfried Gühne, and Hans J Briegel. "Spin squeezing and entanglement". *Phys. Rev. A* 79.4 (2009), 042334.

[277] Michał Horodecki. "Simplifying monotonicity conditions for entanglement measures". *Open Systems & Information Dynamics* 12.3 (2005), 231–237.

[278] CL Liu, Xiao-Dong Yu, and DM Tong. "Flag additivity in quantum resource theories". *Phys. Rev. A* 99.4 (2019), 042322.

[279] Guifré Vidal and Reinhard F Werner. "Computable measure of entanglement". *Phys. Rev. A* 65.3 (2002), 032314.

[280] Matthias Christandl and Andreas Winter. ""Squashed entanglement": an additive entanglement measure". *J. Math. Phys.* 45.3 (2004), 829–840.

[281] 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 Trans. Inf. Theory* 55.7 (2009), 3375–3387.

[282] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "Locking entanglement with a single qubit". *Phys. Rev. Lett.* 94.20 (2005), 200501.

[283] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Quantum-enhanced measurements: beating the standard quantum limit". *Science* 306.5700 (2004), 1330–1336.

[284] Johannes Jakob Meyer. "Fisher information in noisy intermediate-scale quantum applications". *Quantum* 5 (2021), 539.

[285] Nathan Shettell. "Quantum Information Techniques for Quantum Metrology". *arXiv preprint arXiv:2201.01523* (2022).

[286] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Quantum metrology". *Phys. Rev. Lett.* 96.1 (2006), 010401.

[287] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Advances in quantum metrology". *Nat. Photonics* 5.4 (2011), 222–229.

[288] Luca Pezze and Augusto Smerzi. "Quantum theory of phase estimation". *arXiv preprint arXiv:1411.5164* (2014).

[289] Daniel Braun, Gerardo Adesso, Fabio Benatti, Roberto Floreanini, Ugo Marzolino, Morgan W Mitchell, and Stefano Pirandola. "Quantum-enhanced measurements without entanglement". *Rev. Mod. Phys* 90.3 (2018), 035006.

[290] Sergio Boixo, Steven T Flammia, Carlton M Caves, and John M Geremia. "Generalized limits for single-parameter quantum estimation". *Phys. Rev. Lett.* 98.9 (2007), 090401.

[291] Sergio Boixo, Animesh Datta, Matthew J Davis, Steven T Flammia, Anil Shaji, and Carlton M Caves. "Quantum metrology: dynamics versus entanglement". *Phys. Rev. Lett.* 101.4 (2008), 040403.

[292] Sergio Boixo, Animesh Datta, Steven T Flammia, Anil Shaji, Emilio Bagan, and Carlton M Caves. "Quantum-limited metrology with product states". *Phys. Rev. A* 77.1 (2008), 012317.

[293] Sergio Boixo, Animesh Datta, Matthew J Davis, Anil Shaji, Alexandre B Tacla, and Carlton M Caves. "Quantum-limited metrology and Bose-Einstein condensates". *Phys. Rev. A* 80.3 (2009), 032103.

[294] Mario Napolitano, Marco Koschorreck, Brice Dubost, Naeimeh Behbood, RJ Sewell, and Morgan W Mitchell. "Interaction-based quantum metrology showing scaling beyond the Heisenberg limit". *Nature* 471.7339 (2011), 486–489.

[295] SM Roy and Samuel L Braunstein. "Exponentially enhanced quantum metrology". *Phys. Rev. Lett.* 100.22 (2008), 220501.

[296] Marcin Zwierz, Carlos A Pérez-Delgado, and Pieter Kok. "General optimality of the Heisenberg limit for quantum metrology". *Phys. Rev. Lett.* 105.18 (2010), 180402.

[297] Marcin Zwierz, Carlos A Pérez-Delgado, and Pieter Kok. "Ultimate limits to quantum metrology and the meaning of the Heisenberg limit". *Phys. Rev. A* 85.4 (2012), 042112.

[298] Masahiro Hotta and Masanao Ozawa. "Quantum estimation by local observables". *Phys. Rev. A* 70.2 (2004), 022327.

[299] BM Escher. "Quantum Noise-to-Sensibility Ratio". *arXiv preprint arXiv:1212.2533* (2012).

[300] Carl W Helstrom. "Minimum mean-squared error of estimates in quantum statistics". *Physics letters A* 25.2 (1967), 101–102.

[301] Harry L Van Trees and Kristine L Bell. "Bayesian bounds for parameter estimation and nonlinear filtering/tracking". *AMC* 10.12 (2007), 10–1109.

[302] Magdalena Szczykulska, Tillmann Baumgratz, and Animesh Datta. "Multiparameter quantum metrology". *Advances in Physics: X* 1.4 (2016), 621–639.

[303] Manuel Gessner, Luca Pezzè, and Augusto Smerzi. "Sensitivity bounds for multiparameter quantum metrology". *Phys. Rev. Lett.* 121.13 (2018), 130503.

[304] Francesco Albarelli, Jamie F Friel, and Animesh Datta. "Evaluating the holevo cramér-rao bound for multiparameter quantum metrology". *Phys. Rev. Lett.* 123.20 (2019), 200503.

[305] Francesco Albarelli, Marco Barbieri, Marco G Genoni, and Ilaria Gianani. "A perspective on multiparameter quantum metrology: From theoretical tools to applications in quantum imaging". *Physics Letters A* 384.12 (2020), 126311.

[306] Wojciech Górecki. "Heisenberg limit beyond quantum Fisher information". *arXiv preprint arXiv:2304.14370* (2023).

[307] Wenchao Ge, Kurt Jacobs, Zachary Eldredge, Alexey V Gorshkov, and Michael Foss-Feig. "Distributed quantum metrology with linear networks and separable inputs". *Phys. Rev. Lett.* 121.4 (2018), 043604.

[308] Timothy J Proctor, Paul A Knott, and Jacob A Dunningham. "Multiparameter estimation in networked quantum sensors". *Phys. Rev. Lett.* 120.8 (2018), 080501.

[309] Yuxiang Yang, Benjamin Yadin, and Zhen-Peng Xu. "Quantum-enhanced metrology with network states". *arXiv preprint arXiv:2307.07758* (2023).

[310] Mohammad Mehboudi, Anna Sanpera, and Luis A Correa. "Thermometry in the quantum regime: recent theoretical progress". *J. Phys. A* 52.30 (2019), 303001.

[311] David J Wineland, John J Bollinger, Wayne M Itano, FL Moore, and Daniel J Heinzen. "Spin squeezing and reduced quantum noise in spectroscopy". *Phys. Rev. A* 46.11 (1992), R6797.

[312] David J Wineland, John J Bollinger, Wayne M Itano, and DJ Heinzen. "Squeezed atomic states and projection noise in spectroscopy". *Phys. Rev. A* 50.1 (1994), 67.

[313] Masahiro Kitagawa and Masahito Ueda. "Squeezed spin states". *Phys. Rev. A* 47.6 (1993), 5138.

[314] Jerome Esteve, Christian Gross, Andreas Weller, Stefano Giovanazzi, and Markus K Oberthaler. "Squeezing and entanglement in a Bose–Einstein condensate". *Nature* 455.7217 (2008), 1216–1219.

[315] Géza Tóth. "Entanglement detection in optical lattices of bosonic atoms with collective measurements". *Phys. Rev. A* 69.5 (2004), 052327.

[316] Géza Tóth and Morgan W Mitchell. "Generation of macroscopic singlet states in atomic ensembles". *New J. Phys* 12.5 (2010), 053007.

[317] Inigo Urizar-Lanz, Philipp Hyllus, Inigo Luis Egusquiza, Morgan W Mitchell, and Géza Tóth. "Macroscopic singlet states for gradient magnetometry". *Phys. Rev. A* 88.1 (2013), 013626.

[318] Irénée Frérot and Tommaso Roscilde. "Detecting many-body bell nonlocality by solving ising models". *Phys. Rev. Lett.* 126.14 (2021), 140504.

[319] Guillem Müller-Rigat, Albert Aloy, Maciej Lewenstein, and Irénée Frérot. "Inferring nonlinear many-body bell inequalities from average two-body correlations: Systematic approach for arbitrary spin-j ensembles". *PRX Quantum* 2.3 (2021), 030329.

[320] Géza Tóth. "Multipartite entanglement and high-precision metrology". *Phys. Rev. A* 85.2 (2012), 022322.

[321] Giuseppe Vitagliano, Philipp Hyllus, Inigo L Egusquiza, and Géza Tóth. "Spin squeezing inequalities for arbitrary spin". *Phys. Rev. Lett.* 107.24 (2011), 240502.

[322] Giuseppe Vitagliano, Iagoba Apellaniz, Inigo L Egusquiza, and Géza Tóth. "Spin squeezing and entanglement for an arbitrary spin". *Phys. Rev. A* 89.3 (2014), 032307.

[323] John K Stockton, JM Geremia, Andrew C Doherty, and Hideo Mabuchi. "Characterizing the entanglement of symmetric many-particle spin-1 2 systems". *Phys. Rev. A* 67.2 (2003), 022112.

[324] Géza Tóth. "Detection of multipartite entanglement in the vicinity of symmetric Dicke states". *JOSA B* 24.2 (2007), 275–282.

[325] Bernd Lücke, Jan Peise, Giuseppe Vitagliano, Jan Arlt, Luis Santos, Géza Tóth, and Carsten Klempt. "Detecting multiparticle entanglement of Dicke states". *Phys. Rev. Lett.* 112.15 (2014), 155304.

[326] Iagoba Apellaniz, Bernd Lücke, Jan Peise, Carsten Klempt, and Géza Tóth. "Detecting metrologically useful entanglement in the vicinity of Dicke states". *New J. Phys* 17.8 (2015), 083027.

[327] Manuel Gessner, Augusto Smerzi, and Luca Pezzè. "Metrological nonlinear squeezing parameter". *Phys. Rev. Lett.* 122.9 (2019), 090503.

[328] K Eckert, John Schliemann, D Bruß, and M Lewenstein. "Quantum correlations in systems of indistinguishable particles". *Annals of physics* 299.1 (2002), 88–127.

[329] Tsubasa Ichikawa, Toshihiko Sasaki, Izumi Tsutsui, and Nobuhiro Yonezawa. "Exchange symmetry and multipartite entanglement". *Phys. Rev. A* 78.5 (2008), 052105.

[330] Tzu-Chieh Wei. "Exchange symmetry and global entanglement and full separability". *Phys. Rev. A* 81.5 (2010), 054102.

[331] Xiaoguang Wang and Barry C Sanders. "Spin squeezing and pairwise entanglement for symmetric multiqubit states". *Phys. Rev. A* 68.1 (2003), 012101.

[332] Jaroslaw K Korbicz, J Ignacio Cirac, and Maciej Lewenstein. "Spin squeezing inequalities and entanglement of N qubit states". *Phys. Rev. Lett.* 95.12 (2005), 120502.

[333] Géza Tóth, Witlef Wieczorek, David Gross, Roland Krischek, Christian Schwemmer, and Harald Weinfurter. "Permutationally invariant quantum tomography". *Phys. Rev. Lett.* 105.25 (2010), 250403.

[334] Tobias Moroder, Philipp Hyllus, Géza Tóth, Christian Schwemmer, Alexander Niggebaum, Stefanie Gaile, Otfried Gühne, and Harald Weinfurter. "Permutationally invariant state reconstruction". *New J. Phys* 14.10 (2012), 105001.

[335] Christian Schwemmer, Géza Tóth, Alexander Niggebaum, Tobias Moroder, David Gross, Otfried Gühne, and Harald Weinfurter. "Experimental comparison of efficient tomography schemes for a six-qubit state". *Phys. Rev. Lett.* 113.4 (2014), 040503.

[336] Igor Jex, G Alber, SM Barnett, and A Delgado. "Antisymmetric multipartite quantum states and their applications". *Fortschritte der Physik: Progress of Physics* 51.2-3 (2003), 172–178.

[337] Adán Cabello. "Supersinglets". *Journal of Modern Optics* 50.6-7 (2003), 1049–1061.

[338] Aram W Harrow. "Applications of coherent classical communication and the Schur transform to quantum information theory". *arXiv preprint quant-ph/0512255* (2005).

[339] Enrico Sindici and Marco Piani. "Simple class of bound entangled states based on the properties of the antisymmetric subspace". *Phys. Rev. A* 97.3 (2018), 032319.

[340] Enrico Sindici. "Quantum correlations and exchange symmetry" (2019).

[341] Fabian Bernards and Otfried Gühne. "Multiparticle singlet states cannot be maximally entangled for the bipartitions". *arXiv preprint arXiv:2211.03813* (2022).

[342] Benjamin Yadin, Benjamin Morris, and Kay Brandner. "Thermodynamics of permutation-invariant quantum many-body systems: A group-theoretical framework". *Phys. Rev. Research* 5.3 (2023), 033018.

[343] Jasminder S Sidhu and Pieter Kok. "Geometric perspective on quantum parameter estimation". *AVS Quantum Science* 2.1 (2020).

[344] Sixia Yu. "Quantum Fisher information as the convex roof of variance". *arXiv preprint arXiv:1302.5311* (2013).

[345] Géza Tóth and Dénes Petz. "Extremal properties of the variance and the quantum Fisher information". *Phys. Rev. A* 87.3 (2013), 032324.

[346] Géza Tóth and Florian Fröwis. "Uncertainty relations with the variance and the quantum Fisher information based on convex decompositions of density matrices". *Phys. Rev. Research* 4.1 (2022), 013075.

[347] Tiberiu Popoviciu. "Sur les équations algébriques ayant toutes leurs racines réelles". *Mathematica* 9.129-145 (1935), 20.

[348] Rajendra Bhatia and Chandler Davis. "A better bound on the variance". *The american mathematical monthly* 107.4 (2000), 353–357.

[349] Rajesh Sharma. "Some more inequalities for arithmetic mean, harmonic mean and variance". *Journal of Mathematical Inequalities* 2.1 (2008), 109–114.

[350] Minh Cong Tran, Borivoje Dakić, Wiesław Laskowski, and Tomasz Paterek. "Correlations between outcomes of random measurements". *Phys. Rev. A* 94.4 (2016), 042302.

[351] H Aschauer, J Calsamiglia, M Hein, and H-J Briegel. "Local invariants for multi-partite entangled states allowing for a simple entanglement criterion". *Quantum Information and Computation* 4.383 (2004), 383.

[352] Nikolai Wyderka and Otfried Gühne. "Characterizing quantum states via sector lengths". *J. Phys. A* 53.34 (2020), 345302.

[353] Christopher Eltschka and Jens Siewert. "Maximum N-body correlations do not in general imply genuine multipartite entanglement". *Quantum* 4 (2020), 229.

[354] Daniel Miller. "Small quantum networks in the qudit stabilizer formalism". *arXiv preprint arXiv:1910.09551* (2019).

[355] Dagomir Kaszlikowski, Aditi Sen, Ujjwal Sen, Vlatko Vedral, Andreas Winter, et al. "Quantum correlation without classical correlations". *Phys. Rev. Lett.* 101.7 (2008), 070502.

[356] Wiesław Laskowski, Marcin Markiewicz, Tomasz Paterek, and Marcin Wieśniak. "Incompatible local hidden-variable models of quantum correlations". *Phys. Rev. A* 86.3 (2012), 032105.

[357] Christian Schwemmer, Lukas Knips, Minh Cong Tran, Anna De Rosier, Wiesław Laskowski, Tomasz Paterek, and Harald Weinfurter. "Genuine multipartite entanglement without multipartite correlations". *Phys. Rev. Lett.* 114.18 (2015), 180501.

[358] Minh Cong Tran, Margherita Zuppardo, Anna de Rosier, Lukas Knips, Wiesław Laskowski, Tomasz Paterek, and Harald Weinfurter. "Genuine N-partite entanglement without N-partite correlation functions". *Phys. Rev. A* 95.6 (2017), 062331.

[359] Waldemar Kłobus, Wiesław Laskowski, Tomasz Paterek, Marcin Wieśniak, and Harald Weinfurter. "Higher dimensional entanglement without correlations". *The European Physical Journal D* 73 (2019), 1–6.

[360] Nikolai Wyderka. "Learning from correlations: What parts of quantum states tell about the whole" (2020).

[361] A Robert Calderbank, Eric M Rains, Peter M Shor, and Neil JA Sloane. "Quantum error correction via codes over GF (4)". *IEEE Transactions on Information Theory* 44.4 (1998), 1369–1387.

[362] Eric M Rains. "Quantum shadow enumerators". *IEEE transactions on information theory* 45.7 (1999), 2361–2366.

[363] Eric M Rains. "Polynomial invariants of quantum codes". *IEEE Transactions on Information Theory* 46.1 (2000), 54–59.

[364] Christopher Eltschka, Felix Huber, Otfried Gühne, and Jens Siewert. "Exponentially many entanglement and correlation constraints for multipartite quantum states". *Phys. Rev. A* 98.5 (2018), 052317.

[365] Felix Michael Huber. "Quantum states and their marginals: from multipartite entanglement to quantum error-correcting codes" (2017).

[366] Yuriy Makhlin. "Nonlocal properties of two-qubit gates and mixed states, and the optimization of quantum computations". *Quantum Information Processing* 1 (2002), 243–252.

[367] Karol Bartkiewicz, Jiři Beran, Karel Lemr, Michał Norek, and Adam Miranowicz. "Quantifying entanglement of a two-qubit system via measurable and invariant moments of its partially transposed density matrix". *Phys. Rev. A* 91.2 (2015), 022323.

[368] Karol Bartkiewicz, Paweł Horodecki, Karel Lemr, Adam Miranowicz, and Karol Życzkowski. "Method for universal detection of two-photon polarization entanglement". *Phys. Rev. A* 91.3 (2015), 032315.

[369] Julia Kempe. "Multiparticle entanglement and its applications to cryptography". *Phys. Rev. A* 60.2 (1999), 910.

[370] Howard Barnum and Noah Linden. "Monotones and invariants for multiparticle quantum states". *Journal of Physics A: Mathematical and General* 34.35 (2001), 6787.

[371] Ali Saif M Hassan and Pramod S Joag. "On the degree conjecture for separability of multipartite quantum states". *Journal of mathematical physics* 49.1 (2008).

[372] Ali Saif M Hassan and Pramod S Joag. "Geometric measure for entanglement in N-qudit pure states". *Phys. Rev. A* 80.4 (2009), 042302.

[373] Minh Cong Tran, Borivoje Dakić, François Arnault, Wiesław Laskowski, and Tomasz Paterek. "Quantum entanglement from random measurements". *Phys. Rev. A* 92.5 (2015), 050301.

[374] Marcin Markiewicz, Wiesław Laskowski, Tomasz Paterek, and Marek Żukowski. "Detecting genuine multipartite entanglement of pure states with bipartite correlations". *Phys. Rev. A* 87.3 (2013), 034301.

[375] Claude Klöckl and Marcus Huber. "Characterizing multipartite entanglement without shared reference frames". *Phys. Rev. A* 91.4 (2015), 042339.

[376] Felix Huber and Simone Severini. "Some Ulam's reconstruction problems for quantum states". *J. Phys. A* 51.43 (2018), 435301.

[377] Daniel Miller, Daniel Loss, Ivano Tavernelli, Hermann Kampermann, Dagmar Bruß, and Nikolai Wyderka. "Sector length distributions of graph states". *arXiv preprint arXiv:2207.07665* (2022).

[378] Andreas Ketterer, Nikolai Wyderka, and Otfried Gühne. "Characterizing multipartite entanglement with moments of random correlations". *Phys. Rev. Lett.* 122.12 (2019), 120505.

[379] Andreas Ketterer, Nikolai Wyderka, and Otfried Gühne. "Entanglement characterization using quantum designs". *Quantum* 4 (2020), 325.

[380] Philippe Delsarte, Jean-Marie Goethals, and Johan Jacob Seidel. "Spherical codes and designs". *Geometry and Combinatorics*. Elsevier, 1991, 68–93.

[381] Eiichi Bannai and Etsuko Bannai. "A survey on spherical designs and algebraic combinatorics on spheres". *European Journal of Combinatorics* 30.6 (2009), 1392–1425.

[382] Charles J Colbourn. *CRC handbook of combinatorial designs*. CRC press, 2010.

[383] Paul D Seymour and Thomas Zaslavsky. "Averaging sets: a generalization of mean values and spherical designs". *Advances in Mathematics* 52.3 (1984), 213–240.

[384] Ronald H Hardin and Neil JA Sloane. "McLaren's improved snub cube and other new spherical designs in three dimensions". *Discrete & Computational Geometry* 15 (1996), 429–441.

[385] Joseph M Renes, Robin Blume-Kohout, Andrew J Scott, and Carlton M Caves. "Symmetric informationally complete quantum measurements". *Journal of Mathematical Physics* 45.6 (2004), 2171–2180.

[386] Andris Ambainis and Joseph Emerson. "Quantum t-designs: t-wise independence in the quantum world". *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007, 129–140.

[387] William K Wootters. "Statistical distance and Hilbert space". *Phys. Rev. D* 23.2 (1981), 357.

[388] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. "Stabilization of quantum computations by symmetrization". *SIAM Journal on Computing* 26.5 (1997), 1541–1557.

[389] Aram W Harrow. "The church of the symmetric subspace". *arXiv preprint arXiv:1308.6595* (2013).

[390] Fernando GSL Brandao, Matthias Christandl, Aram W Harrow, and Michael Walter. "The mathematics of entanglement". *arXiv preprint arXiv:1604.01790* (2016).

[391] Richard A Low. "Pseudo-randomness and learning in quantum computation". *arXiv preprint arXiv:1006.5227* (2010).

[392] Andreas Ketterer and Otfried Gühne. "Entropic uncertainty relations from quantum designs". *Phys. Rev. Research* 2.2 (2020), 023130.

[393] Lloyd Welch. "Lower bounds on the maximum cross correlation of signals (corresp.)" *IEEE Transactions on Information theory* 20.3 (1974), 397–399.

[394] Andreas Klappenecker and Martin Rotteler. "Mutually unbiased bases are complex projective 2-designs". *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* IEEE. 2005, 1740–1744.

[395] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. "On mutually unbiased bases". *International journal of quantum information* 8.04 (2010), 535–640.

[396] Mihály Weiner. "A gap for the maximum number of mutually unbiased bases". *Proceedings of the American Mathematical Society* 141.6 (2013), 1963–1969.

[397] ID Ivonovic. "Geometrical description of quantal state determination". *Journal of Physics A: Mathematical and General* 14.12 (1981), 3241.

[398] William K Wootters and Brian D Fields. "Optimal state-determination by mutually unbiased measurements". *Annals of Physics* 191.2 (1989), 363–381.

[399] M Wieśniak, Tomasz Paterek, and Anton Zeilinger. "Entanglement in mutually unbiased bases". *New J. Phys* 13.5 (2011), 053047.

[400] Ulrich Seyfarth and Kedar S Ranade. "Construction of mutually unbiased bases with cyclic symmetry for qubit systems". *Phys. Rev. A* 84.4 (2011), 042327.

[401] Gerhard Zauner. “Grundzüge einer nichtkommutativen Designtheorie”. *Ph. D. dissertation, PhD thesis* (1999).

[402] David Gross, Koenraad Audenaert, and Jens Eisert. “Evenly distributed unitaries: On the structure of unitary designs”. *Journal of Mathematical Physics* 48.5 (2007), 052104.

[403] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. “Exact and approximate unitary 2-designs and their application to fidelity estimation”. *Phys. Rev. A* 80.1 (2009), 012304.

[404] Andrew James Scott. “Optimizing quantum process tomography with unitary 2-designs”. *J. Phys. A* 41.5 (2008), 055308.

[405] Georg Köstenberger. “Weingarten calculus”. *arXiv preprint arXiv:2101.00921* (2021).

[406] Roy J Garcia, You Zhou, and Arthur Jaffe. “Quantum scrambling with classical shadows”. *Phys. Rev. Research* 3.3 (2021), 033155.

[407] Fernando GSL Brandão, Wissam Chemissany, Nicholas Hunter-Jones, Richard Kueng, and John Preskill. “Models of quantum complexity growth”. *PRX Quantum* 2.3 (2021), 030316.

[408] Nicholas Hunter-Jones and Junyu Liu. “Chaos and random matrices in supersymmetric SYK”. *Journal of High Energy Physics* 2018.5 (2018), 1–26.

[409] Aidan Roy and Andrew J Scott. “Unitary designs and codes”. *Designs, codes and cryptography* 53 (2009), 13–31.

[410] Zak Webb. “The Clifford group forms a unitary 3-design”. *arXiv preprint arXiv:1510.02769* (2015).

[411] Huangjun Zhu, Richard Kueng, Markus Grassl, and David Gross. “The Clifford group fails gracefully to be a unitary 4-design”. *arXiv preprint arXiv:1609.08172* (2016).

[412] Andreas Elben, Benoıt Vermersch, Marcello Dalmonte, J Ignacio Cirac, and Peter Zoller. “Rényi entropies from random quenches in atomic Hubbard and spin models”. *Phys. Rev. Lett.* 120.5 (2018), 050406.

[413] Tiff Brydges, Andreas Elben, Petar Jurcevic, Benoıt Vermersch, Christine Maier, Ben P Lanyon, Peter Zoller, Rainer Blatt, and Christian F Roos. “Probing Rényi entanglement entropy via randomized measurements”. *Science* 364.6437 (2019), 260–263.

[414] Andreas Elben, Benoıt Vermersch, Christian F Roos, and Peter Zoller. “Statistical correlations between locally randomized measurements: A toolbox for probing entanglement in many-body quantum states”. *Phys. Rev. A* 99.5 (2019), 052323.

[415] Andreas Elben et al. “Cross-platform verification of intermediate scale quantum devices”. *Phys. Rev. Lett.* 124.1 (2020), 010504.

[416] Zhenhuan Liu, Pei Zeng, You Zhou, and Mile Gu. "Characterizing correlation within multipartite quantum systems via local randomized measurements". *Phys. Rev. A* 105.2 (2022), 022407.

[417] Andreas Elben, Steven T Flammia, Hsin-Yuan Huang, Richard Kueng, John Preskill, Benoıt Vermersch, and Peter Zoller. "The randomized measurement toolbox". *Nature Reviews Physics* 5.1 (2023), 9–24.

[418] Steven J van Enk and Carlo WJ Beenakker. "Measuring Tr ρ n on single copies of ρ using random measurements". *Phys. Rev. Lett.* 108.11 (2012), 110503.

[419] Lukas Knips, Jan Dziewior, Waldemar Kłobus, Wiesław Laskowski, Tomasz Paterek, Peter J Shadbolt, Harald Weinfurter, and Jasmin DA Meinecke. "Multipartite entanglement analysis from random correlations". *npj Quantum Information* 6.1 (2020), 51.

[420] AR Usha Devi, R Prabhu, and AK Rajagopal. "Characterizing multiparticle entanglement in symmetric N-qubit states via negativity of covariance matrices". *Phys. Rev. Lett.* 98.6 (2007), 060501.

[421] Robert Lohmayer, Andreas Osterloh, Jens Siewert, and Armin Uhlmann. "Entangled three-qubit states without concurrence and three-tangle". *Phys. Rev. Lett.* 97.26 (2006), 260502.

[422] Szilárd Szalay. "Separability criteria for mixed three-qubit states". *Phys. Rev. A* 83.6 (2011), 062337.

[423] Zhi-Hua Chen, Zhi-Hao Ma, Otfried Gühne, and Simone Severini. "Estimating entanglement monotones with a generalization of the Wootters formula". *Phys. Rev. Lett.* 109.20 (2012), 200503.

[424] Bastian Jungnitsch, Tobias Moroder, and Otfried Gühne. "Taming multiparticle entanglement". *Phys. Rev. Lett.* 106.19 (2011), 190502.

[425] Marcus Huber, Florian Mintert, Andreas Gabriel, and Beatrix C Hiesmayr. "Detection of high-dimensional genuine multipartite entanglement of mixed states". *Phys. Rev. Lett.* 104.21 (2010), 210501.

[426] Michael Krebsbach. "Characterization of bipartite entanglement with moments of randomized measurements". PhD thesis. Bachelorarbeit, Universität Freiburg, 2019, 2019.

[427] Paul G Kwiat, Edo Waks, Andrew G White, Ian Appelbaum, and Philippe H Eberhard. "Ultrabright source of polarization-entangled photons". *Phys. Rev. A* 60.2 (1999), R773.

[428] Gabriel Horacio Aguilar, Stephen Patrick Walborn, PH Souto Ribeiro, and Lucas Chibebe Céleri. "Experimental determination of multipartite entanglement with incomplete information". *Phys. Rev. X* 5.3 (2015), 031042.

[429] Shuheng Liu, Qiongyi He, Marcus Huber, Otfried Gühne, and Giuseppe Vitagliano. "Characterizing entanglement dimensionality from randomized measurements". *PRX Quantum* 4.2 (2023), 020324.

[430] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". *Quantum* 4 (2020), 337.

[431] Rolando D Somma, John Chiaverini, and Dana J Berkeland. "Lower bounds for the fidelity of entangled-state preparation". *Phys. Rev. A* 74.5 (2006), 052302.

[432] Robin Blume-Kohout. "Optimal, reliable estimation of quantum states". *New J. Phys* 12.4 (2010), 043034.

[433] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. "Quantum state tomography via compressed sensing". *Phys. Rev. Lett.* 105.15 (2010), 150401.

[434] Steven T Flammia and Yi-Kai Liu. "Direct fidelity estimation from few Pauli measurements". *Phys. Rev. Lett.* 106.23 (2011), 230501.

[435] Scott Aaronson. "Shadow tomography of quantum states". *Proceedings of the 50th annual ACM SIGACT symposium on theory of computing*. 2018, 325–338.

[436] Juan Carrasquilla, Giacomo Torlai, Roger G Melko, and Leandro Aolita. "Reconstructing quantum states with generative models". *Nature Machine Intelligence* 1.3 (2019), 155–161.

[437] Marco Paini, Amir Kalev, Dan Padilha, and Brendan Ruck. "Estimating expectation values using approximate quantum states". *Quantum* 5 (2021), 413.

[438] Hsin-Yuan Huang, Richard Kueng, and John Preskill. "Predicting many properties of a quantum system from very few measurements". *Nature Physics* 16.10 (2020), 1050–1057.

[439] Benoıt Vermersch, Andreas Elben, Marcello Dalmonte, J Ignacio Cirac, and Peter Zoller. "Unitary n-designs via random quenches in atomic Hubbard and spin models: Application to the measurement of Rényi entropies". *Phys. Rev. A* 97.2 (2018), 023604.

[440] Chao Song et al. "Generation of multicomponent atomic Schrödinger cat states of up to 20 qubits". *Science* 365.6453 (2019), 574–577.

[441] Ken X Wei, Isaac Lauer, Srikanth Srinivasan, Neereja Sundaresan, Douglas T McClure, David Toyli, David C McKay, Jay M Gambetta, and Sarah Sheldon. "Verifying multipartite entangled Greenberger-Horne-Zeilinger states via multiple quantum coherences". *Phys. Rev. A* 101.3 (2020), 032343.

[442] Ahmed Omran et al. "Generation and manipulation of Schrödinger cat states in Rydberg atom arrays". *Science* 365.6453 (2019), 570–574.

[443] Tobias Nauck. "Statistical characterization of multipartite entanglement based on finite samples of randomized measurements". PhD thesis. Bachelorarbeit, Universität Freiburg, 2020.

[444] RB Potts. "Note on the factorial moments of standard distributions". *Australian Journal of Physics* 6.4 (1953), 498–499.

[445] Sophia Ohnemus, Heinz-Peter Breuer, and Andreas Ketterer. "Quantifying multiparticle entanglement with randomized measurements". *Phys. Rev. A* 107.4 (2023), 042406.

[446] Sophia Ohnemus. "Probing multiparticle correlations in random quantum circuits with randomized measurements". *Masterarbeit, Universität Freiburg* (2021).

[447] Jacob L Beckey, N Gigena, Patrick J Coles, and M Cerezo. "Computable and operationally meaningful multipartite entanglement measures". *Phys. Rev. Lett.* 127.14 (2021), 140501.

[448] Louis Schatzki, Guangkuo Liu, Marco Cerezo, and Eric Chitambar. "A hierarchy of multipartite correlations based on concentratable entanglement". *arXiv preprint arXiv:2209.07607* (2022).

[449] Jacob L Beckey, Gerard Pelegrí, Steph Foulds, and Natalie J Pearson. "Multipartite entanglement measures via Bell-basis measurements". *Phys. Rev. A* 107.6 (2023), 062425.

[450] John Goold, Marcus Huber, Arnau Riera, Lídia Del Rio, and Paul Skrzypczyk. "The role of quantum information in thermodynamics—a topical review". *J. Phys. A* 49.14 (2016), 143001.

[451] Amit Mukherjee, Arup Roy, Some Sankar Bhattacharya, and Manik Banik. "Presence of quantum correlations results in a nonvanishing ergotropic gap". *Phys. Rev. E* 93.5 (2016), 052140.

[452] Mir Alimuddin, Tamal Guha, and Preeti Parashar. "Bound on ergotropic gap for bipartite separable states". *Phys. Rev. A* 99.5 (2019), 052320.

[453] David Edward Bruschi, Martí Perarnau-Llobet, Nicolai Friis, Karen V Hovhannisyan, and Marcus Huber. "Thermodynamics of creating correlations: Limitations and optimal protocols". *Phys. Rev. E* 91.3 (2015), 032118.

[454] Martí Perarnau-Llobet, Karen V Hovhannisyan, Marcus Huber, Paul Skrzypczyk, Nicolas Brunner, and Antonio Acín. "Extractable work from correlations". *Phys. Rev. X* 5.4 (2015), 041011.

[455] Marcus Huber, Martí Perarnau-Llobet, Karen V Hovhannisyan, Paul Skrzypczyk, Claude Klöckl, Nicolas Brunner, and Antonio Acín. "Thermodynamic cost of creating correlations". *New J. Phys* 17.6 (2015), 065008.

[456] Nicolai Friis, Marcus Huber, and Martí Perarnau-Llobet. "Energetics of correlations in interacting systems". *Phys. Rev. E* 93.4 (2016), 042135.

[457] Matteo Brunelli, Marco G Genoni, Marco Barbieri, and Mauro Paternostro. "Detecting Gaussian entanglement via extractable work". *Phys. Rev. A* 96.6 (2017), 062311.

[458] Emma McKay, Nayeli A Rodríguez-Briones, and Eduardo Martín-Martı ´nez. "Fluctuations of work cost in optimal generation of correlations". *Phys. Rev. E* 98.3 (2018), 032132.

[459] Nicolas Brunner, Marcus Huber, Noah Linden, Sandu Popescu, Ralph Silva, and Paul Skrzypczyk. "Entanglement enhances cooling in microscopic quantum refrigerators". *Phys. Rev. E* 89.3 (2014), 032115.

[460] Jonatan Bohr Brask, Géraldine Haack, Nicolas Brunner, and Marcus Huber. "Autonomous quantum thermal machine for generating steady-state entanglement". *New J. Phys* 17.11 (2015), 113029.

[461] Francesco Campaioli, Felix A Pollock, and Sai Vinjanampathy. "Quantum batteries". *Thermodynamics in the Quantum Regime: Fundamental Aspects and New Directions* (2018), 207–225.

[462] Robert Alicki and Mark Fannes. "Entanglement boost for extractable work from ensembles of quantum batteries". *Phys. Rev. E* 87.4 (2013), 042123.

[463] Karen V Hovhannisyan, Martí Perarnau-Llobet, Marcus Huber, and Antonio Acín. "Entanglement generation is not necessary for optimal work extraction". *Phys. Rev. Lett.* 111.24 (2013), 240401.

[464] Raffaele Salvia, Giacomo De Palma, and Vittorio Giovannetti. "Optimal local work extraction from bipartite quantum systems in the presence of Hamiltonian couplings". *Phys. Rev. A* 107.1 (2023), 012405.

[465] Felix C Binder, Sai Vinjanampathy, Kavan Modi, and John Goold. "Quantacell: powerful charging of quantum batteries". *New J. Phys* 17.7 (2015), 075015.

[466] Francesco Campaioli, Felix A Pollock, Felix C Binder, Lucas Céleri, John Goold, Sai Vinjanampathy, and Kavan Modi. "Enhancing the charging power of quantum batteries". *Phys. Rev. Lett.* 118.15 (2017), 150601.

[467] Nicolai Friis and Marcus Huber. "Precision and work fluctuations in Gaussian battery charging". *Quantum* 2 (2018), 61.

[468] Thao P Le, Jesper Levinsen, Kavan Modi, Meera M Parish, and Felix A Pollock. "Spin-chain model of a many-body quantum battery". *Phys. Rev. A* 97.2 (2018), 022106.

[469] Dario Ferraro, Michele Campisi, Gian Marcello Andolina, Vittorio Pellegrini, and Marco Polini. "High-power collective charging of a solid-state quantum battery". *Phys. Rev. Lett.* 120.11 (2018), 117702.

[470] Gian Marcello Andolina, Maximilian Keck, Andrea Mari, Michele Campisi, Vittorio Giovannetti, and Marco Polini. "Extractable work, the role of correlations, and asymptotic freedom in quantum batteries". *Phys. Rev. Lett.* 122.4 (2019), 047702.

[471] Sergi Julià-Farré, Tymoteusz Salamon, Arnau Riera, Manabendra N Bera, and Maciej Lewenstein. "Bounds on the capacity and power of quantum batteries". *Phys. Rev. Research* 2.2 (2020), 023113.

[472] James Q Quach and William J Munro. "Using dark states to charge and stabilize open quantum batteries". *Phys. Rev. Applied* 14.2 (2020), 024092.

[473] Ju-Yeon Gyhm, Dominik Šafránek, and Dario Rosa. "Quantum charging advantage cannot be extensive without global operations". *Phys. Rev. Lett.* 128.14 (2022), 140501.

[474] James Q Quach et al. "Superabsorption in an organic microcavity: Toward a quantum battery". *Science advances* 8.2 (2022), eabk3160.

[475] Chang-Kang Hu et al. "Optimal charging of a superconducting quantum battery". *Quantum Science and Technology* 7.4 (2022), 045018.

[476] Ignacio García-Mata, Augusto J Roncaglia, and Diego A Wisniacki. "Quantum-to-classical transition in the work distribution for chaotic systems". *Phys. Rev. E* 95.5 (2017), 050102.

[477] Marcin Łobejko, Jerzy Łuczka, and Peter Talkner. "Work distributions for random sudden quantum quenches". *Phys. Rev. E* 95.5 (2017), 052137.

[478] Aurélia Chenu, Iñigo L Egusquiza, Javier Molina-Vilaplana, and Adolfo del Campo. "Quantum work statistics, Loschmidt echo and information scrambling". *Scientific reports* 8.1 (2018), 12634.

[479] Aurélia Chenu, Javier Molina-Vilaplana, and Adolfo Del Campo. "Work statistics, loschmidt echo and information scrambling in chaotic quantum systems". *Quantum* 3 (2019), 127.

[480] Raffaele Salvia and Vittorio Giovannetti. "On the distribution of the mean energy in the unitary orbit of quantum states". *Quantum* 5 (2021), 514.

[481] Francesco Caravelli, Ghislaine Coulter-De Wit, Luis Pedro García-Pintos, and Alioscia Hamma. "Random quantum batteries". *Phys. Rev. Research* 2.2 (2020), 023095.

[482] Salvatore Francesco Emanuele Oliviero, Lorenzo Leone, Francesco Caravelli, and Alioscia Hamma. "Random matrix theory of the isospectral twirling". *SciPost Physics* 10.3 (2021), 076.

[483] Giuseppe Gennaro, Giuliano Benenti, and G Massimo Palma. "Relaxation due to random collisions with a many-qudit environment". *Phys. Rev. A* 79.2 (2009), 022105.

[484] Gabriele De Chiara and Mauro Antezza. "Quantum machines powered by correlated baths". *Phys. Rev. Research* 2.3 (2020), 033315.

[485] Vahid Shaghaghi, G Massimo Palma, and Giuliano Benenti. "Extracting work from random collisions: A model of a quantum heat engine". *Phys. Rev. E* 105.3 (2022), 034101.

[486] Davide Rossini, Gian Marcello Andolina, Dario Rosa, Matteo Carrega, and Marco Polini. "Quantum advantage in the charging process of Sachdev-Ye-Kitaev batteries". *Phys. Rev. Lett.* 125.23 (2020), 236402.

[487] Dario Rosa, Davide Rossini, Gian Marcello Andolina, Marco Polini, and Matteo Carrega. "Ultra-stable charging of fast-scrambling SYK quantum batteries". *Journal of High Energy Physics* 2020.11 (2020), 1–29.

[488] Yiyang Jia and Jacobus JM Verbaarschot. "Spectral fluctuations in the Sachdev-Ye-Kitaev model". *Journal of High Energy Physics* 2020.7 (2020), 1–59.

[489] Armen E Allahverdyan, Roger Balian, and Th M Nieuwenhuizen. "Maximal work extraction from finite quantum systems". *Europhysics Letters* 67.4 (2004), 565.

[490] Gianluca Francica, John Goold, Francesco Plastina, and Mauro Paternostro. "Daemonic ergotropy: enhanced work extraction from quantum correlations". *npj Quantum Information* 3.1 (2017), 12.

[491] Fabian Bernards, Matthias Kleinmann, Otfried Gühne, and Mauro Paternostro. "Daemonic ergotropy: Generalised measurements and multipartite settings". *Entropy* 21.8 (2019), 771.

[492] Gianluca Francica. "Quantum correlations and ergotropy". *Phys. Rev. E* 105.5 (2022), L052101.

[493] Roe Goodman and Nolan R Wallach. *Representations and invariants of the classical groups*. Cambridge University Press, 2000.

[494] Martin Kliesch and Ingo Roth. "Theory of quantum system certification". *PRX quantum* 2.1 (2021), 010201.

[495] Jens Siewert. "On orthogonal bases in the Hilbert-Schmidt space of matrices". *Journal of Physics Communications* 6.5 (2022), 055014.

[496] J Sperling and W Vogel. "Determination of the Schmidt number". *Phys. Rev. A* 83.4 (2011), 042315.

[497] J Sperling and W Vogel. "The Schmidt number as a universal entanglement measure". *Physica Scripta* 83.4 (2011), 045002.

[498] Marcus Huber, Ludovico Lami, Cécilia Lancien, and Alexander Müller-Hermes. "High-dimensional entanglement in states with positive partial transposition". *Phys. Rev. Lett.* 121.20 (2018), 200503.

[499] Shuheng Liu, Matteo Fadel, Qiongyi He, Marcus Huber, and Giuseppe Vitagliano. "Bounding entanglement dimensionality from the covariance matrix". *arXiv preprint arXiv:2208.04909* (2022).

[500] Peter Talkner, Eric Lutz, and Peter Hänggi. "Fluctuation theorems: Work is not an observable". *Phys. Rev. E* 75.5 (2007), 050102.

[501] Massimiliano Esposito, Upendra Harbola, and Shaul Mukamel. "Nonequilibrium fluctuations, fluctuation theorems, and counting statistics in quantum systems". *Rev. Mod. Phys* 81.4 (2009), 1665.

[502] Michele Campisi, Peter Hänggi, and Peter Talkner. "Colloquium: Quantum fluctuation relations: Foundations and applications". *Rev. Mod. Phys* 83.3 (2011), 771.

[503] Augusto J Roncaglia, Federico Cerisola, and Juan Pablo Paz. "Work measurement as a generalized quantum measurement". *Phys. Rev. Lett.* 113.25 (2014), 250601.

[504] Tiago Debarba, Gonzalo Manzano, Yelena Guryanova, Marcus Huber, and Nicolai Friis. "Work estimation and work fluctuations in the presence of non-ideal measurements". *New J. Phys* 21.11 (2019), 113002.

[505] Gabriele De Chiara, Augusto J Roncaglia, and Juan Pablo Paz. "Measuring work and heat in ultracold quantum gases". *New J. Phys* 17.3 (2015), 035004.

[506] Peter Talkner and Peter Hänggi. "Aspects of quantum work". *Phys. Rev. E* 93.2 (2016), 022131.

[507] Martí Perarnau-Llobet, Elisa Bäumer, Karen V Hovhannisyan, Marcus Huber, and Antonio Acin. "No-go theorem for the characterization of work fluctuations in coherent quantum systems". *Phys. Rev. Lett.* 118.7 (2017), 070601.

[508] Elisa Bäumer, Matteo Lostaglio, Martí Perarnau-Llobet, and Rui Sampaio. "Fluctuating work in coherent quantum systems: Proposals and limitations". *Thermodynamics in the Quantum Regime: Fundamental Aspects and New Directions* (2018), 275–300.

[509] Gabriele De Chiara, Paolo Solinas, Federico Cerisola, and Augusto J Roncaglia. "Ancilla-assisted measurement of quantum work". *Thermodynamics in the Quantum Regime: Fundamental Aspects and New Directions* (2018), 337–362.

[510] Matteo Lostaglio. "Quantum fluctuation theorems, contextuality, and work quasiprobabilities". *Phys. Rev. Lett.* 120.4 (2018), 040602.

[511] Adam Bednorz and Wolfgang Belzig. "Quasiprobabilistic interpretation of weak measurements in mesoscopic junctions". *Phys. Rev. Lett.* 105.10 (2010), 106803.

[512] Yelena Guryanova, Nicolai Friis, and Marcus Huber. "Ideal projective measurements have infinite resource costs". *Quantum* 4 (2020), 222.

[513] Paweł Horodecki. "Measuring quantum entanglement without prior state reconstruction". *Phys. Rev. Lett.* 90.16 (2003), 167901.

[514] Fabio Antonio Bovino, Giuseppe Castagnoli, Artur Ekert, Paweł Horodecki, Carolina Moura Alves, and Alexander Vladimir Sergienko. "Direct measurement of nonlinear properties of bipartite quantum states". *Phys. Rev. Lett.* 95.24 (2005), 240407.

[515] Hilary A Carteret. "Noiseless quantum circuits for the Peres separability criterion". *Phys. Rev. Lett.* 94.4 (2005), 040502.

[516] Christian Schmid, Nikolai Kiesel, Witlef Wieczorek, Harald Weinfurter, Florian Mintert, and Andreas Buchleitner. "Experimental direct observation of mixed state entanglement". *Phys. Rev. Lett.* 101.26 (2008), 260505.

[517] Florian Mintert, Marek Kuś, and Andreas Buchleitner. "Concurrence of mixed multipartite quantum states". *Phys. Rev. Lett.* 95.26 (2005), 260502.

[518] Leandro Aolita and Florian Mintert. "Measuring multipartite concurrence with a single factorizable observable". *Phys. Rev. Lett.* 97.5 (2006), 050501.

[519] Florian Mintert and Andreas Buchleitner. "Observable entanglement measure for mixed quantum states". *Phys. Rev. Lett.* 98.14 (2007), 140505.

[520] SP Walborn, PH Souto Ribeiro, L Davidovich, F Mintert, and A Buchleitner. "Experimental determination of entanglement by a projective measurement". *Phys. Rev. A* 75.3 (2007), 032338.

[521] Dvir Kafri and Sebastian Deffner. "Holevo's bound from a general quantum fluctuation theorem". *Phys. Rev. A* 86.4 (2012), 044302.

[522] Bartłomiej Gardas and Sebastian Deffner. "Quantum fluctuation theorem for error diagnostics in quantum annealers". *Scientific reports* 8.1 (2018), 17191.

[523] Yoshihiko Hasegawa. "Quantum thermodynamic uncertainty relation for continuous measurement". *Phys. Rev. Lett.* 125.5 (2020), 050601.

[524] Yoshihiko Hasegawa. "Thermodynamic uncertainty relation for general open quantum systems". *Phys. Rev. Lett.* 126.1 (2021), 010602.

[525] Konrad Banaszek, Andrzej Dragan, Wojciech Wasilewski, and Czesław Radzewicz. "Experimental demonstration of entanglement-enhanced classical communication over a quantum channel with correlated noise". *Phys. Rev. Lett.* 92.25 (2004), 257901.

[526] Dominik Šafránek, Mehdi Ahmadi, and Ivette Fuentes. "Quantum parameter estimation with imperfect reference frames". *New J. Phys* 17.3 (2015), 033012.

[527] Mehdi Ahmadi, Alexander RH Smith, and Andrzej Dragan. "Communication between inertial observers with partially correlated reference frames". *Phys. Rev. A* 92.6 (2015), 062319.

[528] Dong Xie, Chunling Xu, and An Min Wang. "Quantum metrology in coarsened measurement reference". *Phys. Rev. A* 95.1 (2017), 012117.

[529] Marco Fanizza, Matteo Rosati, Michalis Skotiniotis, John Calsamiglia, and Vittorio Giovannetti. "Squeezing-enhanced communication without a phase reference". *Quantum* 5 (2021), 608.

[530] Wojciech Górecki, Alberto Riccardi, and Lorenzo Maccone. "Quantum metrology of noisy spreading channels". *Phys. Rev. Lett.* 129.24 (2022), 240503.

[531] Joseph Emerson, Robert Alicki, and Karol Życzkowski. "Scalable noise estimation with random unitary operators". *Journal of Optics B: Quantum and Semiclassical Optics* 7.10 (2005), S347.

[532] Xiaoguang Wang and Klaus Mølmer. "Pairwise entanglement in symmetric multi-qubit systems". *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics* 18.3 (2002), 385–391.

[533] Marcin Płodzień, Maciej Lewenstein, Emilia Witkowska, and Jan Chwedeńczuk. "One-axis twisting as a method of generating many-body Bell correlations". *Phys. Rev. Lett.* 129.25 (2022), 250402.

[534] S Choi and B Sundaram. "Bose-Einstein condensate as a nonlinear Ramsey interferometer operating beyond the Heisenberg limit". *Phys. Rev. A* 77.5 (2008), 053613.

[535] Bernd Lücke et al. "Twin matter waves for interferometry beyond the classical limit". *Science* 334.6057 (2011), 773–776.

[536] N David Mermin. "Extreme quantum entanglement in a superposition of macroscopically distinct states". *Phys. Rev. Lett.* 65.15 (1990), 1838.

[537] SM Roy. "Multipartiteseparability inequalities exponentially stronger than local reality inequalities". *Phys. Rev. Lett.* 94.1 (2005), 010402.

[538] Mariami Gachechiladze, Costantino Budroni, and Otfried Gühne. "Extreme violation of local realism in quantum hypergraph states". *Phys. Rev. Lett.* 116.7 (2016), 070401.

[539] Géza Tóth, Tamás Vértesi, Paweł Horodecki, and Ryszard Horodecki. "Activating hidden metrological usefulness". *Phys. Rev. Lett.* 125.2 (2020), 020402.

[540] Róbert Trényi, Árpád Lukács, Paweł Horodecki, Ryszard Horodecki, Tamás Vértesi, and Géza Tóth. "Multicopy metrology with many-particle quantum states". *arXiv preprint arXiv:2203.05538* (2022).

[541] J Hald, JL Sørensen, Christian Schori, and ES Polzik. "Spin squeezed atoms: a macroscopic entangled ensemble created by light". *Phys. Rev. Lett.* 83.7 (1999), 1319.

[542] V Meyer, MA Rowe, David Kielpinski, CA Sackett, Wayne M Itano, C Monroe, and David J Wineland. "Experimental demonstration of entanglement-enhanced rotation angle estimation using trapped ions". *Phys. Rev. Lett.* 86.26 (2001), 5870.

[543] Christoph Dankert. "Efficient simulation of random quantum states and operators". *arXiv preprint quant-ph/0512217* (2005).

[544] AR Usha Devi, MS Uma, R Prabhu, and AK Rajagopal. "Constraints on the uncertainties of entangled symmetric qubits". *Physics Letters A* 364.3-4 (2007), 203–207.

[545] N Behbood, F Martin Ciurana, G Colangelo, M Napolitano, Géza Tóth, RJ Sewell, and MW Mitchell. "Generation of macroscopic singlet states in a cold atomic ensemble". *Phys. Rev. Lett.* 113.9 (2014), 093601.

[546] Jia Kong, Ricardo Jiménez-Martínez, Charikleia Troullinou, Vito Giovanni Lucivero, Géza Tóth, and Morgan W Mitchell. "Measurement-induced, spatially-extended entanglement in a hot, strongly-interacting atomic system". *Nat. Commun* 11.1 (2020), 2415.

[547] Géza Tóth, Witlef Wieczorek, Roland Krischek, Nikolai Kiesel, Patrick Michelberger, and Harald Weinfurter. "Practical methods for witnessing genuine multi-qubit entanglement in the vicinity of symmetric states". *New J. Phys* 11.8 (2009), 083002.

[548] Leon Mirsky. "A trace inequality of John von Neumann". *Monatshefte für mathematik* 79 (1975), 303–306.

[549] Karsten Lange, Jan Peise, Bernd Lücke, Ilka Kruse, Giuseppe Vitagliano, Iagoba Apellaniz, Matthias Kleinmann, Géza Tóth, and Carsten Klempt. "Entanglement between two spatially separated atomic modes". *Science* 360.6387 (2018), 416–418.

[550] Matteo Fadel, Tilman Zibold, Boris Décamps, and Philipp Treutlein. "Spatial entanglement patterns and Einstein-Podolsky-Rosen steering in Bose-Einstein condensates". *Science* 360.6387 (2018), 409–413.

[551] Philipp Kunkel, Maximilian Prüfer, Helmut Strobel, Daniel Linnemann, Anika Frölian, Thomas Gasenzer, Martin Gärttner, and Markus K Oberthaler. "Spatially distributed multipartite entanglement enables EPR steering of atomic clouds". *Science* 360.6387 (2018), 413–416.

[552] DK Shin, BM Henson, SS Hodgman, Tomasz Wasak, Jan Chwedeńczuk, and AG Truscott. "Bell correlations between spatially separated pairs of atoms". *Nat. Commun.* 10.1 (2019), 4447.

[553] Matteo Fadel, Benjamin Yadin, Yuping Mao, Tim Byrnes, and Manuel Gessner. "Multiparameter quantum metrology and mode entanglement with spatially split nonclassical spin ensembles". *New J. Phys* (2023).

[554] Giuseppe Vitagliano, Matteo Fadel, Iagoba Apellaniz, Matthias Kleinmann, Bernd Lücke, Carsten Klempt, and Géza Tóth. "Number-phase uncertainty relations and bipartite entanglement detection in spin ensembles". *Quantum* 7 (2023), 914.

[555] Naum Ilich Akhiezer. *The classical moment problem and some related questions in analysis*. SIAM, 2020.

[556] Jean Bernard Lasserre. *Moments, positive polynomials and their applications*. Vol. 1. World Scientific, 2009.

[557] Konrad Schmüdgen and Konrad Schmüdgen. "The moment problem on compact semi-algebraic sets". *The Moment Problem* (2017), 283–313.

[558] Jean B Lasserre. "Global optimization with polynomials and the problem of moments". *SIAM Journal on optimization* 11.3 (2001), 796–817.

[559] Pablo A Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. California Institute of Technology, 2000.

[560] Gemma De las Cuevas, Tobias Fritz, and Tim Netzer. "Optimal bounds on the positivity of a matrix from a few moments". *Communications in Mathematical Physics* 375.1 (2020), 105–126.

[561] Rajendra Bhatia. *Matrix analysis*. Vol. 169. Springer Science & Business Media, 2013.

[562] Dominic W Berry and Barry C Sanders. "Bounds on general entropy measures". *Journal of Physics A: Mathematical and General* 36.49 (2003), 12255.

[563] Niels Henrik Abel. *Mémoire sur les équations algébriques, où on demontre l'impossibilité de la résolution de l'équation générale du cinquième dégré*. 1824.

[564] Antoine Neven et al. "Symmetry-resolved entanglement detection using partial transpose moments". *npj Quantum Information* 7.1 (2021), 152.

[565] Karol Życzkowski, Karol A Penson, Ion Nechita, and Benoit Collins. "Generating random density matrices". *Journal of Mathematical Physics* 52.6 (2011).

[566] Tinggui Zhang, Naihuan Jing, and Shao-Ming Fei. "Quantum separability criteria based on realignment moments". *Quantum Information Processing* 21.8 (2022), 276.

[567] Shruti Aggarwal, Satyabrata Adhikari, and AS Majumdar. "Entanglement detection in arbitrary dimensional bipartite quantum systems through partial realigned moments". *arXiv preprint arXiv:2302.04797* (2023).

[568] Ke-Ke Wang, Zhi-Wei Wei, and Shao-Ming Fei. "Operational entanglement detection based on Λ-moments". *The European Physical Journal Plus* 137.12 (2022), 1378.

[569] Lin Zhang, Ming-Jing Zhao, Lin Chen, Hua Xiang, and Yi Shen. "A Characterization of Entangled Two-Qubit States via Partial-Transpose-Moments". *Annalen der Physik* 534.11 (2022), 2200289.

[570] Junjun Duan, Lin Zhang, Quan Qian, and Shao-Ming Fei. "A characterization of maximally entangled two-qubit states". *Entropy* 24.2 (2022), 247.

[571] Mazhar Ali. "Partial transpose moments, principal minors and entanglement detection". *Quantum Information Processing* 22.5 (2023), 207.

[572] Lin Zhang, Yi Shen, Hua Xiang, Quan Qian, and Bo Li. "Visualization of all two-qubit states via partial-transpose moments". *Phys. Rev. A* 108.1 (2023), 012414.

[573] Jose Carrasco, Matteo Votto, Vittorio Vitale, Christian Kokail, Antoine Neven, Peter Zoller, Benoıt Vermersch, and Barbara Kraus. "Entanglement phase diagrams from partial transpose moments". *arXiv preprint arXiv:2212.10181* (2022).

[574] Gerald B Folland. "How to integrate a polynomial over a sphere". *The American Mathematical Monthly* 108.5 (2001), 446–448.

[575] Felix Bloch. "Nuclear induction". *Phys. Rev.* 70.7-8 (1946), 460.

[576] Karol Życzkowski, Paweł Horodecki, Anna Sanpera, and Maciej Lewenstein. "Volume of the set of separable states". *Phys. Rev. A* 58.2 (1998), 883.

[577] Omar Gamel. "Entangled Bloch spheres: Bloch matrix and two-qubit state space". *Phys. Rev. A* 93.6 (2016), 062320.

[578] BC Hiesmayr, F Hipp, M Huber, Ph Krammer, and Ch Spengler. "Simplex of bound entangled multipartite qubit states". *Phys. Rev. A* 78.4 (2008), 042327.

[579] John Martin, Olivier Giraud, PA Braun, Daniel Braun, and Thierry Bastin. "Multiqubit symmetric states with high geometric entanglement". *Phys. Rev. A* 81.6 (2010), 062347.

[580] Noah Linden, Sandu Popescu, and WK Wootters. "Almost every pure state of three qubits is completely determined by its two-particle reduced density matrices". *Phys. Rev. Lett.* 89.20 (2002), 207901.

[581] Felix Huber and Nikolai Wyderka. "Refuting spectral compatibility of quantum marginals". *arXiv preprint arXiv:2211.06349* (2022).

[582] Lajos Diósi. "Three-party pure quantum states are determined by two two-party reduced states". *Phys. Rev. A* 70.1 (2004), 010302.

[583] Nick S Jones and Noah Linden. "Parts of quantum states". *Phys. Rev. A* 71.1 (2005), 012324.

[584] Lars Erik Würflinger, Jean-Daniel Bancal, Antonio Acín, Nicolas Gisin, and Tamás Vértesi. "Nonlocal multipartite correlations from local marginal probabilities". *Phys. Rev. A* 86.3 (2012), 032117.

[585] Adam Sawicki, Michael Walter, and Marek Kuś. "When is a pure state of three qubits determined by its single-particle reduced density matrices?" *J. Phys. A* 46.5 (2013), 055304.

[586] Michael Walter, Brent Doran, David Gross, and Matthias Christandl. "Entanglement polytopes: multiparticle entanglement from single-particle information". *Science* 340.6137 (2013), 1205–1208.

[587] Nikolai Miklin, Tobias Moroder, and Otfried Gühne. "Multiparticle entanglement as an emergent phenomenon". *Phys. Rev. A* 93.2 (2016), 020104.

[588] Nikolai Wyderka, Felix Huber, and Otfried Gühne. "Almost all four-particle pure states are determined by their two-body marginals". *Phys. Rev. A* 96.1 (2017), 010102.

[589] Simon Morelli, Claude Klöckl, Christopher Eltschka, Jens Siewert, and Marcus Huber. "Dimensionally sharp inequalities for the linear entropy". *Linear Algebra and its Applications* 584 (2020), 294–325.

[590] Simon Morelli, Christopher Eltschka, Marcus Huber, and Jens Siewert. "Correlation constraints and the Bloch geometry of two qubits". *arXiv preprint arXiv:2303.11400* (2023).

[591] Leonid Mandelstam and IG Tamm. "The uncertainty relation between energy and time in non-relativistic quantum mechanics". *Selected papers*. Springer, 1991, 115–123.

[592] Philip J Jones and Pieter Kok. "Geometric derivation of the quantum speed limit". *Phys. Rev. A* 82.2 (2010), 022107.

[593] Adolfo del Campo, Inigo L Egusquiza, Martin B Plenio, and Susana F Huelga. "Quantum speed limits in open system dynamics". *Phys. Rev. Lett.* 110.5 (2013), 050403.

[594] Diego Paiva Pires, Marco Cianciaruso, Lucas C Céleri, Gerardo Adesso, and Diogo O Soares-Pinto. "Generalized geometric quantum speed limits". *Phys. Rev. X* 6.2 (2016), 021031.

[595] Sebastian Deffner and Eric Lutz. "Quantum speed limit for non-Markovian dynamics". *Phys. Rev. Lett.* 111.1 (2013), 010402.

[596] Iman Marvian, Robert W Spekkens, and Paolo Zanardi. "Quantum speed limits, coherence, and asymmetry". *Phys. Rev. A* 93.5 (2016), 052331.

[597] Armin Uhlmann. "An energy dispersion estimate". *Physics Letters A* 161.4 (1992), 329–331.

[598] Florian Fröwis. "Kind of entanglement that speeds up quantum evolution". *Phys. Rev. A* 85.5 (2012), 052127.

[599] Hans J Bremermann. "Quantum noise and information". *Proceedings of the fifth berkeley symposium on mathematical statistics and probability*. Vol. 4. University of California Press Berkeley, CA. 1967, 15–20.

[600] Seth Lloyd. "Ultimate physical limits to computation". *Nature* 406.6799 (2000), 1047–1054.

[601] Jacob D Bekenstein. "Generalized second law of thermodynamics in black-hole physics". *Phys. Rev. D* 9.12 (1974), 3292.

[602] Sebastian Deffner and Eric Lutz. "Generalized Clausius inequality for nonequilibrium quantum processes". *Phys. Rev. Lett.* 105.17 (2010), 170402.

[603] Obinna Abah and Eric Lutz. "Energy efficient quantum machines". *Europhysics Letters* 118.4 (2017), 40005.

[604] Victor Mukherjee, Wolfgang Niedenzu, Abraham G Kofman, and Gershon Kurizki. "Speed and efficiency limits of multilevel incoherent heat engines". *Phys. Rev. E* 94.6 (2016), 062109.

[605] Manuel Gessner and Augusto Smerzi. "Statistical speed of quantum states: Generalized quantum Fisher information and Schatten speed". *Phys. Rev. A* 97.2 (2018), 022109.

[606] Chao Zhang et al. "Detecting metrologically useful asymmetry and entanglement by a few local measurements". *Phys. Rev. A* 96.4 (2017), 042327.

[607] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. "Entanglement in many-body systems". *Rev. Mod. Phys* 80.2 (2008), 517.

[608] Benjamin Morris, Benjamin Yadin, Matteo Fadel, Tilman Zibold, Philipp Treutlein, and Gerardo Adesso. "Entanglement between identical particles is a useful and consistent resource". *Phys. Rev. X* 10.4 (2020), 041012.

[609] Benjamin Yadin and Vlatko Vedral. "General framework for quantum macroscopicity in terms of coherence". *Phys. Rev. A* 93.2 (2016), 022122.

[610] Iman Marvian. "Coherence distillation machines are impossible in quantum thermodynamics". *Nat. Commun* 11.1 (2020), 25.

[611] Florian Fröwis, Pavel Sekatski, Wolfgang Dür, Nicolas Gisin, and Nicolas Sangouard. "Macroscopic quantum states: Measures, fragility, and implementations". *Rev. Mod. Phys* 90.2 (2018), 025004.

[612] Benjamin Yadin, Felix C Binder, Jayne Thompson, Varun Narasimhachar, Mile Gu, and MS Kim. "Operational resource theory of continuous-variable nonclassicality". *Phys. Rev. X* 8.4 (2018), 041038.

[613] Hyukjoon Kwon, Kok Chuan Tan, Tyler Volkoff, and Hyunseok Jeong. "Nonclassicality as a quantifiable resource for quantum metrology". *Phys. Rev. Lett.* 122.4 (2019), 040503.

[614] Kok Chuan Tan, Varun Narasimhachar, and Bartosz Regula. "Fisher information universally identifies quantum resources". *Phys. Rev. Lett.* 127.20 (2021), 200402.

[615] Helmut Strobel, Wolfgang Muessel, Daniel Linnemann, Tilman Zibold, David B Hume, Luca Pezzè, Augusto Smerzi, and Markus K Oberthaler. "Fisher information and entanglement of non-Gaussian spin states". *Science* 345.6195 (2014), 424–427.

[616] Florian Fröwis. "Lower bounds on the size of general Schrödinger-cat states from experimental data". *J. Phys. A* 50.11 (2017), 114003.

[617] Iman Marvian. "Operational interpretation of quantum fisher information in quantum thermodynamics". *Phys. Rev. Lett.* 129.19 (2022), 190502.

[618] Ángel Rivas, Susana F Huelga, and Martin B Plenio. "Quantum non-Markovianity: characterization, quantification and detection". *Reports on Progress in Physics* 77.9 (2014), 094001.

[619] Márcio M Taddei, Bruno M Escher, Luiz Davidovich, and Ruynet L de Matos Filho. "Quantum speed limit for physical processes". *Phys. Rev. Lett.* 110.5 (2013), 050402.

[620] Remigiusz Augusiak, J Kołodyński, Alexander Streltsov, Manabendra Nath Bera, Antonio Acin, and Maciej Lewenstein. "Asymptotic role of entanglement in quantum metrology". *Phys. Rev. A* 94.1 (2016), 012339.

[621] Francesco Ciccarello, Salvatore Lorenzo, Vittorio Giovannetti, and G Massimo Palma. "Quantum collision models: Open system dynamics from repeated interactions". *Physics Reports* 954 (2022), 1–70.

[622] Dietrich Leibfried, Rainer Blatt, Christopher Monroe, and David Wineland. "Quantum dynamics of single trapped ions". *Rev. Mod. Phys* 75.1 (2003), 281.

[623] Angel Rivas, A Douglas K Plato, Susana F Huelga, and Martin B Plenio. "Markovian master equations: a critical study". *New J. Phys* 12.11 (2010), 113032.

[624] Luca Pezzè, Yan Li, Weidong Li, and Augusto Smerzi. "Witnessing entanglement without entanglement witness operators". *Proceedings of the National Academy of Sciences* 113.41 (2016), 11459–11464.

[625] Benjamin Yadin, Matteo Fadel, and Manuel Gessner. "Metrological complementarity reveals the Einstein-Podolsky-Rosen paradox". *Nat. Commun* 12.1 (2021), 2410.

[626] Anil Bhattacharyya. "On a measure of divergence between two statistical populations defined by their probability distribution". *Bulletin of the Calcutta Mathematical Society* 35 (1943), 99–110.

[627] Julia Kempe, Dave Bacon, Daniel A Lidar, and K Birgitta Whaley. "Theory of decoherence-free fault-tolerant universal quantum computation". *Phys. Rev. A* 63.4 (2001), 042307.

[628] Matteo Scandi and Martí Perarnau-Llobet. "Thermodynamic length in open quantum systems". *Quantum* 3 (2019), 197.

[629] Harry JD Miller, Matteo Scandi, Janet Anders, and Martí Perarnau-Llobet. "Work fluctuations in slow processes: Quantum signatures and optimal control". *Phys. Rev. Lett.* 123.23 (2019), 230603.

[630] Jan Hermans. "Simple analysis of noise and hysteresis in (slow-growth) free energy simulations". *The Journal of Physical Chemistry* 95.23 (1991), 9029–9032.

[631] Christopher Jarzynski. "Nonequilibrium equality for free energy differences". *Phys. Rev. Lett.* 78.14 (1997), 2690.

[632] Dénes Petz. "Covariance and Fisher information in quantum mechanics". *Journal of Physics A: Mathematical and General* 35.4 (2002), 929.

[633] Davide Girolami. "Observable measure of quantum coherence in finite dimensional systems". *Phys. Rev. Lett.* 113.17 (2014), 170401.

[634] Shunlong Luo. "Quantum versus classical uncertainty". *Theoretical and mathematical physics* 143 (2005), 681–688.

[635] Paolo Gibilisco, Daniele Imparato, and Tommaso Isola. "Inequalities for quantum Fisher information". *Proceedings of the American Mathematical Society* 137.1 (2009), 317–327.

[636] Irénée Frérot and Tommaso Roscilde. "Quantum variance: a measure of quantum coherence and quantum correlations for many-body systems". *Phys. Rev. B* 94.7 (2016), 075121.

[637] Frank Hansen. "Metric adjusted skew information". *Proceedings of the National Academy of Sciences* 105.29 (2008), 9909–9916.

[638] Paolo Gibilisco and Tommaso Isola. "Wigner–Yanase information on quantum state space: the geometric approach". *Journal of Mathematical Physics* 44.9 (2003), 3752–3762.

[639] Tameem Albash, Sergio Boixo, Daniel A Lidar, and Paolo Zanardi. "Quantum adiabatic Markovian master equations". *New J. Phys* 14.12 (2012), 123016.

[640] Jordan M Horowitz and Todd R Gingrich. "Thermodynamic uncertainty relations constrain non-equilibrium fluctuations". *Nature Physics* 16.1 (2020), 15–20.

[641] David P DiVincenzo. "Quantum computation". *Science* 270.5234 (1995), 255–261.

[642] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. "The security of practical quantum key distribution". *Rev. Mod. Phys.* 81.3 (2009), 1301.

[643] Daniel A Lidar and Todd A Brun. *Quantum error correction*. Cambridge University Press, 2013.

[644] Christoph Simon and Julia Kempe. "Robustness of multiparty entanglement". *Phys. Rev. A* 65.5 (2002), 052327.

[645] Wolfgang Dür and Hans-J Briegel. "Stability of macroscopic entanglement under decoherence". *Phys. Rev. Lett.* 92.18 (2004), 180403.

[646] André RR Carvalho, Florian Mintert, and Andreas Buchleitner. "Decoherence and multipartite entanglement". *Phys. Rev. Lett.* 93.23 (2004), 230501.

[647] Marc Hein, Wolfgang Dür, and H-J Briegel. "Entanglement properties of multipartite entangled states under the influence of decoherence". *Phys. Rev. A* 71.3 (2005), 032350.

[648] O Gühne, F Bodoky, and M Blaauboer. "Multiparticle entanglement under the influence of decoherence". *Phys. Rev. A* 78.6 (2008), 060301.

[649] Leandro Aolita, Rafael Chaves, Daniel Cavalcanti, Antonio Acín, and Luiz Davidovich. "Scaling laws for the decay of multiqubit entanglement". *Phys. Rev. Lett.* 100.8 (2008), 080501.

[650] Nicolas Brunner and Tamás Vértesi. "Persistency of entanglement and nonlocality in multipartite quantum systems". *Phys. Rev. A* 86.4 (2012), 042113.

[651] Antoine Neven, John Martin, and Thierry Bastin. "Entanglement robustness against particle loss in multiqubit systems". *Phys. Rev. A* 98.6 (2018), 062335.

[652] Ming-Xing Luo and Shao-Ming Fei. "Robust multipartite entanglement without entanglement breaking". *Phys. Rev. Research* 3.4 (2021), 043120.

[653] Matthias Christandl and Andreas Winter. "Uncertainty, monogamy, and locking of quantum correlations". *IEEE Trans. Inf. Theory* 51.9 (2005), 3159–3165.

[654] Debbie Leung. "A survey on locking of bipartite correlations". *Journal of Physics: Conference Series*. Vol. 143. 1. IOP Publishing. 2009, 012008.

[655] David P DiVincenzo, Christopher A Fuchs, Hideo Mabuchi, John A Smolin, Ashish Thapliyal, and Armin Uhlmann. "Entanglement of assistance". *NASA International Conference on Quantum Computing and Quantum Communications*. Springer. 1998, 247–257.

[656] Zong-Guo Li, Ming-Jing Zhao, Shao-Ming Fei, and WM Liu. "Evolution equation for entanglement of assistance". *Phys. Rev. A* 81.4 (2010), 042312.

[657] John A Smolin, Frank Verstraete, and Andreas Winter. "Entanglement of assistance and multipartite state distillation". *Phys. Rev. A* 72.5 (2005), 052317.

[658] Gilad Gour, David A Meyer, and Barry C Sanders. "Deterministic entanglement of assistance and monogamy constraints". *Phys. Rev. A* 72.4 (2005), 042329.

[659] Antonio D'Arrigo, Giuliano Benenti, Rosario Lo Franco, Giuseppe Falci, and Elisabetta Paladino. "Hidden entanglement, system-environment information flow and non-Markovianity". *InterNatl. J. (Wash.) of Quantum Information* 12.02 (2014), 1461005.

[660] Tan Kok Chuan, J Maillard, Kavan Modi, Tomasz Paterek, Mauro Paternostro, and Marco Piani. "Quantum discord bounds the amount of distributed entanglement". *Phys. Rev. Lett.* 109.7 (2012), 070501.

[661] Alexander Streltsov, Hermann Kampermann, and Dagmar Bruß. "Quantum cost for sending entanglement". *Phys. Rev. Lett.* 108.25 (2012), 250501.

[662] Michael Horodecki, Peter W Shor, and Mary Beth Ruskai. "Entanglement breaking channels". *Rev. Math. Phys.* 15.06 (2003), 629–641.

[663] Giacomo Mauro D'Ariano, Paoloplacido Lo Presti, and Paolo Perinotti. "Classical randomness in quantum measurements". *J. Phys. A: Math. Gen.* 38.26 (2005), 5979.

[664] Mary Beth Ruskai. "Qubit entanglement breaking channels". *Rev. Math. Phys.* 15.06 (2003), 643–662.

[665] Carlos Sabín and Guillermo García-Alcaine. "A classification of entanglement in three-qubit systems". *Eur. Phys. J. D* 48.3 (2008), 435–442.

[666] Noah Linden, Sandu Popescu, Ben Schumacher, and M Westmoreland. "Reversibility of local transformations of multiparticle entanglement". *arXiv: quant-ph/9912039* (1999).

[667] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral. "The classical-quantum boundary for correlations: Discord and related measures". *Rev. Mod. Phys.* 84.4 (2012), 1655.

[668] Kaushik P Seshadreesan and Mark M Wilde. "Fidelity of recovery, squashed entanglement, and measurement recoverability". *Phys. Rev. A* 92.4 (2015), 042321.

[669] Barbara Kraus, Ignacio Cirac, Siniša Karnas, and Maciej Lewenstein. "Separability in 2× N composite quantum systems". *Phys. Rev. A* 61.6 (2000), 062302.

List of Figures

Acknowledgements

I would like to thank the following people for their help and support that have made this thesis possible.

- First of all, I would like to thank my supervisor, Otfried Gühne for giving me the opportunity to work as a PhD student at Siegen in the field of quantum information and for his support throughout my PhD. His ideas and suggestions have been instrumental in driving my passion for exploring new research directions. Also, his clear and concise explanations have enabled me to grasp key insights into especially entanglement theory.

- I would like to thank Stefan Nimmrichter for leading me into a new research direction in thermodynamics and for being patient in listening to my ambiguous and unclear ideas every time. I want to thank him for collaborating on the project in Chapter 5.

- I would like to thank Géza Tóth for supporting my research visit to Bilbao and for giving me instructions on quantum metrology and spin squeezing. I want to thank him for collaborating on the projects in Chapters 6 and 7.

- I would like to thank Andreas Ketterer, Xiao-Dong Yu, and Nikolai Wyderka for fruitful discussions and great collaboration on randomized measurements. I want to thank Nikolai Wyderka for his help in building up my first project in Chapter 2 and for his willingness to answer many of my stupid questions. I learned many things from him, for example, sector lengths, Haar integrals, separability problems, Bloch decompositions, rather, many basics of quantum information. Thanks to discussions with him, I acquired a lot of calculation techniques. I want to thank Andreas Ketterer for including me in the project in Chapter 3 and for working on the statistical analysis of randomized measurements. I want to thank Xiao-Dong Yu for including me in the project in Chapter 8 and for his clear explanation of analytical techniques.

- I would like to thank Zhen-Peng Xu for together working on the project in Chapter 12 as my collaborator and also for the wonderful time we had in Siegen as an officemate and a friend of mine.

- I would like to thank Paweł Cieśliński, Jan Dziewior, Lukas Knips, Wiesław Laskowski, Jasmin Meinecke, Tomasz Paterek, and Tamás Vértesi for together completing the review in Ref. [7].

- I would like to thank especially Yuan-Yuan Zhao for completing the project in Ref. [8] and for realizing the experimental demonstration of our theoretical works. Also, I would like to thank her for reviewing Sec. 2.5 and providing great comments.
- I would like to thank Benjamin Yadin for bringing me to the original idea in Result 47 and kindly inviting me to join the project in Chapter 11. I am glad that we later formulated the part of “Weak coupling" together and he led us to the connection with quantum thermodynamics introduced in the part of “Quantum work fluctuations".
- I would like to thank Shravan Shravan and Simon Morelli for collaborating on the project in Chapter 10. In particular, I am glad that we have achieved the analytical proof of Result 42.
- I would like to thank Jan Lennart Bönsel, Sophia Denker, Ties Ohst, Leonardo S. V. Santos, Konrad Szymański, and Benjamin Yadin for reviewing this thesis and giving nice comments. Also I want to thank Jan Lennart Bönsel for his help in writing the German abstract in this thesis and for having many discussions about spin squeezing.
- I would like to thank everyone in the Theoretical Quantum Optics Group for the stimulating and great atmosphere and for their patience with my puzzling questions and ramblings.
- I would like to thank our secretary Daniela Lehmann for helping me with bureaucratic things and for being patient with my laziness.
- I acknowledge various support from the DAAD (German Academic Exchange Service).
- I would like to thank many people at TC Siegen who, despite communicating in English, had a great tennis time and created a wonderful atmosphere. I really enjoyed playing tennis with different types of players on clay courts.
- Finally, I would like to thank my family for their support. Without their help and love, I could never have come this far.