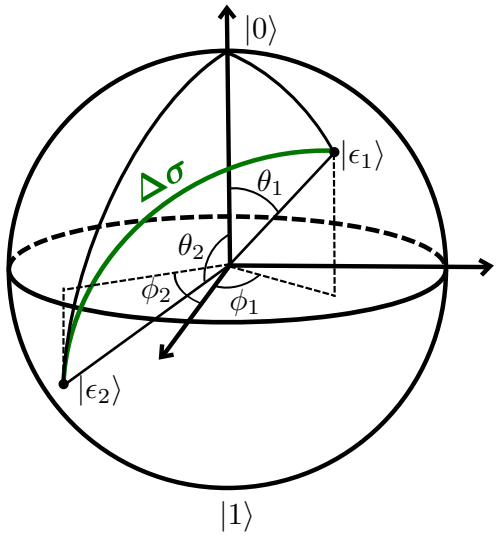
Université de Liège
Faculté des Sciences
I.P.N.A.S.

Development of new tools to detect, characterize and quantify quantum entanglement in multipartite systems

Antoine Neven



Academic year 2017-2018

This work was supported by a FRIA grant from the Belgian FNRS.

Université de Liège
Faculté des Sciences
I.P.N.A.S.

Development of new tools to detect, characterize and quantify quantum entanglement in multipartite systems

Antoine Neven

Supervisor: Prof. Thierry Bastin

Jury: Prof. Peter Schlagheck (President)
Prof. Otfried Gühne (Universität Siegen)
Prof. John Martin
Prof. Pierre Mathonet
Prof. Stefano Pironio (ULB)

Original thesis presented in partial fulfillment of the requirements for the degree of Doctor in Sciences

October 10th, 2018

Abstract

Quantum entanglement is a key property of quantum information theory, that is at the heart of numerous promising applications in fields such as quantum cryptography, quantum computing or quantum sensing. In the past decades, the advent of such innovative technologies has reinforced the need for a better understanding of entanglement. The aim of this thesis is to contribute to this effort through the development of new tools targeting the characterization of several features of entanglement. Concerning the issue of entanglement detection, we present an optimization of the approach that exploits the concept of generalized concurrences to solve the separability problem for pure states. We then reformulate the separability question of mixed states into a matrix analysis problem, from which we obtain general separability criteria for multipartite states of ranks two and three. We also briefly discuss some properties of separable states. In particular, we characterize optimal separable decompositions of symmetric (i.e. permutation invariant) states of two and three qubits with maximal rank properties. Regarding the quantification of entanglement, we propose a function to quantify the entanglement of symmetric multiqubit states within classes of entangled states gathering states that are stochastically equivalent through local operations assisted with classical communication. This function establishes a link between the amount of entanglement of a symmetric state and the distribution of its Majorana points on the Bloch sphere. We finally investigate the robustness of entanglement with respect to particle loss and provide a full description of all multiqubit states that are fragile for the loss of one of their qubits. For symmetric states, the fragility for the loss of one qubit is shown to be related to a particular symmetry of the Majorana points.

Acknowledgments

Carrying out a PhD thesis is a long journey but, fortunately, I was not alone. I would like to express my gratitude to the people that accompanied me along the way.

First of all, I would like to thank my supervisor, Prof. Thierry Bastin, for the time he managed to dedicate to me in his very busy schedule, for his guidance and his useful advice, sometimes given on the tiniest free spaces left on his whiteboard.

I am also grateful to Profs. Otfried Gühne, John Martin, Pierre Mathonet, Stephano Pironio and Peter Schlagheck, who kindly accepted to be part of my jury. I wish them a pleasant reading of this dissertation.

It is a pleasure to thank my office mates Emeline, Lionel and Renaud. Although we spent most of our time working on our theses, there was always room for some jokes and discussions about tennis, politics, the freezing temperature of our office, life, physics or ... Mac adapters! Working in this good atmosphere has been an important driving force for me.

I also owe a lot to my family and I especially wish to thank my parents for their constant support. I have also been blessed with great friends, and that is really valuable to survive a thesis. Thanks to Maju for sharing my passion for sports and to Elodie for having fed me at the office. Thanks to my cycling mates Sylvain, Clémentine and Jérémy for having let me hold so long the record of the climb to the campus. You can speed up now!

I cannot imagine concluding these acknowledgments without thanking Ludivine. You contributed to this work more than you could ever realize. Thank you for having so carefully proofread this text, for putting up with my (particular) sense of humor and for your unfailing support *eight days a week*. May our paths remain entangled forever.

Table of contents

List of publications

Some of the results presented in this thesis have been published in the following references:

• A. Neven, P. Mathonet, O. Gühne, and T. Bastin,
Quantum fidelity of symmetric multipartite states,
Physical Review A **94**, 052332 (2016).

• A. Neven and T. Bastin,
The quantum separability problem is a simultaneous hollowisation matrix analysis problem,
Journal of Physics A: Mathematical and Theoretical **51**, 315305 (2018).

• A. Neven, J. Martin, and T. Bastin,
Entanglement robustness against particle loss in multiqubit systems,
preprint ArXiv:1809.00622 (2018).

Introduction

The concept of quantum entanglement goes back to the early years of quantum mechanics, in the first decades of the twentieth century. At that time, it had quickly been noted that, by contrast to the previous classical theories, the mathematical framework of the emerging quantum mechanics theory allowed a system to be in a *superposition* of different possible states of the system. For composite systems (i.e. systems made of at least two particles), this new possibility has lead to states that cannot be factorized into a collection of states corresponding to each subsystem. In such unfactorizable states, that were later called *entangled* states, there are correlations between the individual properties of the subsystems that cannot be reproduced classically. Quantum entanglement revealed such intriguing potentialities that it lead E. Schrödinger to say [1]: "I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."

From certain perspectives, the departure from the classical conception of nature was even so abrupt that, before it established itself in the physics community, quantum entanglement had first to overcome some controversy, notably into the form of the famous *EPR paradox*. In 1935, A. Einstein, B. Podolsky and N. Rosen presented a thought experiment [2] in which a pair of particles are created in an entangled state and then separated from each other. According to the laws of quantum mechanics, when performing a measurement on one of the entangled particles, the state of the other collapses into a new state determined by the outcome of the measurement on the first particle and the initial state of the pair. This collapse obviously changes the possible outcomes of a subsequent measurement on the second particle. As this also happens if the two measurements are separated by a spacelike interval (so that, according to the laws of special relativity, no information can be sent from one particle to the other between the measurements), it seems that the second particle must in some sense "know" what measurement has been performed on the first particle, and with what outcome. Rejecting this surprising conclusion, notably because it violates the so-called "local realist" picture of causality, the authors suggested that quantum mechanics was not a complete theory and proposed a hidden variable model to restore local realism. In this model, the measurement outcomes are predetermined in hidden variables at the time of creation of the entangled pair and

carried by each particle, removing the need for a kind of communication between the particles.

The EPR paradox was only settled in 1964, when J. S. Bell showed [3] an upper bound on the amount of correlations any hidden variable theory can produce in a specific experiment. Since this upper bound was proved to be violated by certain entangled states [3], it showed that hidden variables could not reproduce all predictions of quantum mechanics. This violation of the so-called Bell inequality was reproduced experimentally [4] in 1982, by a team lead by A. Aspect, confirming that quantum mechanics correctly predicts the non-local properties of entangled states.

From that moment, what seemed to be an odd feature of quantum mechanics became considered as a powerful resource. For instance, the strong correlations highlighted in Bell's experiment were exploited in a protocol for securing communications [5], introducing entanglement into the emerging field of quantum cryptography [6]. Through the quantum teleportation protocol [7], entanglement also opened new horizons in the field of quantum communication. The list of applications using entanglement has continued to grow ever since. To cite a few examples, entangled states are used in quantum computing [8], quantum metrology [9, 10], quantum imaging [11], or also quantum sensing [12].

With the advent of these numerous applications came also the need for a better theoretical characterization of entanglement. For instance, determining whether a state produced experimentally is entangled or not can be a critical issue for the practical realization of quantum protocols. This fundamental problem, known as the *separability problem*, is however still an open problem for general multipartite states. Besides the presence of entanglement, the usefulness of a state may also depend on its amount of entanglement. Being able to quantify entanglement is for instance important in the field of quantum computation, where some protocols are more efficient when using highly entangled states [13], while others require states that are not too much entangled to perform efficiently [14]. Through the years, multiple aspects have been added to the characterization of the entanglement property. Among these aspects, an entangled state can for instance be characterized through is distillability [15, 16], through the class of states it gives access to through local operations and classical communication [17, 18], through its robustness against local noise [19] or through its robustness against particle loss [18].

In this thesis, we aim at contributing to this quest for a better characterization of quantum entanglement. To do so, we develop new tools to study some of the aforementioned features of quantum entanglement. While most of our developments focus on the famous multiqubit systems (i.e. systems with 2-level subsystems), we sometimes also consider multipartite systems with subsystems of arbitrary dimension. Throughout this thesis, we also grant a particular importance to the case of permutation invariant (or *symmetric*) multiqubit states. While we often compare their properties to those of general multiqubit states, we specifically dedicate some chapters to symmetric states. The manuscript is structured as follows.

In Chapter 1, we review the basic concepts of quantum information theory that will be used throughout the subsequent chapters. We first introduce quantum systems associated

to finite dimensional Hilbert spaces. In these systems, we describe the formalisms used to treat pure and mixed states. We also define symmetric states and detail two well-known representations for those states: the Dicke and Majorana representations. We get then to the heart of the matter and dedicate three sections to the introduction of elementary notions of entanglement characterization. The first one tackles entanglement detection, the second one focuses on the operational classification of entanglement through local operations and the last one introduces the field of entanglement quantification.

Chapter 2 is dedicated to fidelity optimization in operational classes. In this chapter, we investigate the following question: Given a symmetric state $|\psi_S\rangle$ and an operational class $\mathcal{C}$ containing symmetric and nonsymmetric states, is the optimal fidelity between the states $|\psi_S\rangle$ and all the states of the class $\mathcal{C}$ obtained for a symmetric state? We first summarize the known results about this problem and then study a conjecture concerning a specific operational class.

Chapter 3 is dedicated to the study of the separability problem, using generalized concurrences. We first optimize the number of generalized concurrences that have to be considered, compared to previous methods, in order to solve the separability problem for pure states. We then extend our study to mixed states using the preconcurrence matrix formalism and reformulate the separability problem into a pure matrix analysis problem. By solving this problem for low dimensional matrices, we finally give separability criteria for low rank states.

In Chapter 4, we study properties of symmetric separable states. By contrast to Chapter 3, we consider entanglement detection techniques based on partial transposition. More specifically, we adapt an algorithm for the rank reduction of PPT states to study optimal separable decompositions of separable symmetric states.

In Chapter 5, we propose a function to quantify the entanglement of symmetric states. We then use it to discuss the relationship between the geometric configuration of the Majorana points of a symmetric state and the amount of entanglement it possesses.

Finally, Chapter 6 is dedicated to the study of entanglement robustness against particle loss. We first focus on the characterization of entanglement robustness for the loss of a single particle, both in multiqubit and multiqudit systems. We then investigate the entanglement robustness properties of symmetric multiqubit states and extend our study to the case where several particles are lost.

Chapter 1

General notions of quantum information theory

In this chapter, we give an overview of basic notions in quantum information theory. We also take advantage of this chapter to specify some notations that will be used throughout this manuscript. Section 1.1 is dedicated to the description of the states of quantum systems associated to a Hilbert space of finite dimension. In Section 1.2, we describe specific features arising when considering a quantum system composed of several subsystems. In Section 1.3, we introduce basic tools used for entanglement characterization.

1.1 Systems associated to Hilbert spaces of finite dimension

While in classical information theory, information is stored into a system ruled by the laws of classical physics, such as a transistor or the beads of an abacus, in quantum information theory, information is encoded into a quantum system whose possible states obey the laws of quantum mechanics. One of the interests of quantum information theory is then to use specific features of quantum mechanics to process the information with an efficiency that outperforms any classical protocol. In quantum information, information can be stored into systems associated to either finite or infinite dimensional Hilbert spaces (the latter case is also called quantum information with continuous variables, see for instance Ref. [20] and references therein). In this thesis, we focus on discrete quantum systems, i.e. quantum systems associated to Hilbert spaces of finite dimension. The states of such systems are described using two distinct formalisms, depending on whether they are *pure* or *mixed*.

1.1.1 Pure states

In classical information theory, the basic unit used to encode information is the *bit*. A bit can only take two discrete values: 0 or 1. In quantum information theory, the smallest system that can be used to encode information is called *qubit*. A qubit is any quantum system associated to a Hilbert space of dimension 2. In this Hilbert space, one usually works in a particular basis, called *computational basis* and composed of the basis states $|0\rangle$ and $|1\rangle$. In this basis, the most general pure state $|\psi\rangle$ of a qubit can be written

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{1.1}$$

with α and β two complex numbers satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. In quantum mechanics, the global phase of the Hilbert space element used to describe the physical state of a system is arbitrary. As a consequence, if we choose to extract a global phase equal to the phase of the complex number α in Eq. (1.1), we can equivalently express the state $|\psi\rangle$ as

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle, \tag{1.2}$$

for some $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi[$. The main interest of this particular parametrization of qubit states, called *Bloch representation*, is that it allows to map any qubit state onto a point on the unit sphere in $\mathbb{R}^3$, which in quantum information theory is called *Bloch sphere*. As can be seen on Fig. 1.1, the angles θ and ϕ appearing in the parametrization (1.2) of the qubit state $|\psi\rangle$ become the polar and azimuthal spherical coordinates of the point representing $|\psi\rangle$ on the Bloch sphere.

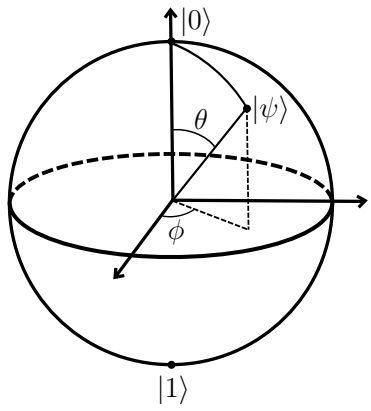


Figure 1.1: Representation of a qubit state $|\psi\rangle$ on the Bloch sphere.

Qubit systems play an important role in the field of quantum information theory but there is no fundamental reason to restrict ourselves to quantum systems with a Hilbert space of dimension 2. We will sometimes consider the more general case of quantum

systems associated to a Hilbert space of finite dimension $d \geq 2$. In this Hilbert space, the computational basis contains d elements, which we write $|0\rangle, |1\rangle, \ldots, |d-1\rangle$. By analogy to the word *qubit*, such systems are called *qudits*[1] in quantum information theory.

1.1.2 Mixed states

A quantum system associated to a Hilbert space $\mathcal{H}$ is not necessarily in a pure state, it can also be in a statistical ensemble (or *mixture*) of pure states. In this case, the system is said to be in a *mixed state* and there exists a set $\{(p_i, |\psi_i\rangle) : i = 1, \ldots, l\}$ with $0 \leq p_i \leq 1$ such that $\sum_{i=1}^{l} p_i = 1$, called *decomposition* of the mixed state and such that the system is in the pure state $|\psi_i\rangle$ with probability p_i. Such a mixed state can also be described by an operator, called *density operator* and generally denoted by ρ, defined in the space $\mathrm{Lin}(\mathcal{H})$ of linear operators on $\mathcal{H}$ as

$$\rho = \sum_{i=1}^{l} p_i |\psi_i\rangle\langle\psi_i|. \tag{1.3}$$

All the physical properties of a mixed state can be computed from its density operator. Because of this strong relationship between a mixed state and its density operator, we often denote a mixed state by its density operator. As can be checked in Eq. (1.3), a density operator ρ is always a positive semi-definite Hermitian operator (which we also write $\rho \geq 0$) with unit trace. Conversely, any operator of $\mathrm{Lin}(\mathcal{H})$ satisfying these two properties describes a physical mixed state of the system. Let us here note that pure states are merely particular cases of mixed states, with decompositions containing only one pure state (associated to a probability equal to 1). The density operator ρ associated to a pure state $|\psi\rangle$ is nothing but the projector onto this state, i.e. $\rho = |\psi\rangle\langle\psi|$. Pure states are also the only states satisfying the purity condition $\rho^2 = \rho$.

Given a genuine mixed state, whereas it is described by a unique density operator ρ, there exists an infinite number of different decompositions $\{(p_i, |\psi_i\rangle) : i = 1, \ldots, l\}$ leading to ρ through Eq. (1.3). These decompositions correspond to the same physical mixed state. Among them is the so-called *eigendecomposition* $\{(\lambda_i, |v_i\rangle) : i = 1, \ldots, r\}$, made of the nonzero eigenvalues λ_i of ρ (possibly repeated according to their multiplicity) and associated eigenvectors $|v_i\rangle$, with r the rank of ρ. By contrast to other decompositions, the eigendecomposition can always be directly deduced from a given density operator. Its cardinality is in addition the smallest possible cardinality for any decomposition of the mixed state [21]. All the other decompositions of a mixed state ρ can be computed from its eigendecomposition. For any other decomposition $\{(\mu_i, |w_i\rangle) : i = 1, \ldots, l\}$ of cardinality $l \geq r$, there indeed exists [21] a $l \times r$ matrix U whose columns are r orthonormal vectors

[1] In the particular case $d = 3$, the word *qutrit* is also often used.

in $\mathbb{C}^l$ such that

$$\begin{pmatrix} \sqrt{\mu_1}\,|w_1\rangle \\ \vdots \\ \sqrt{\mu_l}\,|w_l\rangle \end{pmatrix} = U \begin{pmatrix} \sqrt{\lambda_1}\,|v_1\rangle \\ \vdots \\ \sqrt{\lambda_r}\,|v_r\rangle \end{pmatrix}. \tag{1.4}$$

This relationship between the eigendecomposition of a mixed state ρ and any other decomposition provides also a way to span all possible decompositions of ρ.

Like transistors in classical memories, the potential of quantum systems to encode information naturally grows when combining several subsystems (for example several qubits) to encode a larger piece of information. In addition, specific quantum properties, such as entanglement, arise only in these combined systems, offering new possibilities to process information. We describe these properties in the next section.

1.2 Multipartite systems

A *multipartite* (or *composite*) system is a system composed of a given number $N \geq 2$ of subsystems, which in this context are also called *parties*. If each subsystem is associated to the Hilbert space $\mathcal{H}_i$ ($i = 1, \ldots, N$), the global Hilbert space $\mathcal{H}$ of the multipartite system is given by the tensor product of the Hilbert spaces of the subsystems: $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$. In the most general case, each subsystem can be associated to a Hilbert space $\mathcal{H}_i$ of arbitrary finite dimension $d_i \geq 2$. The dimension of the global Hilbert space $\mathcal{H}$ is then given by the product of the dimensions of the Hilbert spaces associated to each subsystem: $\dim(\mathcal{H}) = \prod_{i=1}^{N} d_i$. In this global Hilbert space, a basis can be created by taking all possible combinations of tensor products between basis elements from each subsystem. For the computational basis, we get basis states of the form $|i_1\rangle \otimes \cdots \otimes |i_N\rangle$ with $i_j \in \{0, \ldots, d_j - 1\}$ for all $j = 1, \ldots, N$. To simplify the notations, we generally use short form $|i_1, \ldots, i_N\rangle \equiv |i_1\rangle \otimes \cdots \otimes |i_N\rangle$ for states that have this tensor product structure. For computational basis states, we even drop the commas (when $d_i \leq 10$, $\forall\, i = 1, \ldots, N$), yielding states expressed as N-digit numbers, such as the 5-partite computational basis state $|20130\rangle$, for example.

In quantum information, it is frequent to study homogeneous multipartite systems, i.e. multipartite systems in which all subsystems are associated to Hilbert spaces of the same dimension. In the following, we often consider *multiqubit* systems, i.e. multipartite system containing only qubit subsystems, or *multiqudit* systems, i.e. multipartite systems in which all the subsystems are qudits associated to Hilbert spaces of the same dimension d.

Our description of the properties of multipartite states begins with a section dedicated to the important property of quantum entanglement. We then describe the partial trace operation, which is a tool used to compute the residual state associated to a given subset of the parties of a multipartite system. In the last section, we introduce the so-called symmetric states.

1.2.1 Quantum entanglement

Quantum entanglement is a property that arises only in multipartite systems. A multipartite pure state $|\psi\rangle$ defined in the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ is a *product* or *(fully) separable* state if there exist states $|\phi_i\rangle \in \mathcal{H}_i$ for all $i = 1, \ldots, N$ such that

$$|\psi\rangle = |\phi_1\rangle \otimes \cdots \otimes |\phi_N\rangle. \tag{1.5}$$

In the same system, a mixed state ρ is (fully) separable if it can be written as a convex combination of projectors onto pure product states, i.e. if there exist pure product states $|\Phi_{\text{sep}}^{(j)}\rangle \in \mathcal{H}$ $(j = 1, \ldots, l)$ and probabilities p_j, with $\sum_{j=1}^{l} p_j = 1$, such that

$$\rho = \sum_{j=1}^{l} p_j \, |\Phi_{\text{sep}}^{(j)}\rangle\langle\Phi_{\text{sep}}^{(j)}|. \tag{1.6}$$

Any state (pure or mixed) that is not fully separable is an *entangled* state. Entanglement is an emblematic quantum property that is notably related to the nonlocal nature of quantum mechanics. For instance, even though all entangled states do not violate all Bell's inequalities, a Bell's inequality can only been violated by entangled states [3].

From an experimental point of view, it is frequent to consider the scenario in which the parties of a multipartite system are shared between spatially separated experimenters. In this scenario, if each experimenter prepares a pure state, they can together only produce a fully separable state of the form (1.5). These experimenters could naturally also prepare each a mixed state and even add correlations between the mixtures they prepare through classical communication [22]. This preparation protocol would yield a mixed state ρ of the form

$$\rho = \sum_i p_i \, \rho_i^{(1)} \otimes \cdots \otimes \rho_i^{(N)}, \tag{1.7}$$

with, as usual, $\sum_i p_i = 1$. Expending each subsystem mixed state as a convex sum of projectors, according to any of its decompositions, shows however that such a state can always be written into the form (1.6) and is therefore separable. This shows that entanglement cannot be produced by local operations on the parties, even when classical communication is allowed between the experimenters. To produce entanglement, a multipartite operation is required.

1.2.2 Partial trace and reduced density operator

Given a mixed state ρ of a general N-partite system associated to a Hilbert space $\mathcal{H}$, we might be interested in the properties of the state corresponding to only some of the N subsystems. Let A be the subset of $\{1, \ldots, N\}$ containing the parties of interest and B its complement. For any such bipartition, the global Hilbert space can always be expressed as the tensor product $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces associated to the subsystems A and B, respectively. The *reduced density operator* ρ_A of the state

corresponding to subsystem A, which is an operator acting on $\mathcal{H}_A$, can be extracted from ρ through a *partial trace* over subsystem B.

For any sets $\{|\phi_i\rangle : i = 1, \ldots, \dim(\mathcal{H}_A)\}$ and $\{|\psi_\mu\rangle : \mu = 1, \ldots, \dim(\mathcal{H}_B)\}$ forming bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, ρ can be decomposed in the corresponding bipartite basis as

$$\rho = \sum_{i,j=1}^{\dim(\mathcal{H}_A)} \sum_{\mu,\nu=1}^{\dim(\mathcal{H}_B)} \rho_{i\mu,j\nu} \Big(|\phi_i\rangle \otimes |\psi_\mu\rangle \Big) \Big(\langle\phi_j| \otimes \langle\psi_\nu| \Big). \tag{1.8}$$

The partial trace of ρ over subsystem B, which is denoted by $\mathrm{Tr}_B(\rho)$, reads then

$$\mathrm{Tr}_B(\rho) = \sum_{i,j=1}^{\dim(\mathcal{H}_A)} \sum_{\mu,\nu=1}^{\dim(\mathcal{H}_B)} \rho_{i\mu,j\nu} \, |\phi_i\rangle\langle\phi_j| \, \mathrm{Tr}\Big(|\psi_\mu\rangle\langle\psi_\nu| \Big), \tag{1.9}$$

and we have $\rho_A = \mathrm{Tr}_B(\rho)$. The partial trace over subsystem A is defined in a similar fashion, with a trace acting on the basis states of subsystem A. It is interesting to note that even when ρ is a pure state, meaning that we exactly know the global state of the system, ρ_A may be a mixed state, meaning that the state of subsystem A is only known through a probability distribution. This situation however only occurs if the state ρ presents some entanglement across the bipartition $A|B$. This provides another illustration that, for an entangled state, the global state must be seen as a whole and cannot be factorized into states corresponding to the different subsystems.

1.2.3 Symmetric states in multiqubit systems

Due to the tensor product structure of the global Hilbert space of a multipartite system, its dimension grows exponentially with the number of parties. This exponential growth of the Hilbert space dimension is often a limiting factor, from both a numerical and an analytical point of view, for the characterization of multipartite states in systems with a large number of parties. For this reason, it can be interesting to focus on classes of states defined in subspaces of the Hilbert space that have a dimension growing slower with the number of parties. The class of *symmetric* states is an emblematic example of such classes.

An N-partite state $|\psi_S\rangle$ is said to be symmetric if it remains invariant under any permutation of the parties, i.e. if $P_\pi|\psi_S\rangle = |\psi_S\rangle$, $\forall\, \pi \in S_N$, where S_N is the permutation group of N elements and P_π is the permutation operator corresponding to the permutation π. In an N-qudit system, the *symmetric subspace* (i.e. the subspace of the Hilbert space containing the symmetric states) has a dimension equal to $\binom{N+d-1}{d-1}$ instead of d^N for the whole Hilbert space. Besides this theoretical advantage, symmetric states have also a particular experimental relevance. As a consequence of the spin-statistics theorem, symmetric states are indeed the only allowed states for systems of indistinguishable bosons. Throughout this thesis, we will frequently consider symmetric states, however

exclusively in the context of multiqubit systems. We summarize here the basic properties of symmetric multiqubit states.

In an N-qubit system, the dimension of the symmetric subspace is equal to $N+1$. This linear growth of the symmetric subspace dimension with the number of qubits constitutes a dramatic decrease compared to the dimension 2^N of the global Hilbert space. For this reason, the usual computational basis used to express multiqubit states is not the most compact way to represent symmetric multiqubit states. These states are usually either expressed in the *Dicke* [23] or in the *Majorana* [24] representation. We detail these two representations in the next paragraphs.

The Dicke representation of a multiqubit symmetric state consists in expressing the state in a particular basis of the symmetric subspace called *Dicke basis*. The $N+1$ states making up this basis, which are called *Dicke states* and denoted by $|D_N^{(k)}\rangle$ $(k = 0, \ldots, N)$, are obtained by symmetrization of the computational basis states. We thus have

$$|D_N^{(k)}\rangle = \frac{1}{\sqrt{\binom{N}{k}}} \sum_{\pi} |\underbrace{1\ldots1}_{k}\underbrace{0\ldots0}_{N-k}\rangle, \tag{1.10}$$

where the sum runs over the $\binom{N}{k}$ distinct permutations of the computational basis state with k qubits in the state $|1\rangle$ and the remaining $N-k$ qubits in the state $|0\rangle$. In the Dicke representation, any symmetric state $|\psi_S\rangle$ is characterized by a list of $N+1$ *Dicke coefficients* d_k $(k = 0, \ldots, N)$, such that $\sum_{k=0}^{N} |d_k|^2 = 1$ and

$$|\psi_S\rangle = \sum_{k=0}^{N} d_k |D_N^{(k)}\rangle. \tag{1.11}$$

Due to the permutation invariance of the symmetric state $|\psi_S\rangle$, it is also always possible to find (normalized) 1-qubit states $|\phi_i\rangle$ $(i = 1, \ldots, N)$ such that

$$|\psi_S\rangle = \mathcal{N} \sum_{\pi \in S_N} |\phi_{\pi(1)}, \ldots, \phi_{\pi(N)}\rangle, \tag{1.12}$$

with $\mathcal{N}$ a normalization constant. In Eq. (1.12), a global phase can be extracted from each 1-qubit state $|\phi_i\rangle$. These states can thus be expressed into the Bloch representation (1.2), so that the symmetric state $|\psi_S\rangle$ can be written

$$|\psi_S\rangle = \mathcal{N} \sum_{\pi \in S_N} |\epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}\rangle, \tag{1.13}$$

where $|\epsilon_i\rangle = \cos(\theta_i/2)\,|0\rangle + e^{i\phi_i} \sin(\theta_i/2)\,|1\rangle$ for some $\theta_i \in [0, \pi]$ and $\phi_i \in [0, 2\pi[$, $\forall\ i = 1, \ldots, N$. This representation of a symmetric state, as a sum over all permutations of the single qubit states of a product state, is the so-called Majorana representation. By mapping the single qubit states $|\epsilon_i\rangle$ $(i = 1, \ldots, N)$ onto N points, called *Majorana points*, on the Bloch sphere, we obtain a useful geometric representation of symmetric states.

As the states $|\epsilon_i\rangle$ are not necessarily different, some of the Majorana points may be degenerated. This is for example the case of separable symmetric states, for which the single qubit states $|\epsilon_i\rangle$ appearing in their Majorana representation are all equal. An N-qubit separable symmetric state is thus geometrically represented by a single point on the Bloch sphere, degenerated N times.

To conclude this section, we show how to link the Dicke and Majorana representations. Given an N-qubit symmetric state $|\psi_S\rangle$ with Dicke coefficients d_k $(k = 0, \ldots, N)$, we define, as in Ref. [25], the polynomial

$$P(z) = \sum_{k=0}^{N} (-1)^k \sqrt{\binom{N}{k}}\, d_k\, z^k. \tag{1.14}$$

Let K be the degree of this polynomial. The value of K ranges from 0 to N, depending on the number of nonzero Dicke coefficients d_k. The complex roots $z_1, \ldots, z_K$ of this polynomial can be related to the angles θ_j and ϕ_j $(j = 1, \ldots, N)$ corresponding to the Bloch representation of the single qubit states appearing in the Majorana representation (1.13) of $|\psi_S\rangle$ through the relation [25]

$$\begin{cases} \cot\theta_j\, e^{-i\phi_j} = z_j & \text{if } j \leq K \\ \theta_j = 0 & \text{if } j > K \end{cases}. \tag{1.15}$$

1.3 Entanglement characterization

The characterization of entanglement is a broad topic (see for instance Ref. [26] and references therein). The aim of this section is not to present an overview of entanglement characterization but rather to introduce the particular aspects of entanglement characterization that will be developed in the upcoming chapters. In Section 1.3.1, we introduce the field of entanglement detection. In Section 1.3.2, we present the LOCC and SLOCC paradigms for the operational characterization of entanglement, as well as the classifications of entangled states these paradigms lead to. Finally, in Section 1.3.3, we introduce the field of entanglement quantification.

1.3.1 Entanglement detection

Determining whether a given state ρ is separable or not may naively seem to be a basic question. Despite intensive research efforts, no general answer (covering the case of mixed states) has however been provided to this fundamental question and the so-called *separability problem* remains one of the most emblematic open problems in quantum information theory.

When restricted to the case of pure states, the separability problem is easy to solve. One solution is to check whether the reduced density operator corresponding to each subsystem is a pure state. This is indeed the case if and only if the pure state is separable.

In Chapter 3, we detail another solution of the separability problem for pure states, based on generalized concurrences.

According to the definition of separability, a mixed state ρ is separable if it admits a *separable decomposition*, i.e. a decomposition containing only pure product states. Searching for such a separable decomposition is a dramatically complex task, requiring to span unitary matrices of large dimensions, and it is not the usual way to tackle the separability problem. One rather tries to exploit the existence of such a separable decomposition to deduce properties of separable states, which can then be translated into separability *criteria*. Over the years, many *practical*[2] separability criteria have been stated, such as the Positive Partial Transpose (PPT) criterion [27], combinatorially independent permutation criteria [28, 29], Bell-type inequalities [30], or criteria based on entanglement witnesses [31, 32]. In general, these criteria are only necessary *or* sufficient conditions of separability, meaning that they allow to detect some but not all entangled states in a given multipartite system. We will not detail here all the aforementioned criteria (further details can, for example, be found in Refs. [26, 33]) but rather focus on one of them, namely the *PPT criterion*, as it has become an ubiquitous tool in quantum information theory.

The PPT criterion was proposed by A. Peres in 1996 [27] for bipartite states, but extends straightforwardly to multipartite states. This entanglement criterion consists in a necessary condition of separability based on an operation on the density operator called *partial transposition*. Given an N-partite state ρ, a partial transposition can be applied to its density operator for any bipartition $A|B$ of the system, where A is a nonempty subset of the N subsystems and B is the complementary subset. If the sets $\{|\psi_i\rangle\}$ and $\{|\phi_\mu\rangle\}$ form orthonormal bases in the Hilbert spaces of the subsystems A and B, respectively, then ρ can be expressed in the corresponding bipartite basis as

$$\rho = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \, |\psi_i\rangle \otimes |\phi_\mu\rangle\langle\psi_j| \otimes \langle\phi_\nu|. \tag{1.16}$$

In this basis, taking the partial transpose of ρ with respect to subsystem A is equivalent to transposing the elements of the tensor $\rho_{i\mu,j\nu}$, but only for the indices corresponding to subsystem A (the Latin indices in this case). The corresponding operator, which is denoted by ρ^{T_A}, reads

$$\rho^{T_A} = \sum_{i,\mu,j,\nu} \rho_{j\mu,i\nu} \, |\psi_i\rangle \otimes |\phi_\mu\rangle\langle\psi_j| \otimes \langle\phi_\nu|. \tag{1.17}$$

The partial transposition of ρ with respect to subsystem B is defined similarly, permuting this time only the indices corresponding to subsystem B (i.e. the Greek indices). Since taking successively the partial transpose of ρ with respect to subsystem A and then with

[2]Practical should here be understood as providing an efficient algorithm (regarding computation time, memory and precision) to test the condition.

respect to subsystem B yields the usual full transpose ρ^T, we have also

$$\rho^{T_B} = \left(\rho^{T_A}\right)^T . \tag{1.18}$$

The PPT criterion, follows from the observation that the partial transpose of a separable density operator always yields another physical density operator and is therefore necessarily a positive semi-definite operator [27]. This can be translated into the following separability criterion:

PPT criterion (Peres [27]). *If ρ is an N-partite separable state, then $\rho^{T_A} \geq 0$ for all bipartitions $A|B$ of the multipartite system.*

As a consequence of Eq. (1.18), ρ^{T_B} and ρ^{T_A} have the same eigenvalues. This implies $\rho^{T_B} \geq 0 \Leftrightarrow \rho^{T_A} \geq 0$ and this is the reason why we only consider partial transposition with respect to only one part of the bipartition in the PPT criterion.

A multipartite state is said to be PPT if it remains positive semi-definite under partial transposition with respect to all distinct bipartitions of the system, and NPT otherwise. As a consequence of the PPT criterion, an NPT state is necessarily entangled, showing how partial transposition and the PPT criterion can be useful tools to detect entanglement. If a state is PPT, however, we cannot infer from the PPT criterion if it is separable or entangled, except in the cases of 2-qubit and qubit-qutrit systems, where the PPT criterion was proved to be also a sufficient condition of separability [31].

1.3.2 Operational classification of multipartite states

As discussed in Section 1.2.1, a multipartite state locally prepared by distant experimenters cannot contain entanglement, even if the experimenters use classical communication (for example to share the outcome of a measurement performed on their party). They could however locally manipulate an entangled state if this state has been created somewhere through a multipartite entangling process before being shared between the experimenters. In this case, one can be interested in the *class* of states the experimenters have access to using local operations. This operational scheme, called LOCC for Local Operations assisted with Classical Communication, is in fact used to define two classifications of multipartite states, into either LOCC or SLOCC classes.

A LOCC class contains states that can be deterministically (i.e. with probability 1) converted into each other through LOCC. Two states ρ and σ belonging to the same LOCC class are said LOCC-equivalent. For pure states, it has been shown [17] that two states $|\psi\rangle$ and $|\phi\rangle$ are LOCC-equivalent if and only if they are also equivalent through *local unitary* (LU) operations. This condition reads formally

$$\begin{aligned} &|\psi\rangle \text{ and } |\phi\rangle \text{ are LOCC-equivalent} \\ &\Leftrightarrow \exists\, U_1, \ldots, U_N \text{ such that } U_i^\dagger U_i = \mathbb{1}\ \forall i = 1, \ldots, N \text{ and } |\psi\rangle = U_1 \otimes \cdots \otimes U_N |\phi\rangle. \end{aligned} \tag{1.19}$$

In other words, LOCC equivalence corresponds to equivalence under local change of basis. Because of this equivalence, LOCC classes and LU classes divide a Hilbert space into the same sets of states and both concepts can be used interchangeably. The LU equivalence is a strong equivalence relation and it turns out [34] that even in the smallest multipartite system, i.e. a 2-qubit system, this classification leads to an infinite number of LOCC classes.

By relaxing the deterministic condition in the LOCC equivalence relation, we get the SLOCC equivalence (where the "S" stands for Stochastic). Two states are SLOCC-equivalent if they can stochastically (that is with a nonzero probability) be converted into each other under LOCC. Compared to a LOCC protocol, a SLOCC protocol converts a state ρ into a probabilistic distribution $\{(p_i, \sigma_i) : i = 1, \ldots, l\}$ of mixed states σ_i, each associated to a probability p_i (such that $\sum_i p_i = 1$). For pure states, it has been shown [18] that two states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent if and only if they can be converted into each other through an *Invertible Local Operation* (ILO). We thus have

$$\begin{aligned} &|\psi\rangle \text{ and } |\phi\rangle \text{ are SLOCC-equivalent} \\ &\Leftrightarrow \exists\, A_1, \ldots, A_N \text{ such that } \det(A_i) \neq 0\ \forall i = 1, \ldots, N \text{ and } |\psi\rangle = A_1 \otimes \cdots \otimes A_N |\phi\rangle. \end{aligned} \tag{1.20}$$

Obviously, two pure states that are LOCC-equivalent are necessarily SLOCC-equivalent but the converse is not true, except in the set $\mathcal{S}$ containing all product states, which is both a LOCC and a SLOCC class. The SLOCC classification is thus a coarse-grained classification of the LOCC classification. In multiqubit systems, the SLOCC classification yields a finite number of different SLOCC classes only if the system contains 2 or 3 qubits [18]. In a 2-qubit system, there are only 2 different SLOCC classes and in a 3-qubit system, 6 different SLOCC classes [18]. In multiqubit systems of at least 4 qubits, the number of SLOCC classes is infinite, and in multiqudit systems with $d \geq 3$ and at least three parties, the number of SLOCC classes is also infinite [18].

As the symmetric subspace of the Hilbert space associated to a multiqubit system has a much lower dimension than the global Hilbert space, the SLOCC classification of symmetric states could result in a lower number of classes. We take a closer look at the operational classification of symmetric states in the following subsection.

SLOCC classification of symmetric multiqubit states

The permutation invariance of symmetric states has some interesting consequences on their SLOCC classification. For symmetric states, the SLOCC equivalence relation (1.20) in terms of ILOs can be simplified to [35, 36]

$$\begin{aligned} &\text{Two symmetric states } |\psi_S\rangle \text{ and } |\phi_S\rangle \text{ are SLOCC-equivalent} \\ &\Leftrightarrow \exists\, A \text{ with } \det(A) \neq 0 \text{ such that } |\psi_S\rangle = A \otimes \cdots \otimes A |\phi_S\rangle. \end{aligned} \tag{1.21}$$

An ILO is called symmetric if, like in equation (1.21), the same invertible operation acts on all the parties, and nonsymmetric otherwise. The SLOCC equivalence condition (1.21) does not mean that two symmetric states cannot be transformed into each other through a nonsymmetric ILO. When it is the case, we however have the guarantee that there also exists a symmetric ILO transforming these two states into each other [35, 36].

Even though there are only 3 SLOCC classes of symmetric states in 3-qubit systems (instead of 6 in the nonsymmetric case), there is still an infinite number of SLOCC classes for symmetric states of at least 4 qubits [25]. The simplified SLOCC equivalence relation (1.21) was nevertheless used in Ref. [25] to develop a classification of symmetric states into a finite number of *families* of SLOCC classes. These families are defined upon the *diversity degree* and *degeneracy configuration* of symmetric states [25], which can be deducted from their Majorana representation.

The diversity degree of a symmetric state $|\psi_S\rangle$ corresponds to the number of distinct single qubit states $|\epsilon_i\rangle$ appearing in its Majorana representation (1.13). If a *degeneracy number* is associated to each of these distinct single qubit states, corresponding to its multiplicity in the Majorana representation of $|\psi_S\rangle$, then the degeneracy configuration of $|\psi_S\rangle$ is defined as the list of these degeneracy numbers, sorted in decreasing order.

Applying a symmetric ILO on a symmetric state does not modify its degeneracy configuration [25]. Because SLOCC-equivalent symmetric states can always be transformed into each other through a symmetric ILO [35, 36], symmetric states with different degeneracy configurations are necessarily SLOCC-inequivalent. This is the reason why it was proposed in Ref. [25] to group symmetric states with the same degeneracy configuration l into a SLOCC class family, denoted by $\mathcal{D}_l$. As there is one family $\mathcal{D}_l$ for each degeneracy configuration l, the number of families in this classification is given by the number of possible degeneracy configurations for the symmetric states of the system. By definition, a given degeneracy configuration corresponds to a way of dividing the set formed by the N (indistinguishable) qubits into nonempty subsets. Such a division is called a *partition* of N in number theory and the number of partitions of a natural number N is given by the *partition function* $p(N)$. The partition function of a natural number gives a finite number, so that we always have a finite number of families $\mathcal{D}_l$. This is an advantage compared to the SLOCC classification. For instance, for a 4-qubit system, we have $p(4) = 5$ and the 5 corresponding $\mathcal{D}_l$ families are $\mathcal{D}_4$, $\mathcal{D}_{3,1}$, $\mathcal{D}_{2,2}$, $\mathcal{D}_{2,1,1}$ and $\mathcal{D}_{1,1,1,1}$.

The number of SLOCC classes that are grouped together into the family $\mathcal{D}_l$ depends on the diversity degree of the degeneracy configuration l. The family $\mathcal{D}_l$ contains a single SLOCC class if the diversity degree of its degeneracy configuration l is at most equal to 3, and an infinite number of SLOCC classes otherwise [25].

1.3.3 Entanglement quantification

Quantifying entanglement is not only interesting from a theoretical point of view, it has also an experimental relevance as certain protocols, such as quantum teleportation [7], have an efficiency that depends on the amount of entanglement of the states used in the

protocol. For this reason, it would be interesting to have a real-valued function E, called *entanglement measure*, for quantifying the amount of entanglement of multipartite states. Quantum entanglement is a complex and rich property and there is no obvious choice for such a function, that would be meaningful and easy to calculate for all multipartite states. To guarantee that it respects the fundamental properties of entanglement, an entanglement measure is generally required to satisfy two axioms [26, 37]. The first one is related to the behavior of entanglement under LOCC.

Axiom 1. *If the state ρ can be converted into the state σ through LOCC, then any entanglement measure E must satisfy:*

$$E(\sigma) \leq E(\rho). \tag{1.22}$$

This first axiom reflects the fact that, because of its nonlocal nature (see Section 1.2.1), entanglement cannot be created or enhanced through LOCC. This axiom has an important consequence: an entanglement measure must give the same value for all LOCC-equivalent states, and therefore be invariant under LU operations. As all separable states are LOCC-equivalent, this means in particular that an entanglement measure must be constant on the set of separable states. This constant value must in addition be the lowest possible value of the entanglement measure, as any state can be converted through LOCC to a separable state (by local measurements, for example). This lowest value can be chosen arbitrarily but it seems sensible to set it to zero. This is actually the second axiom:

Axiom 2. *If ρ is a separable state, then any entanglement measure E must satisfy:*

$$E(\rho) = 0. \tag{1.23}$$

These two axioms gather the properties that an entanglement measure must satisfy to faithfully quantify entanglement. Additional properties of entanglement measures may however be required in some specific contexts. The most common of these requirements is arguably the monotonicity under SLOCC.

Definition 1. *An entanglement measure E is monotonic under SLOCC if, for any SLOCC protocol converting a state ρ into the probabilistic distribution $\{p_i, \sigma_i\}$, E does not increase* on average*, i.e. if*

$$E(\rho) \geq \sum_i p_i \, E(\sigma_i). \tag{1.24}$$

A function satisfying monotonicity under SLOCC is usually called an *entanglement monotone*. Most of the entanglement measures that have been proposed are actually also monotonic under SLOCC [26]. This property obviously implies monotonicity under LOCC and is sometimes easier to prove than monotonicity under LOCC [26], for example for convex entanglement measures.

Definition 2. *An entanglement measure E is convex if,*

$$E\left(\sum_i p_i\,\rho_i\right) \leq \sum_i p_i\; E(\rho_i), \tag{1.25}$$

for any convex combination $\sum_i p_i\,\rho_i$ with $\sum_i p_i = 1$.

Convexity is not fundamentally required to define an entanglement measure but it is a mathematically convenient property. Among other convenient properties of entanglement measures, we can also mention the *additivity* and *full additivity*.

Definition 3. *An entanglement measure E is additive if,*

$$E\left(\rho^{\otimes n}\right) = nE(\rho), \tag{1.26}$$

for any mixed state ρ. It is fully additive if

$$E\left(\rho \otimes \sigma\right) = E(\rho) + E(\sigma), \tag{1.27}$$

for any mixed states ρ and σ.

These properties reflect the idea that gathering the states of several separated systems into a global system should preserve the total amount of entanglement. However, this turns out to be a very strong condition, that many entanglement measures fail to satisfy. For example, whereas the *Entanglement of formation* is conjectured to be additive, entanglement measures such as the *relative entropy of entanglement* or the *negativity* are not additive [37].

This description of the property of entanglement measures concludes our overview of basics notions of quantum information theory. In the following chapter, we consider the problem of fidelity optimization in operational classes, which is related to the classification of entangled states presented in Section 1.3.2.

Chapter 2

Fidelity optimization in operational classes

Quantum states belonging to the same LU or SLOCC operational class have similar entanglement properties regarding local operations but can differ significantly regarding other entanglement properties. In a local protocol using states from a given operational class $\mathcal{C}$, finding the state in $\mathcal{C}$ that optimizes a particular property may therefore help to increase the efficiency of the protocol. In this chapter, we investigate this problem for the optimization of the fidelity between a given state $|\psi\rangle$ and all the states belonging to an operational class $\mathcal{C}$ (that does not contain the state $|\psi\rangle$). We focus on the case in which the state $|\psi\rangle$ is symmetric and the class $\mathcal{C}$ contains symmetric and nonsymmetric states. In the first section, we review the concept of quantum fidelity and remind some important results regarding fidelity optimization in operational classes. We then describe some of the results presented in Ref. [38] and present further developments about a conjecture mentioned in Ref. [38].

2.1 Quantum fidelity and fidelity optimization

Quantum fidelity [39, 40] is widely used in quantum information theory to estimate the "closeness" between two states in the Hilbert space of a quantum system. For two arbitrary mixed states ρ_1 and ρ_2, it is defined as the symmetric real-valued function

$$F(\rho_1, \rho_2) = \left(\mathrm{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} \right)^2 . \tag{2.1}$$

The fidelity between two pure states $|\psi\rangle$ and $|\phi\rangle$ reduces to their squared overlap (i.e. the squared modulus of their scalar product):

$$F(\psi, \phi) = |\langle \psi | \phi \rangle|^2 . \tag{2.2}$$

The fidelity itself does not define a metric on the state space. There are however metrics, such as the Bures distance [41, 42] $d_B(\rho_1, \rho_2) = [2 - 2\sqrt{F(\rho_1, \rho_2)}\,]^{1/2}$, which are monotonic functions of the fidelity. As a consequence, it is safe to say that the higher the fidelity between two states, the "closer" these states are in the Hilbert space.

In the context of the operational classification of entangled (pure) states, one can then use the fidelity to search, in an operational class $\mathcal{C}$, the state that is the closest to a given state $|\psi\rangle$. Such an optimal fidelity

$$F_{|\psi\rangle,\mathcal{C}} \equiv \sup_{|\phi\rangle\in\mathcal{C}} F(\psi, \phi) \tag{2.3}$$

turns out to be very a useful quantity. When considering the class $\mathcal{S}$ containing all separable states, the maximal fidelity $F_{|\psi\rangle,\mathcal{S}}$ can, for example, be used to build *entanglement witnesses* [33] or compute the geometric measure of entanglement $E_G(\psi) = 1 - F_{|\psi\rangle,\mathcal{S}}$ [43]. For other operational classes, optimal fidelities can be used in discrimination strategies of inequivalent classes of multipartite entangled states, either using witnesses [44], or other methods [45].

The difficult part is actually to compute such optimal fidelities. In the general case, this was even proved to be an NP-hard problem [46]. However, when the optimization is performed in the class of separable states, an important simplification in the computation of $F_{|\psi\rangle,\mathcal{S}}$ occurs if the state $|\psi\rangle$ is symmetric. In this case, it has indeed been proven [47] that the maximal fidelity is always obtained for a symmetric separable state. For any symmetric state $|\psi_S\rangle$, we thus have

$$F_{|\psi_S\rangle,\mathcal{S}} = F^S_{|\psi_S\rangle,\mathcal{S}} \equiv \sup_{\text{symmetric } |\phi\rangle\in\mathcal{S}} F(\psi_S, \phi). \tag{2.4}$$

This property implies a dramatic simplification in the computation of the maximal fidelity between a symmetric state and any separable state. Indeed, performing an optimization over all symmetric separable states is equivalent to performing an optimization over all single qubit states (i.e. over two real parameters), so that the complexity of the optimization becomes independent of the number of qubits.

2.2 Fidelity optimization in LU and SLOCC classes

The main focus of Ref. [38] was to determine whether the property (2.4) can be extended to general LU and SLOCC classes in multiqubit systems. Formally, the question addressed was the following: "Given an operational SLOCC or LU class $\mathcal{C}$ containing symmetric states, do we have for any symmetric state $|\psi_S\rangle$

$$F_{|\psi_S\rangle,\mathcal{C}} \stackrel{?}{=} F^S_{|\psi_S\rangle,\mathcal{C}} \equiv \sup_{\text{symmetric } |\phi\rangle\in\mathcal{C}} F(\psi_S, \phi)\ ?" \tag{2.5}$$

Concerning LU classes, the answer to Question (2.5) was shown [38] to be always positive, so that for any LU class $\mathcal{C}_{\text{LU}}$ containing symmetric states and for any symmetric state $|\psi_S\rangle$, we have

$$F_{|\psi_S\rangle,\mathcal{C}_{\text{LU}}} = F^S_{|\psi_S\rangle,\mathcal{C}_{\text{LU}}}. \tag{2.6}$$

For SLOCC classes however, Eq. (2.5) does not hold in general and several counter-examples were identified in Ref. [38]. Counter-examples can for instance be found in the SLOCC classes of some of the Dicke states (see Section 1.2.3 for the definition of the Dicke states). Let $\mathcal{W}_N^{(k)}$ $(k = 0, \ldots, \lfloor N/2 \rfloor$[1]$)$ denote the SLOCC class of the Dicke state $|D_N^{(k)}\rangle$. When restricted to the symmetric subspace, the SLOCC class $\mathcal{W}_N^{(k)}$ coincides with the family $\mathcal{D}_{N-k,k}$ (defined in Section 1.3.2). It turns out that most of the SLOCC classes $\mathcal{W}_N^{(k)}$ violate Eq. (2.5) as we have [38], for any state $|\psi_N^{(1)}\rangle \in \mathcal{W}_N^{(1)}$,

$$F_{|\psi_N^{(1)}\rangle,\mathcal{W}_N^{(k)}} > F^S_{|\psi_N^{(1)}\rangle,\mathcal{W}_N^{(k)}}\ ,\ \forall\ N \geq 4, k = 2, \ldots, \lfloor N/2 \rfloor. \tag{2.7}$$

By contrast, it was conjectured in Ref. [38] that Eq. (2.5) holds for the only Dicke SLOCC class (containing entangled states) not considered in Eq. (2.7), namely $\mathcal{W}_N^{(1)}$, whatever symmetric state $|\psi_S\rangle$ is considered. This conjecture, that we call $\mathcal{W}_N^{(1)}$ *class conjecture*, reads formally

$\mathcal{W}_N^{(1)}$ class conjecture. *For any symmetric state $|\psi_s\rangle$, we have*

$$F_{|\psi_S\rangle,\mathcal{W}_N^{(1)}} = F^S_{|\psi_S\rangle,\mathcal{W}_N^{(1)}}. \tag{2.8}$$

Although it is supported by extensive numerical simulations [38], this conjecture has not been analytically proved yet. In the next section, we present results obtained while attempting to prove the conjecture.

2.3 The $\mathcal{W}_N^{(1)}$ class conjecture

In this section, we present an operational approach of the $\mathcal{W}_N^{(1)}$ class conjecture and several developments exploiting particular properties of the class $\mathcal{W}_N^{(1)}$ to attempt proving the conjecture. Although these attempts do not lead to a definitive proof of the conjecture, they provide new ideas that can be useful in other investigations involving this SLOCC class.

Let us begin with the operational rephrasing of the conjecture. On the one hand, the left-hand side of Eq. (2.8) requires to span the states of the whole SLOCC class $\mathcal{W}_N^{(1)}$. As a SLOCC class contains SLOCC-equivalent states, which can be obtained from one another through an ILO [18], the span of the SLOCC class $\mathcal{W}_N^{(1)}$ can equivalently be realized by a span of the ILOs onto any state belonging to the class $\mathcal{W}_N^{(1)}$. On the other hand, the right-hand side of Eq. (2.8) requires to span only the symmetric states of the class. As it

[1] Throughout this thesis, the symbol $\lfloor x \rfloor$ denotes the floor function of the real number x.

was proved [35] that two symmetric SLOCC-equivalent states can always be transformed into each other through a symmetric ILO, this span can be equivalently achieved by a span of the symmetric ILOs onto any symmetric state belonging to the class $\mathcal{W}_N^{(1)}$. To simplify the comparison between both sides, it is preferable to choose the same state for the span of the whole SLOCC class and the span of its symmetric subspace. As it seems the most natural choice, we take the Dicke state $|D_N^{(1)}\rangle$, that is also often denoted by $|\mathrm{W}_N\rangle$, to be the representative state of the class $\mathcal{W}_N^{(1)}$. We can thus rephrase Eq. (2.8) as

$$\sup_{\text{invertible } A_1,\ldots,A_N} \frac{|\langle\psi_s|A_1\otimes\cdots\otimes A_N|\mathrm{W}_N\rangle|^2}{||A_1\otimes\cdots\otimes A_N|\mathrm{W}_N\rangle||^2} = \sup_{\text{invertible } A} \frac{|\langle\psi_s|A^{\otimes N}|\mathrm{W}_N\rangle|^2}{||A^{\otimes N}|\mathrm{W}_N\rangle||^2}. \tag{2.9}$$

This reformulation allows us to exploit specific properties of the state $|\mathrm{W}_N\rangle$. For example, it was pointed out in Ref. [35] that the state $|\mathrm{W}_N\rangle$ admits a (nonsymmetric) stabilizer[2] S of the form

$$S = J\otimes J^{-1}\otimes \mathbb{1}\otimes\cdots\otimes\mathbb{1}\,, \tag{2.10}$$

where, in the computational basis, the operator J is represented by a 2×2 invertible Jordan matrix

$$J_\lambda = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \text{ with } \lambda\in\mathbb{C}_0. \tag{2.11}$$

Because of the permutation invariance of the state $|\mathrm{W}_N\rangle$, it has to be noted that, in the stabilizer S, the couple of qubits the operators J and J^{-1} act on is totally arbitrary. An equivalent stabilizer could therefore be obtained by considering any permutation in the tensor product defining S in Eq. (2.10).

This stabilizer plays a central role in the following section, in which we show how to partially symmetrize the ILO in the left-hand side of Eq. (2.9). It will then be generalized in Section 2.3.2.

2.3.1 Partial symmetrization of the ILO

This first attempt of proof has been developed in collaboration with P. Mathonet, who proposed to exploit the stabilizer (2.10) to partially symmetrize the nonsymmetric ILO acting on the state $|\mathrm{W}_N\rangle$ in the left-hand side of Eq. (2.9). As shown in the following proposition, this partial symmetrization consists in transforming any nonsymmetric ILO acting on the state $|\mathrm{W}_N\rangle$ into the product of a nonsymmetric LU operation, a nonsymmetric diagonal ILO and a symmetric ILO.

Proposition 2.1. *For any ILO $A_1\otimes\cdots\otimes A_N$ acting on $\left(\mathbb{C}^2\right)^{\otimes N}$, there exist 2×2 unitary matrices $U_1,\ldots,U_N$ and positive diagonal matrices $D_1,\ldots,D_N$ such that*

$$\frac{A_1\otimes\cdots\otimes A_N|\mathrm{W}_N\rangle}{||A_1\otimes\cdots\otimes A_N|\mathrm{W}_N\rangle||} = \frac{(U_1D_1\otimes\cdots\otimes U_ND_N)\,B^{\otimes N}|\mathrm{W}_N\rangle}{||\,(U_1D_1\otimes\cdots\otimes U_ND_N)\,B^{\otimes N}|\mathrm{W}_N\rangle||}, \tag{2.12}$$

[2] An operator S is said to be a stabilizer of a state $|\psi\rangle$ if $S|\psi\rangle = |\psi\rangle$.

where B is an operator represented in the computational basis either by the 2×2 identity matrix, or by a 2×2 invertible Jordan matrix

$$J_\lambda = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \text{ with } \lambda \in \mathbb{C}_0.$$

Proof. Let us use the *QR factorization* [48] to decompose each 2×2 matrix A_i ($i = 1, \ldots, N$) appearing in the left-hand side of equation (2.12) into the product $A_i = U_i R_i$, with U_i a 2×2 unitary matrix and R_i a 2×2 upper triangular matrix with nonnegative diagonal entries. To preserve the invertibility of each matrix A_i, the diagonal elements of the corresponding matrix R_i must be strictly positive, so that these upper triangular matrices can always be written

$$R_i = \begin{pmatrix} \alpha_i & c_i \\ 0 & \beta_i \end{pmatrix}, \text{ with } \alpha_i, \beta_i > 0 \text{ and } c_i \in \mathbb{C}. \tag{2.13}$$

We now divide the proof into two cases: (*i*) the matrices R_i are diagonal for all $i = 1, \ldots, N$ or (*ii*) there exists at least one $k \in \{1, \ldots, N\}$ such that the matrix R_k is not diagonal. In case (*i*), the conclusion follows immediately as Eq. (2.12) is satisfied for $B = \mathbb{1}_2$. We now consider case (*ii*). Let $\mathcal{R}$ be the set containing the indices of the matrices R_i which are not diagonal, i.e. $\mathcal{R} = \{i \in \{1, \ldots, N\} : c_i \neq 0\}$, and r its cardinality ($1 \leq r \leq N$). For all $j \in \{1, \ldots, N\} \setminus \mathcal{R}$, we rename the diagonal matrix R_j as D_j and for all $k \in \mathcal{R}$, we further decompose the matrix R_k into the product $R_k = D_k J_k$, with

$$D_k = \begin{pmatrix} c_k & 0 \\ 0 & c_k \frac{\beta_k}{\alpha_k} \end{pmatrix} \text{ and } J_k = \begin{pmatrix} \frac{\alpha_k}{c_k} & 1 \\ 0 & \frac{\alpha_k}{c_k} \end{pmatrix}. \tag{2.14}$$

We can now use stabilizers of the form (2.10) to collect all the Jordan matrices J_k ($k \in \mathcal{R}$) on a given qubit, say the first. This can be simply achieved if, for all $k \in \mathcal{R}$ with $k \neq 1$, we apply the stabilizer $J_k \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes J_k^{-1} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}$ (with J_k^{-1} acting on qubit k) on the state $|\mathrm{W}_N\rangle$ (the order in which these operations are performed has no importance). The successive transformations we performed up to now onto the ILO appearing in the left hand side of Eq. (2.12) lead to the equality

$$\frac{A_1 \otimes \cdots \otimes A_N |\mathrm{W}_N\rangle}{||A_1 \otimes \cdots \otimes A_N |\mathrm{W}_N\rangle||} = \frac{U_1 D_1 J' \otimes U_2 D_2 \otimes \cdots \otimes U_N D_N |\mathrm{W}_N\rangle}{||U_1 D_1 J' \otimes U_2 D_2 \otimes \cdots \otimes U_N D_N |\mathrm{W}_N\rangle||}, \tag{2.15}$$

with

$$J' = \prod_{k \in \mathcal{R}} J_k. \tag{2.16}$$

Up to a multiplicative constant, the product of two Jordan matrices yields a Jordan matrix. The matrix J' is therefore also a Jordan matrix, up to a multiplicative constant. Because of the linearity of the norm, the multiplicative constants multiplying J' in the numerator

and in the denominator of the right-hand side of Eq. (2.15) cancel each other and we can simply consider J' as a Jordan matrix. Up to a multiplicative constant, the m-th root of a Jordan matrix is also a Jordan matrix, but because of the previous argument, we can here neglect this multiplicative constant. By applying successively $N-1$ stabilizers of the form (2.10) with J an N-th root of J' acting each time on a different qubit between the second and the last and J^{-1} acting on the first qubit, we can distribute an N-th root of J' on each qubit, so as to get a symmetric ILO of Jordan matrices. To conclude the proof, we just need to note that the invariance of Eq. (2.15) under scalar multiplication of the local operators allows us to extract the complex number c_k from the diagonal matrix D_k for all $k \in \mathcal{R}$, which makes them positive diagonal matrices. □

If we could further symmetrize the ILO of diagonal operators in Proposition 2.1, there would only remain an LU operation between two symmetric states and we would be able to prove the $\mathcal{W}_N^{(1)}$ class conjecture by using Property (2.6). Although we have not found how to perform such a symmetrization of the diagonal matrices, Proposition 2.1 can still be used to simplify the operational form of the conjecture. Let us first compute the action (in the computational basis) of the operator $B^{\otimes N}$ from Proposition 2.1 on the state $|\mathrm{W}_N\rangle$. In the case where $B^{\otimes N}$ corresponds to a symmetric ILO of Jordan matrices, we have

$$\frac{(J_\lambda)^{\otimes N}\,|\mathrm{W}_N\rangle}{||\,(J_\lambda)^{\otimes N}\,|\mathrm{W}_N\rangle||} = \frac{|\mathrm{W}_N(\lambda)\rangle}{||\,|\mathrm{W}_N(\lambda)\rangle\,||}, \tag{2.17}$$

where

$$|\mathrm{W}_N(\lambda)\rangle = |\varepsilon(\lambda),0,\ldots,0\rangle + |0,\varepsilon(\lambda),0,\ldots,0\rangle + \cdots + |0,\ldots,0,\,\varepsilon(\lambda)\rangle, \tag{2.18}$$

with

$$|\varepsilon(\lambda)\rangle = \frac{|0\rangle + \lambda\,|1\rangle}{\sqrt{1+|\lambda|^2}}. \tag{2.19}$$

To obtain the single qubit state $|\varepsilon(\lambda)\rangle$ in the more convenient Bloch representation $|\varepsilon(\theta,\phi)\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,e^{i\phi}\,|1\rangle$, we express the nonzero complex number λ into the polar form $\lambda = \tan(\theta/2)\,e^{i\phi}$ with $\theta \in]0,\pi[$ and $\phi \in [0,2\pi[$. We rename accordingly $|\mathrm{W}_N(\lambda)\rangle$ into $|\mathrm{W}_N(\theta,\phi)\rangle$.

The case in which $B^{\otimes N}$ is the identity operator is simply treated by adding the value $\theta = \pi$ to the previous parametrization. Indeed, the state $|\mathrm{W}_N\rangle$ merely corresponds to $|\mathrm{W}_N(\pi,0)\rangle$ (up to normalization).

For any ILO $A_1 \otimes \cdots \otimes A_N$ acting on $\left(\mathbb{C}^2\right)^{\otimes N}$, we can thus write:

$$\frac{A_1 \otimes \cdots \otimes A_N|\mathrm{W}_N\rangle}{||A_1 \otimes \cdots \otimes A_N|\mathrm{W}_N\rangle||} = \frac{(U_1D_1 \otimes \cdots \otimes U_ND_N)\,|\mathrm{W}_N(\theta,\phi)\rangle}{||\,(U_1D_1 \otimes \cdots \otimes U_ND_N)\,|\mathrm{W}_N(\theta,\phi)\rangle||} \tag{2.20}$$

for some 2×2 unitary matrices $U_1,\ldots,U_N$, 2×2 positive diagonal matrices $D_1,\ldots,D_N$ and angles $\theta \in]0,\pi]$, $\phi \in [0,2\pi[$.

We focus now on the action of the nonsymmetric ILO. Using the invariance of Eq. (2.20) for the scalar multiplication of the local operators, one diagonal element can be set to 1 in each diagonal matrix D_i $(i = 1, \ldots, N)$. This choice is arbitrary and we set here the upper left diagonal elements to 1. Concerning the LU operation, we can also use the scalar multiplication invariance to extract a global phase in each unitary matrix U_i $(i = 1, \ldots, N)$ to set its determinant to 1 and make it an element from SU(2). We can also omit the LU operation in the denominator of Eq. (2.20), as it leaves the norm of the state unchanged.

Similar transformations can be applied to the symmetric ILO in the right-hand side of the operational form (2.9) of the $\mathcal{W}_N^{(1)}$ class conjecture. This yields the following simplified operational form of the conjecture:

Simplified operational form of the $\mathcal{W}_N^{(1)}$ class conjecture. *For any symmetric state $|\psi_s\rangle$, we have*

$$\sup_{\substack{\theta\in\,]0,\pi] \\ \phi\in[0,2\pi[\\ U_1,\ldots,U_N\,\in\,\mathrm{SU}(2) \\ r_1,\ldots,r_N>0}} \frac{|\langle\psi_s|U_1 D(r_1)\otimes\cdots\otimes U_N D(r_N)|\mathrm{W}_N(\theta,\phi)\rangle|^2}{||D(r_1)\otimes\cdots\otimes D(r_N)|\mathrm{W}_N(\theta,\phi)\rangle||^2} = \sup_{\substack{\theta\in]0,\pi] \\ \phi\in[0,2\pi[\\ U\,\in\,\mathrm{SU}(2) \\ r>0}} \frac{|\langle\psi_s|\,(UD(r))^{\otimes N}\,|\mathrm{W}_N(\theta,\phi)\rangle|^2}{||D(r)^{\otimes N}|\mathrm{W}_N(\theta,\phi)\rangle||^2}, \tag{2.21}$$

where $D(\alpha)$ is represented, in the computational basis, by the diagonal matrix

$$D(\alpha) \equiv \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \tag{2.22}$$

and

$$|\mathrm{W}_N(\theta,\phi)\rangle = |\varepsilon(\theta,\phi),0,\ldots,0\rangle + |0,\varepsilon(\theta,\phi),0,\ldots,0\rangle + \cdots + |0,\ldots,0,\,\varepsilon(\theta,\phi)\rangle, \tag{2.23}$$

with

$$|\varepsilon(\theta,\phi)\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,e^{i\phi}\,|1\rangle. \tag{2.24}$$

In the left-hand side of the original operational form (2.9) of the conjecture, we had to perform an optimization over N invertible 2×2 matrices. This represents an optimization over $4N$ complex parameters, or equivalently, over $8N$ real parameters. Using the invariance of this expression under scalar multiplication of the local operators, we can lower this number to $6N$ real parameters. In the simplified operational form (2.21), we are left (still in the left-hand side) with an optimization over 2 angles, N unitary matrices from SU(2) and N positive numbers. Each unitary matrix from SU(2) can be parametrized using 3 angles, so that in total, the optimization has to be performed over $4N+2$ real parameters (out of which $3N+2$ are angles). Even though this number of parameters still increases with the number of qubits (by contrast to the symmetric optimization in the right-hand side), the partial symmetrization implied by Proposition 2.1 allows to suppress roughly a third of the (real) parameters required in the optimization.

2.3.2 General ILO stabilizer of the state $|\mathrm{W}_N\rangle$

It has been shown in Ref. [35] that if two symmetric states $|\psi_S\rangle$ and $|\phi_S\rangle$ can be transformed into each other through a nonsymmetric[3] ILO, then they belong either to the separable class, to the SLOCC class of the state $|\mathrm{W}_N\rangle$ or to the SLOCC class of the state $|\mathrm{GHZ}_N\rangle$. When it is the case, there necessarily also exists a symmetric ILO transforming $|\psi_S\rangle$ into $|\phi_S\rangle$ [35]. As a consequence, these three SLOCC classes are the only SLOCC classes in which symmetric states admit nonsymmetric stabilizers. This specific feature of the SLOCC class $\mathcal{W}_N^{(1)}$ was used in the previous attempt of proof of the $\mathcal{W}_N^{(1)}$ class conjecture to simplify the computation of nonsymmetric maximal fidelities within the $\mathcal{W}_N^{(1)}$ SLOCC class. We show here that the nonsymmetric stabilizer (2.10) we used in that section is however not the most general nonsymmetric stabilizer of the state $|\mathrm{W}_N\rangle$.

To find the most general stabilizer of the state $|\mathrm{W}_N\rangle$, we work in the computational basis and search the most general form of invertible matrices $A_1, \ldots, A_N$ satisfying the vector equation

$$A_1 \otimes \cdots \otimes A_N |\mathrm{W}_N\rangle = |\mathrm{W}_N\rangle. \tag{2.25}$$

The set of equations to solve growing exponentially with the number of qubits, we consider first the 2 and 3 qubits cases. In the 2-qubit case, the states $|\mathrm{W}_2\rangle$ and $|\mathrm{GHZ}_2\rangle$ are SLOCC-equivalent. As a consequence, all the nonsymmetric stabilizers of the state $|\mathrm{GHZ}_2\rangle$ identified in [35] induce nonsymmetric stabilizers for the state $|\mathrm{W}_2\rangle$, and we thus expect the state $|\mathrm{W}_2\rangle$ to have stabilizers differing from the Jordan stabilizer (2.10). In this case, Eq. (2.25) contains 8 complex parameters. We parametrize this equation as follows:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} |\mathrm{W}_2\rangle = |\mathrm{W}_2\rangle, \tag{2.26}$$

with $a_{11}, a_{12}, a_{21}, a_{22}, b_{11}, b_{12}, b_{21}, b_{11} \in \mathbb{C}$ such that $a_{11}a_{22} - a_{12}a_{21} \neq 0$ and $b_{11}b_{22} - b_{12}b_{21} \neq 0$. The corresponding system of 4 equations is not difficult to solve. It admits a general solution corresponding to the stabilizer

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{11} & -a_{12} \\ -a_{21} & a_{22} \end{pmatrix} |\mathrm{W}_2\rangle = |\mathrm{W}_2\rangle, \tag{2.27}$$

with $a_{11}, a_{12}, a_{21}, a_{22}$ any complex numbers such that $a_{11}a_{22} - a_{12}a_{21} \neq 0$. In this parametrization, one ILO element of the stabilizer of $|\mathrm{W}_2\rangle$ can be chosen arbitrarily. If A is any 2×2 invertible matrix, this stabilizer can also be written into the simpler form

$$A \otimes \left(\sigma_1 (A^{-1})^T \sigma_1\right) |\mathrm{W}_2\rangle = |\mathrm{W}_2\rangle, \tag{2.28}$$

[3] We exclude here the trivial case of a nonsymmetric ILO made of the tensor product of operators that are all proportional to each other.

with σ_1 the first Pauli matrix. If A is a Jordan matrix, then $\sigma_1(A^{-1})^T\sigma_1$ is simply the inverse of A and we recover the stabilizer (2.10).

For $N > 2$, we expect less degrees of freedom in the stabilizer, as the SLOCC equivalence with the state $|\mathrm{GHZ}_N\rangle$ is lost. We detail here the computation for $N = 3$. In this case, we are looking for solutions of the general equation

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}_{A} \otimes \underbrace{\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}}_{B} \otimes \underbrace{\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}}_{C} |\mathrm{W}_3\rangle = |\mathrm{W}_3\rangle. \tag{2.29}$$

This vector equation is equivalent to the following set of equations

$$\begin{cases} a_{12}\,b_{11}\,c_{11} + a_{11}\,b_{12}\,c_{11} + a_{11}\,b_{11}\,c_{12} = 0 & \text{(2.30a)} \\ a_{12}\,b_{11}\,c_{21} + a_{11}\,b_{12}\,c_{21} + a_{11}\,b_{11}\,c_{22} = 1 & \text{(2.30b)} \\ a_{12}\,b_{21}\,c_{11} + a_{11}\,b_{22}\,c_{11} + a_{11}\,b_{21}\,c_{12} = 1 & \text{(2.30c)} \\ a_{12}\,b_{21}\,c_{21} + a_{11}\,b_{22}\,c_{21} + a_{11}\,b_{21}\,c_{22} = 0 & \text{(2.30d)} \\ a_{22}\,b_{11}\,c_{11} + a_{21}\,b_{12}\,c_{11} + a_{21}\,b_{11}\,c_{12} = 1 & \text{(2.30e)} \\ a_{22}\,b_{11}\,c_{21} + a_{21}\,b_{12}\,c_{21} + a_{21}\,b_{11}\,c_{22} = 0 & \text{(2.30f)} \\ a_{22}\,b_{21}\,c_{11} + a_{21}\,b_{22}\,c_{11} + a_{21}\,b_{21}\,c_{12} = 0 & \text{(2.30g)} \\ a_{22}\,b_{21}\,c_{21} + a_{21}\,b_{22}\,c_{21} + a_{21}\,b_{21}\,c_{22} = 0 & \text{(2.30h)} \end{cases}$$

This system is harder to solve than in the 2-qubit case but we can exploit the permutation invariance of the state $|\mathrm{W}_3\rangle$ to obtain additional equalities. For instance, considering the permutations (AB) and (AC) in Eq. (2.29) yield the vector equations

$$B^{-1}\,A \otimes A^{-1}\,B \otimes \mathbb{1}\,|\mathrm{W}_3\rangle = |\mathrm{W}_3\rangle \tag{2.31}$$

and

$$C^{-1}\,A \otimes \mathbb{1} \otimes A^{-1}\,C\,|\mathrm{W}_3\rangle = |\mathrm{W}_3\rangle, \tag{2.32}$$

respectively, which notably provide the useful equalities

$$a_{11}b_{21} = b_{11}a_{21} \tag{2.33}$$

and

$$a_{11}c_{21} = c_{11}a_{21}. \tag{2.34}$$

If $a_{11} = 0$ in Eqs. (2.33) and (2.34), then we have also $b_{11} = c_{11} = 0$, as $a_{21} = 0$ would not preserve the invertibility of the matrix A. This is however incompatible with Eqs. (2.30b) and (2.30c). As a consequence, a_{11}, b_{11} and c_{11} must be different from zero. These first constraints on the matrix elements show that, by contrast to the 2-qubit case, we cannot build a stabilizer of the state $|\mathrm{W}_3\rangle$ with an arbitrary ILO element.

We now show by contradiction that we must have $a_{21} = b_{21} = c_{21} = 0$, implying that all the ILO elements in any stabilizer of the state $|\mathrm{W}_3\rangle$ must be upper triangular matrices (as it is the case for the stabilizer (2.10)). Let us assume $a_{21} \neq 0$. Multiplying Eq. (2.30h) by a_{11}, Eq. (2.30d) by a_{21} and subtracting the resulting equations, we find

$$b_{21}c_{21}(a_{11}a_{22} - a_{12}a_{21}) = 0. \tag{2.35}$$

Since the invertibility of the matrix A implies $\det(A) = a_{11}a_{22} - a_{12}a_{21} \neq 0$, this equation can only be satisfied if $b_{21} = 0$ or $c_{21} = 0$. In any case, this contradicts Eqs. (2.33) and (2.34) as, given our assumption, a_{21} must be nonzero. The vanishing of a_{21}, which in turn implies the vanishing of b_{21} and c_{21}, is thus required to satisfy Eqs. (2.30a) to (2.30h). This considerably simplifies the resolution of these equations (most of them become even trivial). The general solution can be parametrized by the matrices

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \; B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{11}\frac{a_{22}}{a_{11}} \end{pmatrix}, \; C = \begin{pmatrix} \frac{1}{a_{22}b_{11}} & -\frac{b_{12}a_{11}+a_{12}b_{11}}{a_{11}a_{22}b_{11}^2} \\ 0 & \frac{1}{a_{11}b_{11}} \end{pmatrix}, \tag{2.36}$$

with $a_{11}, a_{22}, b_{11} \in \mathbb{C}_0$ and $a_{12}, b_{12} \in \mathbb{C}$. One ILO element in the stabilizer of the state $|\mathrm{W}_3\rangle$ can thus be any invertible upper triangular matrix. In the second ILO element, we have two degrees of freedom instead of three and the last ILO element is totally fixed by the other matrices.

The procedure we used to solve the system of equations corresponding to the general ILO stabilizer (2.29) generalizes easily to an arbitrary number $N \geq 3$ of qubits. The equalities resulting from the permutation invariance of the state $|\mathrm{W}_N\rangle$, generalizing Eqs. (2.31) and (2.32), imply also that all the ILO elements in any stabilizer of the state $|\mathrm{W}_N\rangle$ must be upper triangular. As a consequence, in the system of equations generalizing System (2.30) to the N-qubit case, all equations are trivial, except the first one and the N equations with a nonzero right-hand side. Choosing to solve these N equations leaving free all elements of one of the matrices fixes the lower right elements of all the other matrices, plus the upper left element in one of the matrices. Using the only remaining free element in this matrix to solve the last equation (the first of the system), we get the general stabilizer

$$A \otimes B_1 \otimes B_2 \otimes \cdots \otimes B_{N-2} \otimes C \; |\mathrm{W}_N\rangle = |\mathrm{W}_N\rangle \tag{2.37}$$

with

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \tag{2.38}$$

$$B_i = \begin{pmatrix} b_{i1} & b_{i2} \\ 0 & b_{i1}\frac{a_{22}}{a_{11}} \end{pmatrix}, \tag{2.39}$$

$$C = \left(D_2 \, A \, D_1 \, B_1 \, D_1 \, B_2 \, D_1 \cdots B_{N-2} \, D_1 \right)^{-1}, \tag{2.40}$$

$$D_1 = \begin{pmatrix} 1 & 0 \\ 0 & \frac{a_{11}}{a_{22}} \end{pmatrix}, D_2 = \begin{pmatrix} \frac{a_{22}}{a_{11}} & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.41}$$

where $a_{11}, a_{22}, b_{i1} \in \mathbb{C}_0, \; \forall \, i = 1, \ldots, N-2$ and $a_{12}, b_{i2} \in \mathbb{C}, \; \forall \, i = 1, \ldots, N-2$.

The most general stabilizer of the state $|\mathrm{W}_N\rangle$ contains thus more free parameters than the Jordan stabilizer (2.10). Unfortunately, the drawback of getting more independent parameters is that the stabilizer has necessarily a nontrivial action on each qubit state. The only way of having a trivial action (corresponding to the identity operation) on at least one qubit state is to set $a_{11} = a_{22}$, which gives a stabilizer equivalent to several applications of the Jordan stabilizer. This is unfortunately a strong limiting factor for the improvement of Proposition 2.1 using this general stabilizer.

Chapter 3

Separability criterion based on generalized concurrences

From his work on non-locality and hidden variable models, J. Bell already proposed [3] in 1964 a way to test whether a given quantum state is entangled through an inequality involving correlations between measurement outcomes. The second breakthrough in the field of entanglement detection came more than 30 years later through a necessary condition of separability proposed by A. Peres [27]. This separability condition, known as the PPT criterion [27], rapidly became the most standard tool for entanglement detection. In his proof, A. Peres had left open the possibility for the PPT criterion to be also a sufficient condition of separability, in which case it would entirely solve the separability problem. Paradoxically, a proof that the PPT criterion *cannot* solve the general separability problem was given in a paper showing that the PPT criterion is a necessary and sufficient separability condition for 2-qubit states and hybrid states of one qubit and one qutrit [31]. Among the separability criteria that were later proposed, few provide a necessary and sufficient condition of separability, even in low-dimensional systems. For instance, whereas the *Range criterion* [49] and the *CCNR criterion* [50, 51] allow to detect many entangled states for which the PPT criterion fails [33, 49], these criteria do not provide necessary and sufficient conditions of separability, even for 2-qubit states [52].

Following another line, necessary and sufficient conditions of separability can be obtained from entanglement measures. This is for instance the case of the *concurrence*, which was introduced in Ref. [53] to quantify the entanglement of mixed states of 2-qubits. As the concurrence vanishes only for separable states [54], it can also be used to detect all 2-qubit entangled states. The 2-qubit concurrence was then generalized to general bipartite [55] and multipartite [56] systems. However, the entanglement measures provided by these generalized versions of the concurrence only yield a necessary and sufficient condition of separability for pure states [56].

In this chapter, we first refine the generalizations of the concurrence of Refs. [55, 56] by the introduction of *independent generalized concurrences*. We then extend a matrix reformulation of concurrences for bipartite states [55, 57] to the general multipartite case and show that the general separability problem is equivalent to a pure matrix analysis problem that consists in determining whether a given set of symmetric matrices are simultaneously *hollowisable*, i.e. simultaneously unitarily congruent to matrices with a diagonal only composed of zeroes. Finally, from the resolution of this mathematical problem for low dimensional matrices, we state practical separability criteria for general multipartite states of ranks 2 and 3. Low rank states are not only interesting because of their reduced theoretical complexity, they can also be produced in experiments [58]. In some cases, producing low-rank states even appears to be an advantage, for instance to increase the practicability of quantum state tomography [59]. To conclude this introduction, let us also mention that some of the results presented in this chapter have been published in Ref. [60].

This chapter is structured as follows. In Section 3.1, we remind the definition and the properties of the 2-qubit concurrence. We present its generalization to general multipartite systems in Section 3.2, where we also show how to obtain independent generalized concurrences. In Section 3.3, we introduce the preconcurrence matrix formalism and show how it can be used to obtain a simple criterion for the vanishing of any generalized concurrence. In Section 3.4, we prove that the separability problem is equivalent to a simultaneous hollowisation problem. We investigate this mathematical problem for 2×2 matrices in Section 3.5 and obtain a separability criterion for mixed states of rank 2. In Section 3.6, we extend these results to 3×3 matrices and mixed states of rank 3. Finally, in Section 3.7, we consider the specific problem of the hollowisation of diagonal matrices.

3.1 The 2-qubit concurrence

The 2-qubit concurrence [53, 54] is a function that compares the states of a 2-qubit system before and after a *spin-flip* operation. Such an operation transforms a 2-qubit pure state $|\psi\rangle$ into the "spin-flipped" state

$$|\widetilde{\psi}\rangle = S\,|\psi^*\rangle, \tag{3.1}$$

where $S \equiv \sigma_y \otimes \sigma_y$ is the spin-flip operator, with σ_y the second Pauli matrix, and $|\psi^*\rangle$ is obtained by conjugating the components of the state $|\psi\rangle$ expressed in the computational basis. For a spin-$\frac{1}{2}$ particle, this transformation corresponds to the time reversal operation, which actually reverses the direction of the spin [61], hence the name of the operation. The concurrence of the state $|\psi\rangle$ corresponds merely to the modulus of its overlap with the state $|\widetilde{\psi}\rangle$:

$$C(\psi) = |\langle\psi|S|\psi^*\rangle|. \tag{3.2}$$

The concurrence had originally been introduced [53] as an intermediate step to compute the entanglement of formation [16] of 2-qubit states. The *entanglement of formation* E_f is an entanglement measure defined for bipartite pure states as the Von Neumann entropy of the reduced density operator corresponding to either of the subsystems. Given a 2-qubit pure state $|\psi\rangle$, if we denote by $\rho_1 = \mathrm{Tr}_2(|\psi\rangle\langle\psi|)$ the reduced density operator corresponding to the first qubit and by $\rho_2 = \mathrm{Tr}_1(|\psi\rangle\langle\psi|)$ the reduced density operator corresponding to the second qubit, we have

$$E_f(\psi) = -\mathrm{Tr}(\rho_1 \log_2 \rho_1) = -\mathrm{Tr}(\rho_2 \log_2 \rho_2). \tag{3.3}$$

The entanglement of formation is related to the concurrence through the relation [54]

$$E_f(\psi) = \mathcal{E}(C(\psi)), \tag{3.4}$$

where

$$\mathcal{E}(C) = h\left(\frac{1+\sqrt{1-C^2}}{2}\right), \tag{3.5}$$

with

$$h(x) = -x \log_2 x - (1-x)\log_2(1-x). \tag{3.6}$$

The Equation (3.4) shows that the entanglement of formation is a monotonic function of the concurrence. As both functions vanish only for product states, this implies that the concurrence itself can also be used to faithfully quantify entanglement. The interest of the concurrence becomes however clearer when considering mixed states.

For any 2-qubit mixed state ρ, the definitions of the concurrence and the entanglement of formation can be extended through the convex-roof constructions:

$$C(\rho) = \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(\psi_i) \tag{3.7}$$

and

$$E_f(\rho) = \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i E_f(\psi_i), \tag{3.8}$$

where the two infima are computed over all possible decompositions of ρ, i.e. all sets $\{p_i, |\psi_i\rangle\}$ such that $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. The optimizations implied by such convex-roof constructions are generally difficult to compute (even for 2-qubit systems). In the case of the concurrence, however, it was shown [54] that the optimization over all decompositions is simply given by

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{3.9}$$

where $\lambda_1, \ldots, \lambda_4$ are the square roots of the eigenvalues of the operator $\rho S \rho^* S$ (with $\rho^* = |\psi^*\rangle\langle\psi^*|$), sorted in decreasing order.

The Equation (3.9) has two important consequences. On the one hand, it allows to easily compute the entanglement of formation of any 2-qubit state ρ, as, for convexity

reasons, we have $E_f(\rho) = \mathcal{E}(C(\rho))$ [54]. On the other hand, it provides the following practical separability criterion for 2-qubit states.

Theorem 3.1 (Wootters [54]). *A mixed state of two qubits with density operator ρ is separable if and only if $C(\rho) = 0$, which is the case if and only if*

$$\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 \leq 0, \tag{3.10}$$

where $\lambda_1, \ldots, \lambda_4$ are the square roots of the eigenvalues of the operator $\rho S \rho^* S$, sorted in decreasing order.

With the hope of finding new separability criteria, the 2-qubit concurrence was quickly generalized to general bipartite [55] and multipartite systems [56], by the introduction of a set of *generalized concurrences*. We detail this in the next section.

3.2 Entanglement detection from generalized concurrences

Even though the 2-qubit spin-flip operation can straightforwardly be extended to N-qubit systems, for any even N [62], by considering the spin-flip operator $S^{(N)} = \sigma_y^{\otimes N}$, the corresponding N-qubit concurrence $C^{(N)}(\psi) = |\langle\psi|S^{(N)}|\psi^*\rangle|$ (called N-tangle in Ref. [62]) does not provide an extension of the separability criterion of Theorem 3.1 to multiqubit states. For instance, whereas the entangled 4-qubit state $|\mathrm{GHZ}_4\rangle$ has $C^{(4)}(\mathrm{GHZ}_4) = 1$, the entangled 4-qubit Dicke state $|D_4^{(1)}\rangle$ has a vanishing 4-qubit concurrence, just as the 4-qubit product state $|0000\rangle$.

In any multipartite system associated to a Hilbert space $\mathcal{H}$ with $\dim(\mathcal{H}) > 4$, a single concurrence is not enough to detect all entangled states. A separability criterion inspired by the 2-qubit concurrence can nevertheless be obtained by the introduction of a set of generalized concurrences C_α ($\alpha = 1, 2, \ldots$), defined similarly as in Eq. (3.2), but each with a specific generalized "spin-flip" operator S_α [55, 56]. In this section, we first detail an efficient method for generating the minimal number of generalized concurrences required to obtain a necessary and sufficient separability condition for pure states. We then illustrate this generation method for a specific Hilbert space and finally address the case of mixed states.

3.2.1 Independent generalized concurrences for pure states

The generalized "spin-flip" operators S_α introduced in Refs. [55, 56] to build generalized concurrences are generated either from tensor products of $\mathrm{SO}(n)$ generators [56] or from 2×2 minor equations from tensor matricizations [55, 63]. Both methods unfortunately produce highly redundant sets of operators. Here, we show how to extract from them the only independent operators. For this purpose, we make use of the 2×2 minor

equations method [55], as it is better suited for this task. We consider an arbitrary multipartite system with Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N$, where $\mathcal{H}_j$ $(j = 1, \ldots, N)$ are the individual Hilbert spaces of dimension $m_j \geq 2$ for each party. In the computational basis $|\mathbf{i}\rangle \equiv |i_1, \ldots, i_N\rangle \equiv |i_1\rangle \otimes \cdots \otimes |i_N\rangle$, with $i_j = 0, \ldots, m_j - 1$ $(j = 1, \ldots, N)$, any pure state $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \sum_{\mathbf{i}} a_{\mathbf{i}} |\mathbf{i}\rangle \equiv \sum_{i_1=0}^{m_1-1} \cdots \sum_{i_N=0}^{m_N-1} a_{i_1,\ldots,i_N} \, |i_1, \ldots, i_N\rangle. \tag{3.11}$$

The state $|\psi\rangle$ is separable if and only if the N-order tensor A with components $a_{\mathbf{i}} \equiv a_{i_1,\ldots,i_N}$ is of rank 1 [64]. This is the case if and only if all mode-k matricizations $A^{(k)}$ of A $(k = 1, \ldots, N)$ are themselves of rank 1 [64]. The mode-k matricization $A^{(k)}$ of A is the $m_k \times \dim\mathcal{H}/m_k$ matrix whose columns are indexed by all possible values of $\mathbf{i}_{\neg k} \equiv (i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_N)$ and filled with the corresponding elements $a_{\mathbf{i}}$ with i_k ranging from 0 to $m_k - 1$. The N mode-k matricizations of A are of rank 1 if and only if all their 2×2 minors vanish, i.e. if and only if

$$a_{\mathbf{i}} a_{\mathbf{i}'} = a_{\mathbf{i}_{[i'_k]}} a_{\mathbf{i}'_{[i_k]}}, \quad \forall k, \forall \mathbf{i}, \mathbf{i}' : i'_k > i_k, \mathbf{i}'_{\neg k} > \mathbf{i}_{\neg k}, \tag{3.12}$$

where $\mathbf{i}_{[i'_k]} \equiv (i_1, \ldots, i_{k-1}, i'_k, i_{k+1}, \ldots, i_N)$, $\mathbf{i}'_{[i_k]} \equiv (i'_1, \ldots, i'_{k-1}, i_k, i'_{k+1}, \ldots, i'_N)$, and $\mathbf{i}'_{\neg k} > \mathbf{i}_{\neg k}$ means that at least one component of $\mathbf{i}'_{\neg k}$ differs from its equivalent in $\mathbf{i}_{\neg k}$ and that the first of these differing components is greater for $\mathbf{i}'_{\neg k}$ than for $\mathbf{i}_{\neg k}$. If we introduce the generalized concurrences

$$C_{k,\mathbf{i},\mathbf{i}'}(\psi) \equiv |\langle\psi| S_{k,\mathbf{i},\mathbf{i}'} |\psi^*\rangle| \tag{3.13}$$

with

$$S_{k,\mathbf{i},\mathbf{i}'} = |\mathbf{i}\rangle\langle\mathbf{i}'| - |\mathbf{i}_{[i'_k]}\rangle\langle\mathbf{i}'_{[i_k]}| + \text{h.c.}, \tag{3.14}$$

then Eq. (3.12) is equivalent to

$$C_{k,\mathbf{i},\mathbf{i}'}(\psi) = 0, \quad \forall k, \forall \mathbf{i}, \mathbf{i}' : i'_k > i_k, \mathbf{i}'_{\neg k} > \mathbf{i}_{\neg k}. \tag{3.15}$$

This expresses a necessary and sufficient condition (NSC) of separability for the multipartite pure state $|\psi\rangle$.

The total number of generalized concurrences implied by Eq. (3.15) amounts to $\sum_{k=1}^{N} \binom{m_k}{2} \binom{\dim\mathcal{H}/m_k}{2}$, which simplifies to $Nd^N(d^{N-1}-1)(d-1)/4$ for an N-qudit system (i.e. $m_k = d$, $\forall k$). Actually, many of these concurrences are redundant, if not identical, and they do not cancel independently of each other. It is useful to identify a minimal set of these equalities that provides equivalently an NSC of separability. To this aim, we first introduce some notations. In Eq. (3.12), the conditions $i'_k > i_k$ and $\mathbf{i}'_{\neg k} > \mathbf{i}_{\neg k}$ imply that the indexes $\mathbf{i}$ and $\mathbf{i}'$ in an equality necessarily differ in a number of components greater than or equal to 2. Let $q_{\mathbf{i},\mathbf{i}'}$ be this number of different components and $\mathcal{Q}_{\mathbf{i},\mathbf{i}'}$ the set gathering their positions: $\mathcal{Q}_{\mathbf{i},\mathbf{i}'} = \{\, k : \, i_k \neq i'_k \}$ and $q_{\mathbf{i},\mathbf{i}'} = \#\mathcal{Q}_{\mathbf{i},\mathbf{i}'}$. The (possibly

empty) complement $\overline{\mathcal{Q}}_{\mathbf{i},\mathbf{i}'}$ is the set $\{\, k \,:\, i_k = i'_k\}$. We then define the two $q_{\mathbf{i},\mathbf{i}'}$-tuples $\mathbf{d}_{\mathbf{i},\mathbf{i}'} \equiv (i_{(\mathcal{Q}_{\mathbf{i},\mathbf{i}'})_1}, \ldots, i_{(\mathcal{Q}_{\mathbf{i},\mathbf{i}'})_{q_{\mathbf{i},\mathbf{i}'}}})$ and $\mathbf{d}'_{\mathbf{i},\mathbf{i}'} \equiv (i'_{(\mathcal{Q}_{\mathbf{i},\mathbf{i}'})_1}, \ldots, i'_{(\mathcal{Q}_{\mathbf{i},\mathbf{i}'})_{q_{\mathbf{i},\mathbf{i}'}}})$, as well as, if $q_{\mathbf{i},\mathbf{i}'} \neq N$, the $(N-q_{\mathbf{i},\mathbf{i}'})$-tuple $\mathbf{c}_{\mathbf{i},\mathbf{i}'} \equiv (i_{(\overline{\mathcal{Q}}_{\mathbf{i},\mathbf{i}'})_1}, \ldots, i_{(\overline{\mathcal{Q}}_{\mathbf{i},\mathbf{i}'})_{N-q_{\mathbf{i},\mathbf{i}'}}})$, where $(\mathcal{A})_k$ denotes the k-th element of the set $\mathcal{A}$ ($\mathcal{A} = \mathcal{Q}_{\mathbf{i},\mathbf{i}'}, \overline{\mathcal{Q}}_{\mathbf{i},\mathbf{i}'}$).

We then structure the set of equalities of Eq. (3.12) into subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$ that each gather all equalities with index couples $(\mathbf{i},\mathbf{i}')$ said $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$-compatible, i.e. such that $\mathcal{Q}_{\mathbf{i},\mathbf{i}'} = \mathcal{Q}$, $\mathbf{c}_{\mathbf{i},\mathbf{i}'} = \mathbf{c}$ and $(\mathbf{d}_{\mathbf{i},\mathbf{i}'}, \mathbf{d}'_{\mathbf{i},\mathbf{i}'}) = (\mathbf{d}, \mathbf{d}')$ up to swaps of $\mathbf{d}'$ components with their related components in $\mathbf{d}$. We have $\#\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')} = q2^{q-2}$, with $q = \#\mathcal{Q}$. In each subset $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$, one easily checks that the number of distinct pairs $\{\mathbf{i},\mathbf{i}'\}$ and $\{\mathbf{i}_{[i'_k]}, \mathbf{i}'_{[i_k]}\}$ amounts together to 2^{q-1} and that the number of independent equalities is equal to $2^{q-1}-1$. The independent equalities of each subset $\mathcal{S}$ remain all independent when the subsets are grouped together. To see this, let us consider an arbitrary equality indexed by $(k,\mathbf{i},\mathbf{i}')$ and belonging to a subset $\mathcal{S}$, and let us show that it is independent from all equalities of any other subsets $\mathcal{S}'$. To this end, we consider the state $|\psi\rangle = a_{\mathbf{i}}|\mathbf{i}\rangle + a_{\mathbf{i}'}|\mathbf{i}'\rangle$. For this state, all equalities of any subset $\mathcal{S}' \neq \mathcal{S}$ are trivially satisfied since they read $0 = 0$, while the equality $(k,\mathbf{i},\mathbf{i}')$ of $\mathcal{S}$ reads $a_{\mathbf{i}}a_{\mathbf{i}'} = 0$. Hence, the separability of the state (which requires here $a_{\mathbf{i}} = 0$ or $a_{\mathbf{i}'} = 0$) can only be certified with the help of this latter equality, which must therefore be independent from the equalities from the other subsets. It follows that the total number of independent equalities amounts to

$$Q(\mathcal{H}) = \sum_{q=2}^{N} \left(2^{q-1}-1\right) \sum_{\substack{\mathcal{Q}_{\mathbf{i},\mathbf{i}'}:\\ q_{\mathbf{i},\mathbf{i}'}=q}} \prod_{k=1}^{q} \binom{m_{(\mathcal{Q}_{\mathbf{i},\mathbf{i}'})_k}}{2} \prod_{k=1}^{N-q} m_{(\overline{\mathcal{Q}}_{\mathbf{i},\mathbf{i}'})_k}, \tag{3.16}$$

that simplifies to

$$Q((\mathbb{C}^d)^{\otimes N}) = d^{N+1}\frac{d-1}{4}\left(1 - 2\left(1+\frac{1}{d}\right)^N + \left(1+\frac{2}{d}\right)^N\right) \tag{3.17}$$

for an N-qudit system.

Rather than generating all the equalities and then discarding the redundant ones, it is more efficient to directly generate only the independent ones. Such an equivalent set of independent equalities is obtained if, in each subset $\mathcal{S}$, we rather consider the equalities $a_{\mathbf{i}}a_{\mathbf{i}'} = a_{\mathbf{j}}a_{\mathbf{j}'}$, with $(\mathbf{i},\mathbf{i}')$ any fixed $\mathcal{S}$-compatible index couple and $(\mathbf{j},\mathbf{j}')$ all possible $\mathcal{S}$-compatible index couples distinct from $(\mathbf{i},\mathbf{i}')$ and such that $(\mathbf{d}_{\mathbf{j},\mathbf{j}'}, \mathbf{d}'_{\mathbf{j},\mathbf{j}'}) = (\mathbf{d}_{\mathbf{i},\mathbf{i}'}, \mathbf{d}'_{\mathbf{i},\mathbf{i}'})$ up to swaps of any components but the last of $\mathbf{d}'_{\mathbf{i},\mathbf{i}'}$ with their equivalents in $\mathbf{d}_{\mathbf{i},\mathbf{i}'}$. All these equalities can be equivalently written

$$C_{(\mathbf{i},\mathbf{i}'),(\mathbf{j},\mathbf{j}')}(\psi) = 0, \tag{3.18}$$

with the generalized concurrences

$$C_{(\mathbf{i},\mathbf{i}'),(\mathbf{j},\mathbf{j}')}(\psi) = |\langle\psi|S_{(\mathbf{i},\mathbf{i}'),(\mathbf{j},\mathbf{j}')}|\psi^*\rangle|, \tag{3.19}$$

where

$$S_{(\mathbf{i},\mathbf{i}'),(\mathbf{j},\mathbf{j}')} = |\mathbf{i}\rangle\langle\mathbf{i}'| - |\mathbf{j}\rangle\langle\mathbf{j}'| + \text{h.c.} \tag{3.20}$$

The Equalities (3.18) are hereafter merely indexed by the subscript $\alpha = 1, \ldots, Q(\mathcal{H})$ and similarly for all related generalized concurrences (3.19) and generalized spin-flip operators (3.20). The NSC of separability (3.15) for pure states can then be refined accordingly:

Theorem 3.2. *A general N-partite pure state $|\psi\rangle$ in $\mathcal{H} = \mathbb{C}^{m_1} \otimes \cdots \otimes \mathbb{C}^{m_N}$ ($m_j \geq 2$ for all $j = 1, \ldots, N$) is separable if and only if $C_\alpha(\psi) = 0$, $\forall \alpha = 1, \ldots, Q(\mathcal{H})$.*

Even though the number $Q(\mathcal{H})$ of independent generalized concurrences C_α quickly grows with the number of parties and dimensions of the subsystem spaces, the elimination of all redundancies is not anecdotal. The gain obtained by considering independent generalized concurrences instead of all generalized concurrences can for instance be estimated from the fraction of independent generalized concurrences, i.e. the quotient between the number of independent generalized concurrences $Q^{\text{indep}}(\mathcal{H})$ and the total number of generalized concurrence $Q^{\text{SO}(n)}(\mathcal{H})$ or $Q^{\text{minors}}(\mathcal{H})$, depending on the generation method. For multiqubit systems of between 2 and 20 qubits, the fraction of independent generalized concurrences for both methods can be seen in Fig. 3.1. For both methods, this fraction

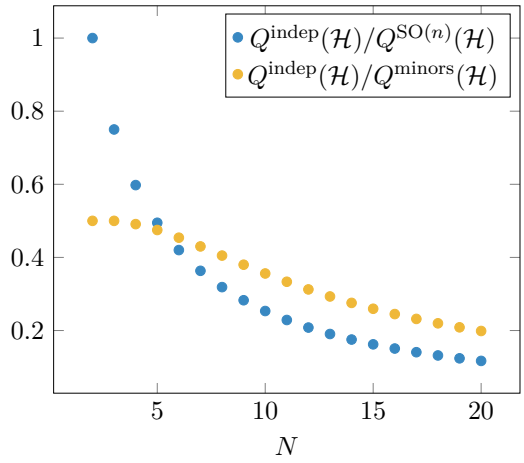


Figure 3.1: Fraction of independent generalized concurrences in multiqubit systems as a function of the number of qubits N in the system (between 2 and 20). The fraction of independent generalized concurrences is shown for both the SO(n) generators generation method (blue dots) and the 2×2 minors generation method (yellow dots).

decreases as the number of qubits increases. In a 20-qubit system, for instance, around a

fifth of the concurrences generated from 2×2 minors are independent, and this proportion even drops to a tenth for the SO(n) generators method. The comparison between the two methods in Fig. 3.1 also reveals that, for systems of less than 6 qubits, it is the SO(n) generators methods that produces the less redundant generalized concurrences, whereas for larger multiqubit systems, it is the 2×2 minors method that is more efficient.

For multiqudit systems, the gain obtained by considering independent generalized concurrences is even greater. This can be seen in Fig. 3.2, where the fraction of independent generalized concurrences for the 2×2 minors method is represented for multiqudit systems with $d = 2, 3, 4, 5$. Although there is a clear gap between the curves corresponding to $d = 2$ (i.e. to qubits) and $d = 3$, the fraction of independent generalized concurrences stabilizes for multiqudit systems with larger subsystem dimensions.

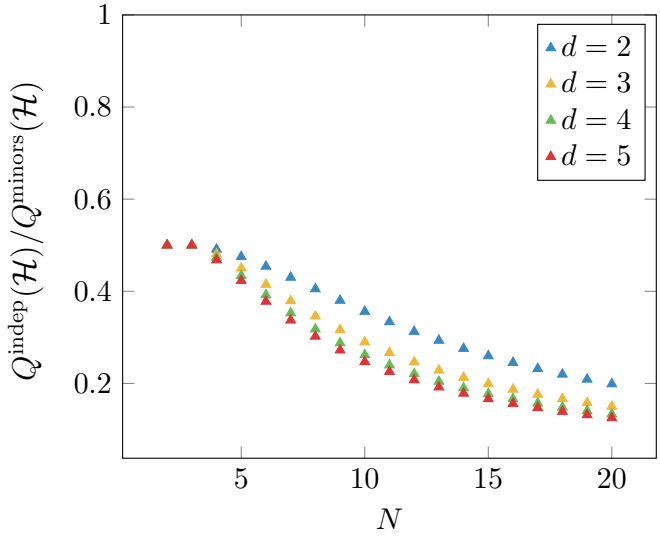


Figure 3.2: Fraction of independent generalized concurrences in several N-qudit systems for the 2×2 minors generation method, as a function of the number of parties (between 2 and 20). The fraction of independent concurrences is represented for dimensions of the subsystems ranging from 2 to 5.

Before addressing the case of mixed states, we illustrate our generation method with an example.

3.2.2 Illustrative example for $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$

We illustrate here our method for generating the independent generalized concurrences in the hybrid system associated to the Hilbert space $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, and thus composed of one qutrit and two qubits. We have chosen to consider the less frequent case of an hybrid

system rather than a multiqudit system to show the philosophy behind the generation method in full generality.

As explained below Eq. (3.17), our method for the generation of the independent generalized concurrences requires to find, for all distinct subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$, one $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$-compatible index couple $(\mathbf{i},\mathbf{i}')$ and then build all independent generalized concurrences $C_{(\mathbf{i},\mathbf{i}'),(\mathbf{j},\mathbf{j}')}$ with $(\mathbf{j},\mathbf{j}')$ all possible $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$-compatible index couples distinct from $(\mathbf{i},\mathbf{i}')$ and such that $(\mathbf{d}_{\mathbf{j},\mathbf{j}'},\mathbf{d}'_{\mathbf{j},\mathbf{j}'}) = (\mathbf{d}_{\mathbf{i},\mathbf{i}'},\mathbf{d}'_{\mathbf{i},\mathbf{i}'})$ up to swaps of any components but the last of $\mathbf{d}'_{\mathbf{i},\mathbf{i}'}$ with their equivalents in $\mathbf{d}_{\mathbf{i},\mathbf{i}'}$. We choose here to span the subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$ according to the parameter $q = \#\mathcal{Q}$. Since the set $\mathcal{Q}$ must contain at least 2 elements, we have only two possibilities for q in our tripartite example, namely $q = 2$ or $q = 3$. We begin with the case $q = 2$.

- $\mathbf{q = 2}$

  In this case, the subset $\mathcal{Q}$ is any subset of two elements in $\{1,2,3\}$, so that we have the three possibilities $\mathcal{Q} = \{1,2\}$, $\mathcal{Q} = \{1,3\}$ or $\mathcal{Q} = \{2,3\}$. As a reminder, this set contains the positions (in the list of the parties) associated to each element of the q-tuples $\mathbf{d}$ and $\mathbf{d}'$, while the complementary subset $\overline{\mathcal{Q}}$ contains the positions associated to the elements of the $(N-q)$-tuple $\mathbf{c}$.

  For $\mathcal{Q} = \{1,2\}$, the 2-tuples $\mathbf{d}$ and $\mathbf{d}'$ contain thus computational basis indices corresponding to the qutrit and the first qubit, while the 1-tuple $\mathbf{c}$ contains a computational basis index corresponding to the second qubit. For the 1-tuple $\mathbf{c}$, there are simply two possibilities: $\mathbf{c} = (0)$ or $\mathbf{c} = (1)$. For the 2-tuples $\mathbf{d}$ and $\mathbf{d}'$, remembering that the elements of $\mathbf{d}$ must always differ from their respective counterpart in $\mathbf{d}'$ and that distinct couples $(\mathbf{d_1},\mathbf{d'_1})$ and $(\mathbf{d_2},\mathbf{d'_2})$ that differ only by swaps between corresponding elements lead to the same subset $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$, we find three couples $(\mathbf{d},\mathbf{d}')$ corresponding to distinct subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$, namely $(\mathbf{d},\mathbf{d}') = ((0,0),(1,1))$, $(\mathbf{d},\mathbf{d}') = ((0,0),(2,1))$ and $(\mathbf{d},\mathbf{d}') = ((1,0),(2,1))$.

  Combining these possibilities, we find 6 distinct subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$ having $\mathcal{Q} = \{1,2\}$. A compatible index couple $(\mathbf{i},\mathbf{i}')$ is easily associated to each of these subsets. For instance, for the subset $\mathcal{S}_{\{1,2\},(0),((0,0),(1,1))}$, we get the index couple $(\mathbf{i},\mathbf{i}') = (000,110)$. As $\mathbf{d}_{\mathbf{i},\mathbf{i}'}$ and $\mathbf{d}'_{\mathbf{i},\mathbf{i}'}$ contain here only two elements, there is only one way of finding a compatible index couple $(\mathbf{j},\mathbf{j}')$ (distinct from $(\mathbf{i},\mathbf{i}')$) by swaps of any components but the last of $\mathbf{d}'_{\mathbf{i},\mathbf{i}'}$ with their equivalents in $\mathbf{d}_{\mathbf{i},\mathbf{i}'}$ (we can here only swap the first component in $\mathbf{d}'_{\mathbf{i},\mathbf{i}'}$ and $\mathbf{d}_{\mathbf{i},\mathbf{i}'}$). For instance, for $(\mathbf{i},\mathbf{i}') = (000,110)$, we can only have $(\mathbf{j},\mathbf{j}') = (100,010)$. For the 6 subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$ previously identified, we thus find the 6 independent generalized concurrences $C_{(000,110),(100,010)}$, $C_{(001,111),(101,011)}$, $C_{(000,210),(200,010)}$, $C_{(001,211),(201,011)}$, $C_{(100,210),(200,110)}$ and $C_{(101,211),(201,111)}$.

  For $\mathcal{Q} = \{1,3\}$, the 2-tuples $\mathbf{d}$ and $\mathbf{d}'$ contain computational basis indices corresponding to the qutrit and the second qubit, while the 1-tuple $\mathbf{c}$ contains a computational basis index corresponding the first qubit. We thus find the same generalized

concurrences up to a swap between the computational basis indices of the two qubits. This leads to the independent concurrences $C_{(000,101),(100,001)}$, $C_{(010,111),(110,011)}$, $C_{(000,201),(200,001)}$, $C_{(010,211),(210,011)}$, $C_{(100,201),(200,101)}$ and $C_{(110,211),(210,111)}$.

Finally, for $\mathcal{Q} = \{2, 3\}$, the 2-tuples $\mathbf{d}$ and $\mathbf{d}'$ contain computational basis indices corresponding to the two qubits, while the 1-tuple $\mathbf{c}$ contains a computational basis index corresponding to the qutrit. This leads to the following three possibilities for the 1-tuple $\mathbf{c}$: $\mathbf{c} = (0)$, $\mathbf{c} = (1)$ or $\mathbf{c} = (2)$. For the couple $(\mathbf{d}, \mathbf{d}')$, there is only one distinct possibility, namely $(\mathbf{d}, \mathbf{d}')$=$((0, 0), (1, 1))$. Again, since $\mathbf{d}$ and $\mathbf{d}'$ contain here only two elements, we can only swap their first element to get an index couple $(\mathbf{j}, \mathbf{j}')$ from any $\mathcal{S}_{\{2,3\},\mathbf{c},(\mathbf{d},\mathbf{d}')}$-compatible $(\mathbf{i}, \mathbf{i}')$ couple. The three resulting independent concurrences read $C_{(000,011),(010,001)}$, $C_{(100,111),(110,101)}$ and $C_{(200,211),(210,201)}$.

- $\mathbf{q = 3}$

  When $q = 3$, we necessarily have $\mathcal{S} = \{1, 2, 3\}$. The complement of $\mathcal{S}$ is thus empty and there is no tuple $\mathbf{c}$ to consider. A first possibility for the 3-tuples $\mathbf{d}$ and $\mathbf{d}'$ is $\mathbf{d} = (0, 0, 0)$, $\mathbf{d}' = (1, 1, 1)$, for which we simply have $(\mathbf{i}, \mathbf{i}') = (000, 111)$ as compatible index couple. As there are now three elements in $\mathbf{d}$ and $\mathbf{d}'$, three distinct swaps among the first two elements in $\mathbf{d}$ and $\mathbf{d}'$ can be performed to get compatible index couples $(\mathbf{j}, \mathbf{j}')$. This leads to the three independent concurrences $C_{(000,111),(100,011)}$, $C_{(000,111),(010,101)}$ and $C_{(000,111),(110,001)}$.

  Another possibility for $\mathbf{d}$ and $\mathbf{d}'$ is $\mathbf{d} = (0, 0, 0)$, $\mathbf{d}' = (2, 1, 1)$, for which we simply have $(\mathbf{i}, \mathbf{i}') = (000, 211)$ as compatible index couple. The swaps among the first two components lead to the independent concurrences $C_{(000,211),(200,011)}$, $C_{(000,211),(010,201)}$ and $C_{(000,211),(210,001)}$.

  Finally, the last possibility for 3-tuples $\mathbf{d}$ and $\mathbf{d}'$ leading to a distinct subsets $\mathcal{S}_{\{1,2,3\},(\mathbf{d},\mathbf{d}')}$ corresponds to $\mathbf{d} = (1, 0, 0)$ and $\mathbf{d}' = (2, 1, 1)$. In this case, we have the compatible index couple $(\mathbf{i}, \mathbf{i}') = (100, 211)$ and the swaps among the first two components lead to the independent concurrences $C_{(100,211),(200,111)}$, $C_{(100,211),(110,201)}$ and $C_{(100,211),(210,101)}$.

These generalized concurrences conclude the span of all incompatible subsets $\mathcal{S}_{\mathcal{Q},\mathbf{c},(\mathbf{d},\mathbf{d}')}$. In total, we found all 24 independent generalized concurrences corresponding to the system with Hilbert space $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. For this system, the global 2×2 minor equations method would have given 48 generalized concurrences and the SO(n) generators method 33 generalized concurrences. This illustrative example concludes our study of the separability of pure states based on generalized concurrences. We now turn to mixed states.

3.2.3 Generalized concurrences for mixed states

Let us now consider a mixed state ρ acting on the same multipartite Hilbert space $\mathcal{H}$. The independent generalized concurrences C_α can be extended to mixed states using the

standard convex-roof construction. For all $\alpha = 1, \ldots, Q(\mathcal{H})$, we define

$$C_\alpha(\rho) = \inf_{\{p_k, |\psi_k\rangle\}} \sum_k p_k \, C_\alpha(\psi_k), \tag{3.21}$$

where the infimum is taken over all possible decompositions of ρ. If ρ is separable, then it admits a decomposition in which each state $|\psi_k\rangle$ is separable. This implies $C_\alpha(\psi_k) = 0$, $\forall \alpha$, $\forall k$ and hence $C_\alpha(\rho) = 0$, $\forall \alpha$. The converse is not true. The cancellation of all concurrences $C_\alpha(\rho)$ implies that for each of them a decomposition exists where the considered concurrence vanishes for each pure state of the decomposition. For different concurrences, however, such decompositions may be different. Therefore, the cancellation of all concurrences $C_\alpha(\rho)$ does not imply that there exists a decomposition for which all concurrences of each pure state of the decomposition vanish. The cancellation of all concurrences is thus a necessary but not sufficient condition of separability for mixed states:

$$\rho \text{ separable} \Rightarrow C_\alpha(\rho) = 0, \forall \alpha. \tag{3.22}$$

For instance, the 3-qubit mixed state

$$\rho = \Big(|D_3^{(0,2)}\rangle\langle D_3^{(0,2)}| + |D_3^{(1,2)}\rangle\langle D_3^{(1,2)}| + |D_3^{(1,3)}\rangle\langle D_3^{(1,3)}| \Big)/3, \tag{3.23}$$

with $|D_3^{(k,k')}\rangle \equiv \big(|D_3^{(k)}\rangle + |D_3^{(k')}\rangle\big)/\sqrt{2}$ for all $k, k' \in \{0, \ldots, 3\}$ $(k \neq k')$, where $|D_3^{(0)}\rangle, \ldots,$ $|D_3^{(3)}\rangle$ denote the four 3-qubit Dicke states (see Section 1.2.3), has a negative semi-definite partial transpose with respect to any qubit and is therefore entangled [27] although all concurrences $C_\alpha(\rho)$ $(\alpha = 1, \ldots, 9)$ vanish for this state (these concurrences are easily computed using Eq. (3.31) hereafter).

To obtain a necessary and sufficient separability condition for mixed states using generalized concurrences, a deeper analysis of the possible decompositions is required. Such an analysis appears to be easier to perform in the so-called *preconcurrence matrix* formalism, which was introduced in Refs. [54, 55, 57] for bipartite systems. In the next section, we extend this formalism to multipartite systems and exploit it to prove a simple necessary and sufficient condition for the cancellation of a given concurrence $C_\alpha(\rho)$.

3.3 Preconcurrence matrices and hollowisability

Given a decomposition $\mathcal{D} = \{p_k, |\psi_k\rangle, k = 1, \ldots, p\}$ of a mixed state ρ acting on the Hilbert space $\mathcal{H}$, we build a preconcurrence matrix $\tau_\alpha^{\mathcal{D}}$ for each generalized concurrence C_α $(\alpha = 1, \ldots, Q(\mathcal{H}))$. Introducing the unnormalized states $|\tilde{\psi}_k\rangle \equiv \sqrt{p_k}|\psi_k\rangle$ so as to write $\rho = \sum_{k=1}^p |\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$, the preconcurrence matrix $\tau_\alpha^{\mathcal{D}}$ is defined as the square $p \times p$ matrix with elements

$$(\tau_\alpha^{\mathcal{D}})_{ij} = \langle\tilde{\psi}_i|S_\alpha|\tilde{\psi}_j^*\rangle, \quad i, j = 1, \ldots, p. \tag{3.24}$$

The preconcurrence matrix is symmetric: $(\tau_\alpha^{\mathcal{D}})^T = \tau_\alpha^{\mathcal{D}}$. Its diagonal elements are the C_α concurrences (up to the absolute value) of the (unnormalized) states $|\tilde{\psi}_k\rangle$ of the decomposition $\mathcal{D}$, hence the name of the matrix.

Of particular interest is the eigendecomposition $\mathcal{E}$ of ρ, i.e. the decomposition of ρ over its eigenvectors $|v_k\rangle$ with nonzero eigenvalues λ_k: $\rho = \sum_{k=1}^r \lambda_k |v_k\rangle\langle v_k| = \sum_{k=1}^r |\tilde{v}_k\rangle\langle\tilde{v}_k|$, with $|\tilde{v}_k\rangle = \sqrt{\lambda_k}|v_k\rangle$ and where r is the rank of ρ. We set $\tau_\alpha \equiv \tau_\alpha^{\mathcal{E}}$. No other decomposition of ρ can contain a number of states smaller than r [21]. For an arbitrary decomposition $\mathcal{D} = \{p_k, |\psi_k\rangle, k = 1, \ldots, p\}$ of ρ, a $p \times p$ unitary matrix U always exists such that[1] $(|\tilde{\psi}_1\rangle, \ldots, |\tilde{\psi}_p\rangle)^T = U^*(|\tilde{v}_1\rangle, \ldots, |\tilde{v}_p\rangle)^T$ with $|\tilde{v}_k\rangle \equiv 0$ for $k > r$ [21]. Applying this decomposition change to the preconcurrence matrix $\tau_\alpha^{\mathcal{D}}$ shows that it is unitarily congruent to the matrix τ_α extended, if $p > r$, with $p - r$ rows and columns only composed of zeroes: $\tau_\alpha^{\mathcal{D}} = U\tau_\alpha^{\text{ext}}U^T$, with τ_α^{ext} the so extended τ_α matrix. Conversely, any $p \times p$ unitary U^* applied on $(|\tilde{v}_1\rangle, \ldots, |\tilde{v}_p\rangle)^T$ defines an alternate decomposition of ρ (containing between r and p pure states) [21] and the preconcurrence matrix related to this decomposition is directly obtained by the corresponding unitary congruence $U\tau_\alpha^{\text{ext}}U^T$.

We now show that this formalism provides a simple necessary and sufficient condition to have $C_\alpha(\rho) = 0$ for a given α. The concurrence $C_\alpha(\rho)$ vanishes if and only if there exists a decomposition $\mathcal{D}$ of ρ such that all the pure states of the decomposition have a vanishing C_α concurrence, or equivalently, such that the preconcurrence matrix $\tau_\alpha^{\mathcal{D}}$ is hollow (i.e. has a diagonal only composed of zeroes). This is indeed the case if there exists an extension τ_α^{ext} of τ_α that is unitarily congruent to a hollow matrix.

As shown in the Lemma 2 of Ref. [65], two symmetric matrices are unitarily congruent if and only if they have the same singular values. A symmetric matrix τ_α^{ext} is therefore unitarily congruent to a symmetric hollow matrix if and only if there exists a symmetric hollow matrix with the same singular values. This problem can be solved using the following theorem of Ref. [65].

Theorem 3.3 (Thompson [65]). *Let $d_1, \ldots, d_n$ be complex numbers, and $s_1, \ldots, s_n$ nonnegative real numbers, enumerated so that*

$$|d_1| \geq \cdots \geq |d_n|\,, \quad s_1 \geq \cdots \geq s_n\,.$$

Then a complex symmetric matrix S exists with $d_1, \ldots, d_n$ as its diagonal elements and $s_1, \ldots, s_n$ as its singular values if and only if

$$\sum_{i=1}^{k} |d_i| \leq \sum_{i=1}^{k} s_i\,, \quad 1 \leq k \leq n, \tag{3.25}$$

$$\sum_{i=1}^{k-1} |d_i| - \sum_{i=k}^{n} |d_i| \leq \sum_{\substack{i=1 \\ i\neq k}}^{n} s_i - s_k\,, \quad 1 \leq k \leq n, \tag{3.26}$$

[1] In this change of decomposition, we use the unitary matrix U^* instead of U for later convenience.

$$\sum_{i=1}^{n-3} |d_i| - |d_{n-2}| - |d_{n-1}| - |d_n| \leq \sum_{i=1}^{n-2} s_i - s_{n-1} - s_n \,, \quad \text{if } n \geq 3. \tag{3.27}$$

The application of this theorem to hollow symmetric matrices (for which $d_i = 0$, $\forall\, i = 1, \ldots, n$) is straightforward: when $n \neq 3$, the Condition (3.26) for $k = 1$ is the only inequality that is not trivially satisfied, and when $n = 3$, the Condition (3.26) for $k = 1$ and the Condition (3.27) can only be fulfilled at the same time if $s_1 - s_2 - s_3 = 0$. This leads to the following corollary.

Corollary 3.1. *There exists a hollow $n \times n$ symmetric matrix with singular values $s_1 \geq \cdots \geq s_n$ if and only if*

$$s_1 - \sum_{i=2}^{n} s_i \leq 0 \ \text{ if } n \neq 3, \tag{3.28}$$

$$s_1 - s_2 - s_3 = 0 \ \text{ if } n = 3\,. \tag{3.29}$$

This corollary provides the desired condition for the existence of a hollow matrix unitarily congruent to the preconcurrence matrix τ_α^{ext} and we have thus a simple criterion to check whether a given concurrence vanishes. Since the nonzero singular values of any extension τ_α^{ext} of τ_α are exactly the same as those of τ_α itself, we merely get that $C_\alpha(\rho) = 0$ if and only if the singular values $s_1, \ldots, s_r$ of τ_α, sorted in decreasing order, verify $s_1 - \sum_{k=2}^{r} s_k \leq 0$. In this case, the symmetric matrix τ_α (or its 4×4 extension in the special case (SC) $r = 3$ and $s_1 - s_2 - s_3 < 0$) is itself unitarily congruent to a hollow matrix (we say *hollowisable*) and a decomposition of ρ over exactly r (or $r + 1$ in the SC) states $|\psi_k\rangle$ with $C_\alpha(\psi_k) = 0, \forall k$ is ensured to exist. In the SC, the symmetric matrix τ_α is itself not hollowisable and a decomposition of ρ over exactly $r = 3$ states $|\psi_k\rangle$ with $C_\alpha(\psi_k) = 0, \forall k$ does not exist. This is the only case in which an extension of the preconcurrence matrix τ_α is required to have unitary congruence to a hollow matrix. We summarize this necessary and sufficient condition for the vanishing of a generalized concurrence C_α in the following theorem.

Theorem 3.4. *A given concurrence C_α of a general N-partite mixed state ρ vanishes if and only if the (symmetric) $r \times r$ preconcurrence matrix $\tau_\alpha \equiv \tau_\alpha^{\mathcal{E}}$ (or its 4×4 extension if $r = 3$) is hollowisable by unitary congruence ($r = \text{rank}\rho$). This is the case if and only if the singular values $s_1, \ldots, s_r$ of τ_α, sorted in decreasing order, satisfy*

$$s_1 - \sum_{k=2}^{r} s_k \leq 0. \tag{3.30}$$

The nonzero singular values of τ_α appear to be identical to the square roots of the nonzero eigenvalues of $\rho S_\alpha \rho^* S_\alpha$, showing that Theorem 3.4 is a direct generalization of Theorem 3.1 to the case of generalized concurrences.

The singular values $s_1, \ldots, s_r$ of τ_α (sorted in decreasing order) actually fully characterize the generalized concurrence $C_\alpha(\rho)$. As a direct generalization of Eq. (3.9), we have

$$C_\alpha(\rho) = \max(0, s_1 - \sum_{k=2}^{r} s_k). \tag{3.31}$$

Indeed, we can first write $C_\alpha(\rho) = \inf_{\mathcal{D}=\{p_k,|\psi_k\rangle\}} \sum_{k=1}^{p} p_k C_\alpha(\psi_k) = \inf_{\mathcal{D}} \sum_k C_\alpha(\tilde{\psi}_k) = \inf_{\mathcal{D}} \sum_k |(\tau_\alpha^{\mathcal{D}})_{kk}| = \inf_{p\geq r, U\in \mathrm{U}(p)} \sum_k |(U\tau_\alpha^{\mathrm{ext}}U^T)_{kk}|$, with $\mathrm{U}(p)$ the $p \times p$ unitary group. According to Thompson's Theorem 3.3, and Lemma 2 of Ref.[65], the diagonal elements d_k $(k = 1, \ldots, p)$ of the symmetric matrix $U\tau_\alpha^{\mathrm{ext}}U^T$ verify, if sorted in decreasing order of their absolute values, $\sum_{k=1}^{i-1} |d_k| - \sum_{k=i}^{p} |d_k| \leq \sum_{k=1,k\neq i}^{p} s_k - s_i$ for $1 \leq i \leq p$, where $s_1, \ldots, s_p$ are the singular values of $\tau_\alpha^{\mathrm{ext}}$ sorted in decreasing order. For $i = 1$, this condition implies that the sum $\sum_{k=1}^{p} |d_k|$ is lower bounded by $s_1 - \sum_{k=2}^{p} s_k$. This sum is also trivially lower bounded by 0, and hence by $\max(0, s_1 - \sum_{k=2}^{p} s_k)$. This lower bound is furthermore necessarily realized. This can for example be seen by observing that Thompson's Theorem 3.3 ensures the existence of a symmetric matrix unitarily congruent to $\tau_\alpha^{\mathrm{ext}}$ and with diagonal elements satisfying $d_1 = \max(0, s_1 - \sum_{k=2}^{p} s_k)$ and $d_2 = \cdots = d_p = 0$. Since the nonzero singular values of any extension $\tau_\alpha^{\mathrm{ext}}$ of τ_α are the same as those of τ_α itself, the conclusion follows immediately.

Although it allows to compute easily the C_α concurrence of any multipartite state ρ, Theorem 3.4 cannot be used to conclude about the separability of ρ. As we show in the following section, there is one condition to add to obtain a necessary and sufficient condition of separability from the hollowisation of the preconcurrence matrices.

3.4 Separability criterion from simultaneous hollowisation

We finally address the separability question of the mixed state ρ. The separability of ρ is equivalent to the existence of a decomposition $\mathcal{D} = \{p_k, |\psi_k\rangle, k = 1, \ldots, p\}$ of ρ such that all the pure states $|\psi_k\rangle$ are separable, i.e. satisfy $C_\alpha(|\psi_k\rangle) = 0$, $\forall k$, $\forall \alpha$. This is the case if there exists a decomposition $\mathcal{D}$ of ρ such that the preconcurrence matrices $\tau_\alpha^{\mathcal{D}}$ are hollow for all α, or equivalently if there exists a $p \times p$ unitary matrix U such that the matrices $U\tau_\alpha^{\mathrm{ext}}U^T$ are hollow for all α, where $\tau_\alpha^{\mathrm{ext}}$ is the $p \times p$ extension of the preconcurrence matrix $\tau_\alpha^{\mathcal{E}}$. This shows that the separability of a state ρ is equivalent to the existence of a unitary matrix U allowing the simultaneous hollowisation by unitary congruence of all its preconcurrence matrices $\tau_\alpha^{\mathrm{ext}}$. Since it was shown in Ref. [66] that any separable state ρ admits a separable decomposition containing between $r(\rho)$ and $(r(\rho))^2$ separable states, we can conclude the following theorem:

Theorem 3.5. *A general N-partite mixed state ρ acting on the Hilbert space $\mathcal{H}$ is separable if and only if there exists a number p between $r(\rho)$ and $(r(\rho))^2$ such that, for all $\alpha = 1, \ldots, Q(\mathcal{H})$, the $p \times p$ extended preconcurrence matrices τ_α^{ext} are all* simultaneously *hollowisable by unitary congruence (i.e. all hollowisable using the same $p \times p$ unitary matrix U). In this case, a separable decomposition of ρ is given by $\rho = \sum_{k=1}^{p} |\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$, with $(|\tilde{\psi}_1\rangle, \ldots, |\tilde{\psi}_p\rangle)^T = U^*(|\tilde{v}_1\rangle, \ldots, |\tilde{v}_p\rangle)^T$, where $|\tilde{v}_k\rangle$ ($k = 1, \ldots, r(\rho)$) are the (subnormalized) eigenvectors of ρ associated to nonzero eigenvalues and $|\tilde{v}_k\rangle = 0$ for $k > r(\rho)$.*

This theorem shows that the general separability problem for mixed states is equivalent to a pure matrix analysis problem that consists in determining whether a given set of symmetric matrices is simultaneously unitarily congruent to hollow matrices. In the same way that quantum compatibility of observables is equivalent to simultaneous diagonalisability of Hermitian matrices, quantum separability is equivalent to simultaneous hollowisability of symmetric matrices.

For 2 qubits, since the system is entirely characterized by a single concurrence C_α and a single preconcurrence matrix τ_α, the simultaneous hollowisability question comes down to a single hollowisability question and this is why the inequality (3.30) fully characterizes the separability of mixed states of 2 qubits [54]. For higher dimensional systems, or systems composed of more than 2 parties, the number of generalized concurrences inevitably increases and the simultaneous hollowisability question cannot be avoided anymore. While there exist criteria to solve the related problem of simultaneous unitary congruence between pairs of matrices (see for example Refs. [67, 68]), the simultaneous hollowisability by unitary congruence of a set of symmetric matrices remains an open matrix analysis problem.

To conclude this section, we illustrate the necessary and sufficient condition of separability given in Theorem 3.5 with a nontrivial rank-5 3-qubit mixed state ρ, expressed in the computational basis $|000\rangle, |001\rangle, \ldots$ as

$$\rho = \frac{1}{20} \begin{pmatrix} 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 & 1 & -3 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 \\ 1 & -3 & 0 & 0 & 1 & 5 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3.32}$$

Since this state has positive semi-definite partial transposes with respect to all the possible bipartitions, the PPT criterion does not allow to decide about its separability. We can however prove that it is separable using Theorem 3.5. To compute the preconcurrence matrices of ρ, let us first compute the nine independent generalized spin-flip operators

characterizing 3-qubit systems. Following the method explained in Section 3.2.1 and illustrated in Section 3.2.2, we find the nine operators $S_\alpha = |000\rangle\langle 011| - |010\rangle\langle 001| + h.c.$, $|100\rangle\langle 111| - |110\rangle\langle 101| + h.c.$, $|000\rangle\langle 101| - |100\rangle\langle 001| + h.c.$, $|010\rangle\langle 111| - |110\rangle\langle 011| + h.c.$, $|000\rangle\langle 110| - |100\rangle\langle 010| + h.c.$, $|001\rangle\langle 111| - |101\rangle\langle 011| + h.c.$, $|000\rangle\langle 111| - |100\rangle\langle 011| + h.c.$, $|000\rangle\langle 111| - |010\rangle\langle 101| + h.c.$, $|000\rangle\langle 111| - |110\rangle\langle 001| + h.c.$ From the eigenvectors of ρ (multiplied by the square root of the associated eigenvalues), we then compute the nine 5×5 preconcurrence matrices τ_α. Among these, three correspond to the zero matrix. The zero matrix being hollowisable by any unitary matrix, we can ignore them. Out of the 6 remaining ones, 5 are already hollow and only one preconcurrence matrix has nonzero diagonal elements. Because of the particular structure of these matrices, we can here solve the simultaneous hollowisation problem. All the preconcurrence matrices are found to be simultaneously unitary congruent to hollow matrices using the unitary matrix

$$U = \frac{1}{\sqrt{6}} \begin{pmatrix} -\sqrt{3} & 0 & 0 & 0 & \sqrt{3} \\ \sqrt{2} & 0 & -\sqrt{2} & 0 & \sqrt{2} \\ 1 & 0 & 2 & 0 & 1 \\ 0 & -\sqrt{3} & 0 & -\sqrt{3} & 0 \\ 0 & -\sqrt{3} & 0 & \sqrt{3} & 0 \end{pmatrix}, \tag{3.33}$$

out of which Theorem 3.5 yields the separable decomposition $\rho = (1/5)\sum_{i=1}^{5} |\psi_i\rangle\langle\psi_i|$, with $|\psi_1\rangle = |-01\rangle$, $|\psi_2\rangle = |-0-\rangle$, $|\psi_3\rangle = |10+\rangle$, $|\psi_4\rangle = |-10\rangle$, $|\psi_5\rangle = |010\rangle$, where $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$.

In the next sections, we investigate the simultaneous hollowisation problem for low dimensional symmetric matrices and show that partial solutions of the problem can provide interesting results about the separability problem for certain classes of states.

3.5 Simultaneous hollowisability of 2×2 symmetric matrices

In this section, we focus on the simultaneous hollowisation problem for 2×2 symmetric matrices. In Section 3.5.1, we exploit the hollowisability condition provided by Thompson's Theorem 3.3 to find the most general form of a 2×2 hollowisable matrix. In Section 3.5.2, we use a suitable parametrization of U(2) to find the set of 2×2 unitary matrices hollowising any given 2×2 hollowisable matrix. From the intersections of the sets of unitary matrices hollowising different hollowisable matrices, we conclude in Section 3.5.3 a general simultaneous hollowisability criterion for 2×2 symmetric matrices. In Section 3.5.4, we finally use this simultaneous hollowisability criterion to prove a separability criterion for mixed states of rank 2.

3.5.1 Hollowisable 2×2 matrices

Let A be a 2×2 symmetric matrix, that we parametrize as follows:

$$A = \begin{pmatrix} c_1 & c_3 \\ c_3 & c_2 \end{pmatrix}, \text{with } c_1, c_2, c_3 \in \mathbb{C}. \tag{3.34}$$

As a consequence of Thompson's Theorem 3.3, the matrix A is hollowisable if and only if its singular values are identical. The singular values s_1 and s_2 of A are given by

$$s_{\substack{1\\2}} = \frac{1}{\sqrt{2}} \left(|c_1|^2 + |c_2|^2 + 2|c_3|^2 \pm \sqrt{z} \right)^{1/2}, \tag{3.35}$$

with

$$z = \left(|c_1|^2 - |c_2|^2 \right)^2 + 4\,|c_3|^2 \left(|c_1|^2 + |c_2|^2 \right) + 8\,\Re\left(c_3^2 \bar{c}_1 \bar{c}_2 \right), \tag{3.36}$$

where $\Re(c)$ and $\bar{c}$ denote the real part and complex conjugate of the complex number c, respectively. These singular values are thus equal if and only if $z = 0$. Using the polar decomposition $c_i = |c_i| e^{i\phi_i}$ with $\phi_i \in [0, 2\pi[$ for all $i = 1, 2, 3$, this condition is equivalent to

$$4\,|c_3|^2 \left(2\,|c_1|\,|c_2|\,\cos(2\,\phi_3 - \phi_1 - \phi_2) + |c_1|^2 + |c_2|^2 \right) = -\left(|c_1|^2 - |c_2|^2 \right)^2. \tag{3.37}$$

As the left-hand side is always positive and the right-hand side always negative, this equation only holds if both sides are equal to zero. This implies $|c_1| = |c_2|$ and either $|c_3| = 0$ or $\phi_2 = 2\,\phi_3 - \phi_1 + \pi + 2k\pi$, $k \in \mathbb{Z}$.

In any case, we can conclude the following proposition:

Proposition 3.1. *A 2×2 symmetric matrix A is hollowisable if and only if it can be written*

$$A = \begin{pmatrix} |c_1|\, e^{i\phi_1} & |c_3|\, e^{i\phi_3} \\ |c_3|\, e^{i\phi_3} & -|c_1|\, e^{i(2\,\phi_3 - \phi_1)} \end{pmatrix}, \text{ with } |c_1|, |c_3| \in \mathbb{R}^+ \text{ and } \phi_1, \phi_3 \in [0, 2\pi[. \tag{3.38}$$

3.5.2 Unitary matrices hollowising a 2×2 hollowisable matrix

In order to find a simultaneous hollowisability criterion for 2×2 matrices, we now search for the set of 2×2 unitary matrices hollowising the hollowisable matrix A from Proposition 3.1. Let us first note that a unitary U hollowises A if and only if it also hollowises the matrix cA, for any complex number c. As a consequence, the set of unitary matrices hollowising A can equivalently be found when considering any multiple of A. If all the elements of A are equal to zero, A is already hollow and hollowisable by any

unitary matrix. When it is not the case, we choose to work with the multiple γA, with

$$\gamma = \frac{e^{-i\phi_3}}{\sqrt{|c_1|^2 + |c_3|^2}}, \tag{3.39}$$

as it admits the simpler 2-angle parametrization

$$\gamma A = \begin{pmatrix} \cos\theta\, e^{i\phi} & \sin\theta \\ \sin\theta & -\cos\theta\, e^{-i\phi} \end{pmatrix} \text{ with } \theta \in [0, \pi/2] \text{ and } \phi \in [0, 2\pi[. \tag{3.40}$$

This rescaled hollowisable matrix γA turns out to be a symmetric unitary matrix. Transforming this matrix by unitary congruence preserves both its unitarity and its symmetry. As a consequence, the hollowisation of this matrix necessarily yields the σ_1 Pauli matrix, multiplied by some phase.

Using a similar argument, we can also extract two phases from any hollowising unitary. Indeed, any 2×2 unitary matrix U' can be decomposed into a product of the form [69]

$$U' = \underbrace{\begin{pmatrix} e^{i\delta_1} & 0 \\ 0 & e^{i\delta_2} \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} \cos\psi & -\sin\psi\, e^{-i\sigma} \\ \sin\psi\, e^{i\sigma} & \cos\psi \end{pmatrix}}_{U} \tag{3.41}$$

for some angles $\delta_2, \psi \in [-\pi, \pi[$ and $\delta_1, \sigma \in [-\pi/2, \pi/2]$. For convenience, we work here with the modified space of parameters $\delta_1, \delta_2, \sigma \in [0, 2\pi[$ and $\psi \in [0, \pi/2]$. As the unitary matrix U' hollowises γA if and only if U hollowises γA, we can first look for the unitary U hollowising γA and add the diagonal matrix of phases D afterward.

The matrix $U\,\gamma A\,U^T$ is hollow if its two diagonal elements vanish, i.e. if

$$\begin{cases} e^{-i\phi}\left(e^{2i\phi}\cos^2\psi\cos\theta - e^{-2i\sigma}\cos\theta\sin^2\psi - e^{i(\phi-\sigma)}\sin(2\psi)\sin\theta\right) = 0 \\ e^{-i\phi}\left(-\cos^2\psi\cos\theta + e^{2i(\phi+\sigma)}\cos\theta\sin^2\psi + e^{i(\phi+\sigma)}\sin(2\psi)\sin\theta\right) = 0 \end{cases}. \tag{3.42}$$

These two equations are in fact equivalent. We can eliminate one angle by posing $\delta = \phi + \sigma$, so that the only independent equation to solve reads:

$$e^{i\delta}\cos^2\psi\cos\theta - e^{-i\delta}\cos\theta\sin^2\psi - \sin(2\psi)\sin\theta = 0. \tag{3.43}$$

The cancellation of the imaginary part of this equation yields merely $\sin\delta\cos\theta = 0$, which implies either $\sin\delta = 0$ or $\cos\theta = 0$. When $\cos\theta = 0$, the matrix γA is already hollow. The hollowising unitary U must then either have $\psi = 0$ or $\psi = \pi/2$. Up to the phases of U, which can in this case be absorbed into the diagonal matrix D, these solutions are compatible with the solution $\sin\delta = 0$, that we consider now. As $\delta \in [0, 4\pi[$, the solution $\sin\delta = 0$ implies $\delta = k\pi$, $k \in \{0, 1, 2, 3\}$. These values of δ give two different equations for the vanishing of the real part of Eq. (3.43). We have to consider separately (i) $\delta = k\pi$ with $k \in \{0, 2\}$ and (ii) $\delta = k\pi$ with $k \in \{1, 3\}$.

In case (i), we have $\sigma = k\pi - \phi$ for some $k \in \{0, 2\}$ such that $\sigma \in [0, 2\pi[$ and the vanishing of the real part of Eq. (3.43) is equivalent to

$$\cos\theta\cos(2\psi) - \sin(2\psi)\sin\theta = 0. \tag{3.44}$$

This equation admits the unique solution

$$\psi = \frac{\pi/2 - \theta}{2}. \tag{3.45}$$

In case (ii), we have $\sigma = k\pi - \phi$ for some $k \in \{1, 3\}$ such that $\sigma \in [0, 2\pi[$ and the vanishing of the real part of Eq. (3.43) is equivalent to

$$-\cos\theta\cos(2\psi) - \sin(2\psi)\sin\theta = 0. \tag{3.46}$$

This equation admits the unique solution

$$\psi = \frac{\pi/2 + \theta}{2}. \tag{3.47}$$

The solutions for cases (i) and (ii) transform the matrix γA into the same hollow matrix, up to a global minus sign. Adding the diagonal matrix of phases D to these solutions, we find the general form of the unitary matrices hollowising γA. This is summarized in the following proposition.

Proposition 3.2. *Given a 2×2 hollowisable symmetric matrix A, there exists a complex number c such that the matrix cA can be written*

$$cA = \begin{pmatrix} \cos\theta\, e^{i\phi} & \sin\theta \\ \sin\theta & -\cos\theta\, e^{-i\phi} \end{pmatrix} \text{ for some } \theta \in [0, \pi/2] \text{ and } \phi \in [0, 2\pi[. \tag{3.48}$$

A unitary matrix U hollowises the matrix A if and only if it can either be written

$$U = \begin{pmatrix} \cos\left(\frac{\pi/2-\theta}{2}\right) e^{i\delta_1} & -\sin\left(\frac{\pi/2-\theta}{2}\right) e^{i(\delta_1+\phi)} \\ \sin\left(\frac{\pi/2-\theta}{2}\right) e^{i(\delta_2-\phi)} & \cos\left(\frac{\pi/2-\theta}{2}\right) e^{i\delta_2} \end{pmatrix} \tag{3.49}$$

or

$$U = \begin{pmatrix} \cos\left(\frac{\pi/2+\theta}{2}\right) e^{i\delta_1} & \sin\left(\frac{\pi/2+\theta}{2}\right) e^{i(\delta_1+\phi)} \\ -\sin\left(\frac{\pi/2+\theta}{2}\right) e^{i(\delta_2-\phi)} & \cos\left(\frac{\pi/2+\theta}{2}\right) e^{i\delta_2} \end{pmatrix}, \tag{3.50}$$

for some $\delta_1, \delta_2 \in [0, 2\pi[$.

3.5.3 Simultaneous hollowisability criterion for 2×2 symmetric matrices

Two hollowisable matrices are simultaneously hollowisable only if their sets of hollowising unitaries have a nonempty intersection. As we show in the following theorem, the sets of unitary matrices hollowising 2×2 symmetric matrices have a nonempty intersection only if the symmetric matrices are proportional to each other, yielding a very strict simultaneous hollowisability criterion for 2×2 symmetric matrices.

Theorem 3.6. *A set of 2×2 symmetric matrices is simultaneously hollowisable if and only if all the matrices of the set are individually hollowisable and proportional to each other.*

Proof. The sufficient condition is trivial: a set of hollowisable matrices (of arbitrary dimension) that are all proportional to each other is always simultaneously hollowisable. In the necessary condition, the individual hollowisability condition is also trivial, so there only remains to be proved that simultaneously hollowisable matrices are necessarily proportional to each other.

As a consequence of Proposition 3.2, two hollowisable symmetric matrices with a rescaled form (3.48) corresponding to two different values of θ have disjoint sets of hollowising unitaries and cannot be simultaneously hollowisable. Similarly, two hollowisable matrices with a rescaled form (3.48) corresponding to the same value of θ but to two different values ϕ_1 and ϕ_2 ($\phi_1 \neq \phi_2$) of ϕ have disjoint sets of hollowising unitaries and cannot be simultaneously hollowisable, unless $\theta = 0$ and $\phi_2 = \phi_1 + \pi$. In this case, the two rescaled hollowisable matrices are however equal up to a global minus sign. We can therefore conclude that hollowisable matrices are simultaneously hollowisable only if their rescaled forms are proportional to each other, in which case the hollowisable matrices are themselves proportional to each other. □

Even though this theorem presents a mathematical interest by itself, our objective is of course to combine it with Theorem 3.5, in order to obtain a separability criterion. As the dimension of the preconcurrence matrices τ_α of a mixed state ρ corresponds to the rank of ρ, we can use Theorem 3.6 to study the separability of multipartite states of rank 2, i.e. multipartite states corresponding to the mixture of two independent states.

3.5.4 Separability criterion for multipartite states of rank 2

Using Theorem 3.6, we can check whether the 2×2 preconcurrence matrices τ_α of a rank-2 multipartite state ρ are simultaneously hollowisable or not. To conclude about the separability of ρ using Theorem 3.5, we must however not neglect the possibility of extending the preconcurrence matrices τ_α by addition of up to two extra rows and columns of zeroes to reach simultaneous hollowisability. We first show that such an extension of 2×2 symmetric matrices to 3×3 or 4×4 matrices does not change their simultaneous hollowisability.

Lemma 3.1. *Let $A_1, \ldots, A_n$ be n 2×2 symmetric hollowisable matrices. The 3×3 or 4×4 matrices $A_1^{\text{ext}}, \ldots, A_n^{\text{ext}}$ obtained by extending the matrices $A_1, \ldots, A_n$ with 1 or 2 extra row(s) and column(s) of zeroes are simultaneously hollowisable if and only if the matrices $A_1, \ldots, A_n$ are proportional to each other.*

Proof. The sufficient condition is trivial. To prove the necessary condition we can restrict ourselves to the case in which there are only two hollowisable matrices: A_1 and A_2. We begin with the 3×3 extensions. Rather than working with two general hollowisable matrices A_1^{ext} and A_2^{ext}, we can transform them by unitary congruence (using the same unitary). The resulting matrices are indeed simultaneously hollowisable if and only if A_1^{ext} and A_2^{ext} are also simultaneously hollowisable. For the same reason, we can also multiply each one by an arbitrary complex number. As a symmetric matrix can always be transformed by unitary congruence into a diagonal matrix in which the diagonal elements are the singular values of the matrix with arbitrary phases [48], we can, without loss of generality, work with the matrices

$$A_1^{\text{ext}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2^{\text{ext}} = \begin{pmatrix} \cos\theta\, e^{i\phi} & \sin\theta & 0 \\ \sin\theta & -\cos\theta\, e^{-i\phi} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{3.51}$$

for some $\theta \in [0, \pi/2]$ and $\phi \in [0, 2\pi[$. The 3×3 unitary matrix

$$U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} \tag{3.52}$$

hollowises the matrix A_1^{ext} if and only if

$$\begin{cases} u_{11}^2 - u_{12}^2 = 0 \\ u_{21}^2 - u_{22}^2 = 0 \\ u_{31}^2 - u_{32}^2 = 0 \end{cases}. \tag{3.53}$$

The solutions of this system are $u_{j2} = \pm u_{j1}$ for $j = 1, 2, 3$ (the third column of U does not play any role in the unitary congruence of the extended matrices). The signs cannot be identical for the three values of j as the columns of U must be orthonormal. There are therefore only two possibilities: (*i*) u_{j1} and u_{j2} are identical for 2 values of j or (*ii*) u_{j1} and u_{j2} are opposite for 2 values of j. The ones that are identical or opposite has no importance as the different possibilities correspond to permutations of the rows of U. We consider thus, without loss of generality, that the values of j for which u_{j1} and u_{j2} are identical are always the smallest. We can easily check in both cases if such a unitary U also hollowises A_2^{ext}:

In case (i), we have

$$U = \begin{pmatrix} u_{11} & u_{11} & u_{13} \\ u_{21} & u_{21} & u_{23} \\ u_{31} & -u_{31} & u_{33} \end{pmatrix} \text{ hollowises } A_2^{\text{ext}} \Leftrightarrow \begin{cases} u_{11}^2\Big(i\sin\phi\cos\theta + \sin\theta\Big) = 0 \\ u_{21}^2\Big(i\sin\phi\cos\theta + \sin\theta\Big) = 0 \\ u_{31}^2\Big(i\sin\phi\cos\theta - \sin\theta\Big) = 0 \end{cases} . \tag{3.54}$$

The orthonormality of the columns of U imposes $u_{31} \neq 0$. As a consequence, $\theta = 0$ and $\phi = 0$ or π are the only solutions of the system. In case (ii), we have almost the same system to solve:

$$U = \begin{pmatrix} u_{11} & u_{11} & u_{13} \\ u_{21} & -u_{21} & u_{23} \\ u_{31} & -u_{31} & u_{33} \end{pmatrix} \text{ hollowises } A_2^{\text{ext}} \Leftrightarrow \begin{cases} u_{11}^2\Big(i\sin\phi\cos\theta + \sin\theta\Big) = 0 \\ u_{21}^2\Big(i\sin\phi\cos\theta - \sin\theta\Big) = 0 \\ u_{31}^2\Big(i\sin\phi\cos\theta - \sin\theta\Big) = 0 \end{cases} . \tag{3.55}$$

The orthonormality of the columns of U implies $u_{11} = 0$, so that the only solutions of the system are again $\theta = 0$ and $\phi = 0$ or π. This implies that A_1^{ext} and A_2^{ext} are simultaneously hollowisable only if they are proportional to each other (which implies that A_1 and A_2 are also proportional to each other).

The proof for the case of the 4×4 extensions is rigorously the same (we just have an extra equation in the systems, but the same solution). □

We have now all the ingredients to prove that the condition given in Theorem 3.6 for the simultaneous hollowisability of 2×2 symmetric matrices actually provides a necessary and sufficient condition for the separability of multipartite states of rank 2. In the following theorem, we prove in addition that the 2×2 unitary matrices realizing the simultaneous hollowisation of the preconcurrence matrices lead to a unique separable decomposition over 2 separable states.

Theorem 3.7. *A rank-2 mixed state ρ defined in a general multipartite Hilbert space $\mathcal{H}$ is separable if and only if, for all $\alpha = 1, \ldots, Q(\mathcal{H})$, its preconcurrence matrices τ_α are all individually hollowisable and proportional to each other. When it is the case, the separable rank-2 state ρ admits a unique separable decomposition over 2 separable states.*

Proof. The sufficient condition follows simply from Theorem 3.5: if the preconcurrence matrices τ_α are all individually hollowisable and proportional to each other, then they are all simultaneously hollowisable, and Theorem 3.5 allows us to conclude that ρ is separable.

We now prove the necessary condition. If the rank-2 state ρ is separable, then Theorem 3.5 implies that there exists a number p between 2 and 4 such that the $p \times p$ extended preconcurrence matrices τ_α^{ext} are all simultaneously hollowisable. If $p = 2$, then Theorem 3.6 shows that all the preconcurrence matrices τ_α must be individually hollowisable and proportional to each other. We reach the same conclusion if $p = 3$ or $p = 4$

by using Lemma 3.1. This concludes the proof of the first part of the theorem. We now focus on the statement about the separable decompositions of ρ.

As the extended preconcurrence matrices are simultaneously hollowisable if and only if the 2×2 preconcurrence matrices are themselves simultaneously hollowisable (because of Lemma 3.1), Theorem 3.5 allows us to conclude that a rank-2 separable state always admits a separable decomposition containing only 2 separable states. There only remains to be proved that this decomposition is unique. Let ρ be a rank-2 separable state and τ_1' a rescaled version of the preconcurrence matrix τ_1 of ρ reading

$$\tau_1' = \begin{pmatrix} \cos\theta\, e^{i\phi} & \sin\theta \\ \sin\theta & -\cos\theta\, e^{-i\phi} \end{pmatrix} \text{ for some } \theta \in [0, \pi/2] \text{ and } \phi \in [0, 2\pi[. \tag{3.56}$$

According to Proposition 3.2, such a rescaled form always exists and the unitaries hollowising τ_1' (and thus τ_1 and all the other preconcurrence matrices) are either of the form

$$U = \begin{pmatrix} \cos\left(\frac{\pi/2-\theta}{2}\right) e^{i\delta_1} & -\sin\left(\frac{\pi/2-\theta}{2}\right) e^{i(\delta_1+\phi)} \\ \sin\left(\frac{\pi/2-\theta}{2}\right) e^{i(\delta_2-\phi)} & \cos\left(\frac{\pi/2-\theta}{2}\right) e^{i\delta_2} \end{pmatrix} \tag{3.57}$$

or

$$U' = \begin{pmatrix} \cos\left(\frac{\pi/2+\theta}{2}\right) e^{i\delta_1} & \sin\left(\frac{\pi/2+\theta}{2}\right) e^{i(\delta_1+\phi)} \\ -\sin\left(\frac{\pi/2+\theta}{2}\right) e^{i(\delta_2-\phi)} & \cos\left(\frac{\pi/2+\theta}{2}\right) e^{i\delta_2} \end{pmatrix}, \tag{3.58}$$

with $\delta_1, \delta_2 \in [0, 2\pi[$.

The unitary U' appears to be related to U through the product

$$U' = \begin{pmatrix} e^{i\delta_1} & 0 \\ 0 & e^{i\delta_2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -e^{-i(\phi+\delta_1)} & 0 \\ 0 & e^{i(\phi-\delta_2)} \end{pmatrix} U. \tag{3.59}$$

This implies that when using U' instead of U to compute the separable decomposition of ρ from its eigendecomposition as explained in Theorem 3.5, the two states of the decomposition are simply swapped and have each an extra global phase. As a consequence, U' and U lead to the same decomposition. Similarly, when using two matrices having the form of U, but with different angles δ_1 and δ_2, the difference between the resulting separable decompositions consists only in different global phases of the separable states. This shows that the 2×2 unitary matrices realizing the simultaneous hollowisation of the preconcurrence matrices of ρ lead all to the same, unique, separable decomposition of ρ over 2 product states. □

The separability problem for mixed states of rank 2 had previously been solved in Ref. [70], using a different method based on the PPT criterion. This method also allowed to show that separable states of rank 2 always admit a separable decomposition containing only 2 product states. The advantage of Theorem 3.7 is that it provides a simple and direct way to compute such a separable decomposition over 2 product states, and further proves that this decomposition is unique.

Throughout this section, we solved the simultaneous hollowisation problem for 2×2 matrices and showed how to exploit the solution to prove a separability criterion for mixed states of rank 2. With the goal of finding a separability criterion for multipartite mixed states of rank 3, we study the simultaneous hollowisation problem for 3×3 matrices in the next section.

3.6 Simultaneous hollowisation of 3×3 symmetric matrices

For 3×3 symmetric matrices, the hollowisation condition given by Thompson's Theorem 3.3 is still an equality but less restrictive than for 2×2 matrices. Given a 3×3 hollowisable matrix A, we first characterize all the hollow matrices A can be transformed into by unitary congruence. We then search, in a special basis, the form of hollowising unitaries and finally address the simultaneous hollowisation problem.

3.6.1 Hollow forms of 3×3 hollowisable matrices

According to Thompson's Theorem 3.3, a (symmetric) 3×3 matrix A is hollowisable if and only if its singular values $s_1 \geq s_2 \geq s_3$ satisfy $s_1 - s_2 - s_3 = 0$. When it is the case, the matrix A can be transformed by unitary congruence into at least one hollow matrix H of the form

$$H = \begin{pmatrix} 0 & h_1 & h_2 \\ h_1 & 0 & h_3 \\ h_2 & h_3 & 0 \end{pmatrix}, \text{ with } h_1, h_2, h_3 \in \mathbb{C}. \tag{3.60}$$

As a consequence of the Lemma 2 of Ref. [65], the singular values of H must be the same as the singular values of A. The singular values of the hollow matrix H are given by the square roots of the roots of the polynomial

$$P(z) = z^3 - 2ax^2 + a^2x - 4b\,, \tag{3.61}$$

with

$$\begin{cases} a &= |h_1|^2 + |h_2|^2 + |h_3|^2 \\ b &= |h_1|^2\,|h_2|^2\,|h_3|^2 \end{cases}. \tag{3.62}$$

Since the polynomial P has a fixed coefficient (the one of the highest degree term), there is a one-to-one correspondence between its roots and its coefficients. This implies a one-to-one correspondence between the singular values of H (or A) and the values of a and b. The matrix A can therefore be transformed into all hollow matrices H having a and b corresponding to its singular values. We now compute explicitly the set of hollow matrices A can be transformed into.

As a and b depend only on the norms of the elements of H, the phases of the elements of H have no influence on the possibility of transforming A into H by unitary congruence.

To suppress these trivial degrees of freedom, it is therefore interesting to factor all phases out of H and look at real (positive) hollow matrices. This can be done using a diagonal (unitary) matrices of phases, as there exist angles $\phi_1, \phi_2, \phi_3 \in [0, 2\pi[$ such that

$$H = \begin{pmatrix} 0 & |h_1|\, e^{i\,\phi_1} & |h_2|\, e^{i\,\phi_2} \\ |h_1|\, e^{i\,\phi_1} & 0 & |h_3|\, e^{i\,\phi_3} \\ |h_2|\, e^{i\,\phi_2} & |h_3|\, e^{i\,\phi_3} & 0 \end{pmatrix} = D_\phi(\phi_1, \phi_2, \phi_3)\, H' \left(D_\phi(\phi_1, \phi_2, \phi_3)\right)^T, \quad (3.63)$$

with

$$D_\phi(\phi_1, \phi_2, \phi_3) = \begin{pmatrix} e^{i\,\frac{\phi_1+\phi_2-\phi_3}{2}} & 0 & 0 \\ 0 & e^{i\,\frac{\phi_1+\phi_3-\phi_2}{2}} & 0 \\ 0 & 0 & e^{i\,\frac{\phi_2+\phi_3-\phi_1}{2}} \end{pmatrix} \quad (3.64)$$

and

$$H' = \begin{pmatrix} 0 & |h_1| & |h_2| \\ |h_1| & 0 & |h_3| \\ |h_2| & |h_3| & 0 \end{pmatrix}. \quad (3.65)$$

Such a phase factorization is only possible because the hollow matrix H is a 3×3 matrix with 3 distinct complex elements. A 3×3 diagonal matrix of phases has therefore enough degrees of freedom to absorb all the phases. Even though this was also possible in the case of 2×2 hollow matrices, for which there was only one phase to absorb (see Section 3.5.2), we would not be able to do it for 4×4 hollow matrices. These matrices have indeed 6 distinct complex elements, so that a diagonal matrix of 4 phases could not allow such a factorization.

To find the set containing all the hollow matrices of the form H' corresponding to given singular values $s_1 \geq s_2 \geq s_3$, we must first express a and b as a function of these singular values. This can be done by expressing the coefficients of the polynomial P defined in Eq. (3.61) in terms of its roots (which are the squares of the singular values of H'). We get the following relations:

$$\begin{cases} a &= \left(s_1^2 + s_2^2 + s_3^2\right)/2 = s_1^2 - s_2 s_3 \\ b &= \left(s_1^2\, s_2^2\, s_3^2\right)/4 \end{cases}. \quad (3.66)$$

The relationship between the nonzero elements of H' and its singular values is then obtained by solving System (3.62). This yields the following set of triplets:

$$\begin{aligned} (|h_1|, |h_2|, |h_3|) \in &\left\{ \left(\lambda, \frac{1}{\sqrt{2}} \sqrt{s_1^2 - s_2 s_3 - \lambda^2 - \gamma}, \frac{1}{\sqrt{2}} \sqrt{s_1^2 - s_2 s_3 - \lambda^2 + \gamma} \right) \;\middle|\; \lambda \in [s_3, s_2] \right\} \\ &\bigcup \left\{ \left(\lambda, \frac{1}{\sqrt{2}} \sqrt{s_1^2 - s_2 s_3 - \lambda^2 + \gamma}, \frac{1}{\sqrt{2}} \sqrt{s_1^2 - s_2 s_3 - \lambda^2 - \gamma} \right) \;\middle|\; \lambda \in [s_3, s_2] \right\} \end{aligned} \quad (3.67)$$

with

$$\gamma = \sqrt{\frac{(\lambda^2 - s_1^2)(\lambda^2 - s_2^2)(\lambda^2 - s_3^2)}{\lambda^2}}. \tag{3.68}$$

As a conclusion, given an hollowisable 3×3 matrix A with singular values $s_1 \geq s_2 \geq s_3$, the hollow matrices A can be transformed into (by unitary congruence) have non diagonal elements whose norms correspond to one of the triplets of Eq. (3.67) and have arbitrary phases.

3.6.2 Hollowising 3×3 unitary matrices

We now search the form of the unitaries transforming A into one of the accessible hollow matrices. As in the 2×2 case, a diagonal matrix of phases can be factored out of any 3×3 unitary matrix. To that purpose, let us define, as in Ref. [69], the n-dimensional unimodular matrix $U_{pq}(\phi, \sigma)$ with $1 \leq p < q \leq n$ and $\phi \in]-\pi, \pi]$, $\sigma \in [-\pi/2, \pi/2]$, as the unitary matrix differing from $n \times n$ identity matrix only through the 4 elements

$$\begin{cases} (U_{pq}(\phi,\sigma))_{pp} = (U_{pq}(\phi,\sigma))_{qq} = \cos\phi \\ (U_{pq}(\phi,\sigma))_{pq} = -\sin\phi\, e^{-i\sigma} \\ (U_{pq}(\phi,\sigma))_{qp} = \sin\phi\, e^{i\sigma} \end{cases}. \tag{3.69}$$

Using 3-dimensional unimodular matrices $U_{pq}(\phi, \sigma)$ and a 3×3 diagonal matrix of phases, a 3×3 unitary matrix U can always be written as the product [69]

$$U = diag(e^{i\delta_1}, e^{i\delta_2}, e^{i\phi_3})\ \underbrace{U_{23}(\phi_2, \sigma_3)\, U_{12}(\theta, \sigma_2)\, U_{13}(\phi_1, \sigma_1)}_{U'}, \tag{3.70}$$

where all angles range from $-\pi/2$ to $\pi/2$ except for the angles ϕ_i $(i = 1, 2, 3)$, which range from $-\pi$ to π. Since U hollowises a matrix A if and only if U' hollowises A, we may omit the diagonal matrix of phases in the following developments.

Searching the unitaries hollowising a symmetric matrix A is not an easy task. This task can however be made easier when working in a well chosen basis. As every symmetric matrix A is diagonalizable by unitary congruence [48], working in a basis in which A is diagonal is always possible. After diagonalization, the elements on the diagonal are the singular values of A, in any desired order and with arbitrary phases [48]. As we show in the following proposition, working with a traceless diagonal matrix simplifies the search for hollowising unitaries.

Proposition 3.3. *If a unitary matrix U hollowises the matrix*

$$D = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & -s_2 & 0 \\ 0 & 0 & -s_3 \end{pmatrix}, \ \textit{with } s_1 - s_2 - s_3 = 0 \tag{3.71}$$

then there exists a diagonal matrix of phases V and a real orthogonal matrix O such that $U = VO$.

Proof. Given the hypotheses, the matrix $H = U D U^T$ is hollow. As shown in Eq. (3.63), there exist angles $\phi_1, \phi_2, \phi_3 \in [0, 2\pi[$ such that $H = D_\phi(\phi_1, \phi_2, \phi_3)\, H'\, D_\phi(\phi_1, \phi_2, \phi_3)^T$, with H' a symmetric, hollow and positive matrix and D_ϕ a diagonal matrix of phases. The matrix H' being real and symmetric, there exists a real orthogonal matrix O such that the matrix $\Sigma = O^T H' O$ is diagonal [48]. The diagonal elements of Σ are the eigenvalues of H' (in any desired order), i.e. the singular values of H' up to a possible minus sign. As H' is unitarily congruent to H, which is itself unitarily congruent to D, H' and D have the same singular values, namely s_1, s_2 and s_3. In addition, H' having a zero trace and a positive determinant (this can be checked explicitly), its eigenvalues sum up to zero and have a positive product. We can therefore conclude that the eigenvalues of H' are $s_1, -s_2$ and $-s_3$. It is then always possible to choose O so that $O^T H' O = D$.

From the two expressions of H we computed, we have

$$D_\phi(\phi_1, \phi_2, \phi_3)\, O\, D\, O^T\, D_\phi(\phi_1, \phi_2, \phi_3)^T = U\, D\, U^T, \tag{3.72}$$

which is equivalent to

$$\left(U^\dagger\, D_\phi(\phi_1, \phi_2, \phi_3)\, O\right)\, D = D\left(U^\dagger\, D_\phi(\phi_1, \phi_2, \phi_3)\, O\right)^*, \tag{3.73}$$

where X^* and $X^\dagger$ are used to denote the complex and Hermitian conjugates of the matrix X, respectively. Since D is a real diagonal matrix that cannot be multiple of the identity matrix, the previous equality only holds if $U^\dagger\, D_\phi(\phi_1, \phi_2, \phi_3)\, O$ is a real diagonal matrix too. This implies that $U^\dagger\, D_\phi$ is a real unitary matrix, i.e. an orthogonal matrix, that must be equal to O^T up to a possible change of sign of each column. Including this possible change of sign into the matrix $D_\phi(\phi_1, \phi_2, \phi_3)$, which becomes $D_\phi(\phi_1', \phi_2', \phi_3')$, we recover the statement of the proposition as $U = D_\phi(\phi_1', \phi_2', \phi_3')O$. □

As a consequence of the previous proposition, determining all the unitary matrices U hollowising D is equivalent, up to diagonal matrices of phases, to finding all the real orthogonal matrices O hollowising D. This constitutes a dramatic simplification of the problem, as orthogonal matrices have a parameter space of only 3 angles, compared to the 9 angles of general unitary matrices. In this particular basis, we can actually find the analytical form of all the hollowising unitaries.

Using similar matrices as in Eq. (3.70), a general real orthogonal matrix O can be written

$$O = diag(1, 1, \pm 1)\, U_{23}(\phi_2, 0)\, U_{12}(\theta, 0)\, U_{13}(\phi_1, 0). \tag{3.74}$$

The diagonal matrix in this parametrization is there to guarantee that, for each orthogonal matrix with determinant 1 (i.e. from $SO(3)$), we have the equivalent matrix with determinant -1 (i.e. from $O(3) \setminus SO(3)$). As this matrix is nothing but a diagonal matrix

of phases, it has no impact on the fact that O hollowises D or not, and we can thus deal with orthogonal matrices from $SO(3)$ only.

With this parametrization, the orthogonal matrix O hollowises D if and only if the equations

$$\begin{cases} \frac{1}{2}\cos^2(\theta)\left(s_2+(s_2+2s_3)\cos(2\phi_1)\right)-s_2\sin^2(\theta)=0 \\ s_2-3s_2\cos(2\theta)-2(s_2+2s_3)\cos^2(\theta)\cos(2\phi_1)=0 \\ -6s_2\cos^2(\theta)\cos(2\phi_2)-(s_2+2s_3)\Big(\cos(2\phi_1)\cos(2\phi_2)(-3+\cos(2\theta))+4\sin(\theta)\sin(2\phi_1)\sin(2\phi_2)\Big)=0 \end{cases} \tag{3.75}$$

are all satisfied. Since the first two equations of this system are equivalent, we have two independent equations for three unknowns and we expect a continuous set of solutions. These solutions can be parametrized as follows:

$$-\arctan\left(\sqrt{\frac{s_1}{s_2}}\right)\leq\theta\leq\arctan\left(\sqrt{\frac{s_1}{s_2}}\right), \tag{3.76}$$

$$\phi_1=\pm\frac{1}{2}\arccos\left(\frac{s_2(2\tan^2(\theta)-1)}{s_1+s_3}\right)+k\pi \quad \text{with } k\in\mathbb{Z}\ s.t.\ -\pi<\phi_1\leq\pi \tag{3.77}$$

and

$$\phi_2=\begin{cases} \frac{\pi}{4}+k\,\frac{\pi}{2} \text{ with } k\in\mathbb{Z}\ s.t.\ -\pi<\phi_2\leq\pi \text{ , if } \theta=0 \text{ or } \sin(2\phi_1)=0, \\ \frac{1}{2}\arctan\left(\frac{2s_2(\tan^2(\theta)-1)}{(s_1+s_3)\sin(\theta)\sin(2\phi_1)}\right)+k\,\frac{\pi}{2} \quad \text{with } k\in\mathbb{Z}\ s.t.\ -\pi<\phi_2\leq\pi \text{ , otherwise,} \end{cases} \tag{3.78}$$

unless $s_3=0$ and $\theta=\pi/4$, in which case there is no condition on ϕ_2 ($\phi_2\in]-\pi,\pi]$).

The orthogonal matrices satisfying these conditions for given values of $s_1\geq s_2\geq s_3$, transform the diagonal matrix D into all the positive hollow matrices H' having elements belonging to the sets (3.67), but also into real hollow matrices with some negative elements. Due to the symmetries of the matrix D, it can happen that orthogonal matrices with different angles θ,ϕ_1 and ϕ_2 transform D into the same hollow matrix up to the signs of its elements (which could be absorbed into a diagonal matrix of phases). The range of the angle θ, as well as the different solutions for ϕ_1 and ϕ_2, for a given value of θ, explain some of these redundancies. Considering an orthogonal matrix with angles $\{\theta,\phi_1,\phi_2\}$ satisfying Eqs. (3.76) to (3.78) that transforms D into the hollow matrix

$$H=\begin{pmatrix} 0 & h_1 & h_2 \\ h_1 & 0 & h_3 \\ h_2 & h_3 & 0 \end{pmatrix}, \tag{3.79}$$

some elementary transformations on the angles θ, ϕ_1 and ϕ_2 inducing redundant hollow matrices are listed in Table 3.1.

By combining some of the transformations listed in Table 3.1, one can for example show that orthogonal matrices O_1, O_2 that both hollowise D and are characterized by the angles $\{\theta,\phi_1,\phi_2\}$ and $\{-\theta,-\phi_1,\phi_2+\pi\}$, respectively, transform the matrix D into the

Angle transformation	Corresponding hollow elements
$\theta \to -\theta$	$\{-h_1, h_2, -h_3\}$
$\phi_1 \to -\phi_1$	$\{h_1, -h_2, -h_3\}$
$\phi_1 \to \phi_1 + \pi$	$\{h_1, h_2, h_3\}$
$\phi_2 \to \phi_2 + \pi/2$	$\{h_2, -h_1, -h_3\}$

Table 3.1: Effect of certain transformations on the angles θ, ϕ_1 and ϕ_2 characterizing an orthogonal matrix transforming the diagonal matrix D into the hollow matrix H of Eq. (3.79) on the non diagonal elements of the resulting hollow matrix.

same hollow matrix. Other symmetries, such as permutation symmetries, are naturally present in this solution, but are more difficult to identify. A permutation in the triplet (h_1, h_2, h_3) can for example be obtained by applying the inverse permutation on the rows of the orthogonal matrix used in the unitary congruence, which cannot always be expressed easily as an angle transformation.

A deeper analysis of these symmetries allows to conclude that a minimal set of hollowising orthogonal matrices, i.e. a set of orthogonal matrices transforming D into hollow matrices that are not equivalent through unitary congruence with a diagonal matrix of phases or rows and columns permutations, can be obtain through the set of angles

$$\begin{cases} 0 \leq \theta \leq \arctan\left(\sqrt{\frac{s_2}{2s_1+s_2}}\right) \\ \phi_1 = \frac{1}{2}\arccos\left(\frac{s_2(2\tan^2(\theta)-1)}{s_1+s_3}\right) \\ \phi_2 = \begin{cases} \pi/4, \text{ if } \theta = 0 \\ \frac{1}{2}\arctan\left(\frac{2s_2(\tan^2(\theta)-1)}{(s_1+s_3)\sin(\theta)\sin(2\phi_1)}\right), \text{ otherwise} \end{cases} \end{cases} . \tag{3.80}$$

3.6.3 Simultaneous hollowisation of 3×3 matrices

Symmetric hollowisable matrices are in general not simultaneously diagonalizable. As a consequence, the hollowising orthogonal matrices found in the previous section cannot be directly used to study the conditions guaranteeing simultaneous hollowisability of symmetric 3×3 matrices. These orthogonal matrices can however be exploited in a numerical algorithm (Algorithm 3.1 hereafter), allowing to check efficiently whether n symmetric 3×3 matrices $S_1, \ldots, S_n$ are simultaneously hollowisable or not.

Algorithm 3.1 (Simultaneous hollowisability check for symmetric 3×3 matrices). *Given a set of n symmetric 3×3 matrices $S_1, \ldots, S_n$, we first check that each matrix is individually hollowisable. This is the case if and only if each matrix S_i $(i = 1, \ldots, n)$ has singular values $s_1^i \geq s_2^i \geq s_3^i$ satisfying $s_1^i - s_2^i - s_3^i = 0$.*

If these conditions are satisfied, we then search a unitary matrix U that transforms the matrix S_1 by unitary congruence into a diagonal matrix of the form

$$D_1 = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & -s_2 & 0 \\ 0 & 0 & -s_3 \end{pmatrix}, \tag{3.81}$$

where $s_i = s_i^1$ for $i = 1, 2, 3$ (we drop the superscripts of the singular values of S_1 for simplicity). Such a unitary matrix can, for example, be found by adjusting the phases of any unitary matrix diagonalizing the Hermitian matrix $S_1 S_1^*$ [48]. Rather than considering the problem of simultaneous hollowisability of $S_1, \ldots, S_n$, we consider now the equivalent problem of simultaneous hollowisability of $D_1, S_2', \ldots, S_n'$, with $S_i' = U S_i U^T$ for all $i = 2, \ldots, n$.

The last step of the algorithm consists in checking numerically if there exists an orthogonal matrix O of the form

$$O = U_{23}(\phi_2, 0)\, U_{12}(\theta, 0)\, U_{13}(\phi_1, 0)\,, \tag{3.82}$$

with

$$\begin{cases} -\arctan\left(\sqrt{\frac{s_1}{s_2}}\right) \leq \theta \leq \arctan\left(\sqrt{\frac{s_1}{s_2}}\right) \\ \phi_1 = \pm\frac{1}{2}\arccos\left(\frac{s_2(2\tan^2(\theta)-1)}{s_1+s_3}\right) \\ \phi_2 = \begin{cases} \pi/4, \text{ if } \theta = 0 \text{ or } \sin(2\phi_1) = 0 \\ \frac{1}{2}\arctan\left(\frac{2s_2(\tan^2(\theta)-1)}{(s_1+s_3)\sin(\theta)\sin(2\phi_1)}\right), \text{ otherwise} \end{cases} \end{cases}, \tag{3.83}$$

that hollowises all the matrices $S_2', \ldots, S_n'$. If it is not the case, then the matrices $S_1, \ldots, S_n$ are not simultaneously hollowisable.

The set of orthogonal matrices used in this algorithm corresponds to the largest subset of the set gathering all orthogonal matrices hollowising D_1 (which we obtained in the previous section) that contains orthogonal matrices transforming 3×3 symmetric matrices into distinct matrices (up to rows and columns permutation or rephasing). As a consequence, if none of these orthogonal matrices hollowise the matrices $S_2', \ldots, S_n'$, then $S_2', \ldots, S_n'$ and D_1 cannot be simultaneously hollowisable. The reason why we have to consider the full range for the angle θ, as well as two solutions for the angle ϕ_1, instead of the minimal solution (3.80) for the matrices hollowising D_1 is that the matrices $S_2', \ldots, S_n'$ do not necessarily have the same form and the same symmetries as D_1, so that the unitary congruences with orthogonal matrices do not produce the same redundancies.

This algorithm transforms thus the simultaneous hollowisation problem for 3×3 symmetric matrices into an optimization over one real parameter. An advantage of this algorithm is that, when matrices are found to be simultaneously hollowisable, the unitary matrix realizing the hollowisation is given in the last step (as the product between the hollowising orthogonal matrix O and the diagonalizing unitary matrix U).

Transforming, in the first step of the algorithm, the matrix S_1 into a traceless diagonal matrix of the form (3.81) also provides a necessary condition for the simultaneous hollowisability of the matrices $D_1, S'_2, \ldots, S'_n$. Indeed, as a consequence of Proposition 3.3, if a unitary matrix U hollowises D_1, there exist a diagonal matrix of phases V and an orthogonal matrix O such that $U = VO$, which implies that U hollowises D_1 if and only if O hollowises D_1. Therefore, the matrices $D_1, S'_2, \ldots, S'_n$ are simultaneously hollowisable only if the matrices $S'_2, \ldots, S'_n$ are also hollowisable using an orthogonal matrix. As the unitary congruence with an orthogonal matrix preserves the trace, and since hollow matrices have a vanishing trace, the matrices $D_1, S'_2, \ldots, S'_n$ are simultaneously hollowisable only if $S'_2, \ldots, S'_n$ have a vanishing trace.

This condition can be added to the algorithm. If it is not fulfilled, it is indeed pointless to continue the execution of the algorithm. If it is fulfilled, then each matrix OS'_iO^T $(i = 2, \ldots, n)$ keeps a zero trace for any orthogonal matrix O of the form (3.82), and with angles θ, ϕ_1 and ϕ_2 satisfying conditions (3.83). To check if each OS'_iO^T is hollow, it is then sufficient to look at the vanishing of only two diagonal elements. If the elements of S'_i are written

$$S'_i = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}, \tag{3.84}$$

and we consider the first two diagonal elements, this is equivalent to the condition

$$\begin{aligned} \Big| \sin(2\theta)\Big(e\sin(\phi_1) - b\cos(\phi_1)\Big) + d\sin^2(\theta) + \cos^2(\theta)\left(a\cos^2(\phi_1) - c\sin(2\phi_1) + f\sin^2(\phi_1)\right) \Big| + \\ \Big| \Big(\cos(\phi_1)\cos(\phi_2)\sin(\theta) - \sin(\phi_1)\sin(\phi_2)\Big)\, t(b,c,a) + \cos(\theta)\cos(\phi_2)\, t(d,e,b) - \\ \Big(\sin(\phi_1)\cos(\phi_2)\sin(\theta) + \cos(\phi_1)\sin(\phi_2)\Big)\, t(e,f,c) \Big| = 0, \end{aligned} \tag{3.85}$$

with

$$\begin{aligned} t(a,b,c) = a\cos(\theta)\cos(\phi_2) - \sin(\phi_1)\Big(b\cos(\phi_2)\sin(\theta) + c\sin(\theta)\Big) \\ + \cos(\phi_1)\Big(c\cos(\phi_2)\sin(\theta) - b\sin(\phi_2)\Big). \end{aligned} \tag{3.86}$$

To avoid computing each time the matrix product OS'_iO^T, one could directly implement this condition into the algorithm.

3.6.4 Separability criterion for mixed states of rank 3

In this section, we show that the algorithm presented in the previous section to solve the simultaneous hollowisation problem for symmetric 3×3 matrices can be used to solve the separability problem for multipartite states of rank 3.

As shown in Theorem 3.5, having a criterion for simultaneous hollowisability (even if it is limited to matrices of given dimension) can provide a separability criterion. In general, if we want to address the separability problem for states of rank r (which have

preconcurrence matrices of dimension r), we need a simultaneous hollowisation criterion for matrices of dimension up to r^2, as we also have to take into account the extensions of the preconcurrence matrices up to dimension r^2. Using results from Ref. [70], we first show that for rank-3 states, we almost never have to consider extensions of the preconcurrence matrices to decide about separability.

Let us first consider a rank-3 multipartite mixed state ρ acting on a Hilbert space $\mathcal{H}$ and such that, when omitting the parties of ρ that have a rank-1 reduced density operator, ρ is not a bipartite state with rank-2 reduced density operators for both parties. According to Theorem 3.5, if such a state ρ is separable, then there exists a number p between 3 and 9 such that all the $p \times p$ extensions τ_α^{ext} of the preconcurrence matrices of ρ are simultaneously hollowisable for all $\alpha = 1, \ldots, Q(\mathcal{H})$, implying furthermore the existence of a separable decomposition of ρ containing p separable pure states. It was however shown in Ref. [70] that, if such a state ρ is separable, then it necessarily admits a separable decomposition containing only 3 product states. This means that ρ is separable if and only if its (unextended) preconcurrence matrices τ_α are all simultaneously hollowisable, which implies that it is never necessary to look at the simultaneous hollowisability of their extensions to decide about the separability of ρ.

This is a surprising result, even if it had already been noted that the case of preconcurrence matrices of dimensions 3 is particular. It is indeed the only dimension for which a preconcurrence matrix τ_α may not be hollowisable, while one of its extensions is. This happens if the singular values $s_1 \geq s_2 \geq s_3$ of τ_α satisfy $s_1 - s_2 - s_3 < 0$ (see the proof of Theorem 3.4). As a consequence, if ρ satisfies $C_\alpha(\rho) = 0$, extending the 3×3 preconcurrence matrix τ_α of ρ to a 4×4 matrix may be mandatory to find a hollow preconcurrence matrix associated to the C_α concurrence, whereas if ρ is separable (in which case it necessarily satisfies $C_\alpha(\rho) = 0, \forall \alpha$), its preconcurrence matrices τ_α must be *themselves* hollowisable, $\forall \alpha$. In other words, if for any value of α, the preconcurrence matrix τ_α needs to be extended to be hollowisable, then ρ cannot be separable. We can accordingly refine, for such rank-3 states ρ, the necessary condition of separability given by the vanishing of all concurrences $C_\alpha(\rho)$.

Proposition 3.4. *Let ρ be a rank-3 multipartite mixed state such that, when omitting the parties of ρ that have a rank-1 reduced density operator, ρ is not a bipartite state with rank-2 reduced density operators for both parties. If ρ is separable, then $C_\alpha(\rho) = 0$, $\forall \alpha$, and each associated preconcurrence matrix τ_α has singular values $s_1^\alpha \geq s_2^\alpha \geq s_3^\alpha$ satisfying*

$$s_1^\alpha - s_2^\alpha - s_3^\alpha = 0. \tag{3.87}$$

Let us now consider a rank-3 state ρ that, up to parties with rank-1 reduced density operator, is a bipartite state with rank-2 reduced density operator for both parties. As the parties with rank-1 reduced density operator have no influence on the separability of ρ, we can restrict ourselves to study the separability of σ, the bipartite reduced density operator of ρ corresponding to the two parties with rank-2 reduced density operator. Whatever Hilbert space the state ρ acts on, σ can be seen as a density operator acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$, i.e.

as a 2-qubit state. Its separability question (and thus the separability question of ρ) can therefore simply be answered using the 2-qubit separability criterion given in Theorem 3.1. By contrast to the other rank-3 states, separable states of this type can have separable decompositions containing 4 separable states [55, 70]. This is essentially due to the fact that the separability of these states is characterized by only one concurrence, so that there is no limitation on the number of states in any separable decomposition of such state coming from the simultaneous hollowisation of its preconcurrence matrices.

In conclusion, we can always decide about the separability of mixed states of rank 3 using criteria based on generalized concurrence and simultaneous hollowisation. This is summarized in the following theorem.

Theorem 3.8. *Let ρ be a rank-3 multipartite mixed state defined in the Hilbert space $\mathcal{H}$.*

When omitting parties with rank-1 reduced density operator, if ρ is a bipartite state with rank-2 reduced density operator for both parties, then ρ is separable if and only if

$$C(\sigma) = 0, \tag{3.88}$$

where C is the 2-qubit concurrence and σ is the reduced density operator of ρ corresponding to the two parties with rank-2 reduced density operator.

Otherwise, ρ is separable if and only if, for all $\alpha = 1, \ldots, Q(\mathcal{H})$, all its 3×3 preconcurrence matrices τ_α are simultaneously hollowisable.

In the second part of the theorem, the simultaneous hollowisability condition can be checked efficiently using Algorithm 3.1. As a consequence, concurrence based criteria can always efficiently solve the separability problem for mixed states of rank 3. Although it provides a new way to look at the separability problem, the separability criterion given in Theorem 3.8 is not the unique practical solution of the separability problem for multipartite mixed states of rank 3. It has indeed been shown that the PPT criterion is also a necessary and sufficient condition for the separability these states [70].

3.7 Hollowisation in a diagonal basis

Even though Thompson's Theorem 3.3 provides a simple criterion for the hollowisability of symmetric matrices, it does not allow to find the form of the hollowising unitaries. In this section, we consider the problem of hollowisation in a diagonal basis and show that in such basis, we can always find some particular examples of hollowising unitaries. This approach is based on the following reformulation of Thompson's Theorem 3.3, which was also shown in Ref. [65].

Theorem 3.9 (Thompson [65]). *Let $d = (d_1, \ldots, d_n)^T$ and $s = (s_1, \ldots, s_n)^T$ be complex column n-tuples with the numbering such that*

$$|d_1| \geq \cdots \geq |d_n|\,, \quad |s_1| \geq \cdots \geq |s_n|\,.$$

Then there exists a unitary matrix $U = (u_{ij})$ such that

$$d = (u_{ij}^2)s \tag{3.89}$$

if and only if

$$\sum_{i=1}^{k} |d_i| \leq \sum_{i=1}^{k} |s_i|\,, \quad 1 \leq k \leq n, \tag{3.90}$$

$$\sum_{i=1}^{k-1} |d_i| - \sum_{i=k}^{n} |d_i| \leq \sum_{\substack{i=1 \\ i\neq k}}^{n} |s_i| - |s_k|\,, \quad 1 \leq k \leq n, \tag{3.91}$$

$$\sum_{i=1}^{n-3} |d_i| - |d_{n-2}| - |d_{n-1}| - |d_n| \leq \sum_{i=1}^{n-2} |s_i| - |s_{n-1}| - |s_n|\,, \quad \text{if } n \geq 3. \tag{3.92}$$

Translated into the context of hollowisation, this theorem shows that a unitary matrix U with elements $(U)_{ij} = u_{ij}$ hollowises the diagonal matrix $diag(s_1, \ldots, s_n)$ if and only if

$$\begin{pmatrix} u_{11}^2 & u_{12}^2 & \ldots & u_{1n}^2 \\ u_{21}^2 & u_{22}^2 & \ldots & u_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1}^2 & u_{n2}^2 & \ldots & u_{nn}^2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3.93}$$

A symmetric matrix A is always unitarily congruent to a diagonal matrix whose elements are the singular values of A, in any order and with any phases [48]. As a consequence, Theorem 3.9 shows that for each unitary U hollowising A in this diagonal form, the diagonal elements must be solutions of an homogeneous linear system involving the squares of the elements of U. This system provides a new condition on the unitaries realizing the hollowisation: if a unitary matrix U hollowises a nonzero diagonal matrix, then the matrix V obtained by squaring all the elements of U must be singular, i.e. satisfy $\det(V) = 0$.

As an illustration, we show that the 4×4 hollowising unitary U found by W. K. Wootters [54] in his proof of Formula (3.9) corresponds to a solution of Eq. (3.93) with a matrix V having the lowest possible rank. We first remind how to build this hollowising unitary, which can be obtained for any 2-qubit mixed state ρ such that the square roots $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ (ordered decreasingly) of the eigenvalues of the operator $\rho S \rho^* S$ (with S the 2-qubit spin-flip operator) satisfy $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$. For such a state ρ, there always exists a decomposition $\mathcal{D} = \{|x_i\rangle, i = 1, \ldots, r\}$ (with r the rank of ρ), subnormalized so that $\rho = \sum_{i=1}^{r} |x_i\rangle\langle x_i|$, and such that $\tau^{\mathcal{D}}$ is the diagonal matrix $diag(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ [54]. Because of the condition $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$, ρ can only have rank 3 or 4. For convenience, if ρ has rank 3, we add a zero vector $|x_4\rangle$ in the decomposition $\mathcal{D}$. The separable decomposition

$\{|z_i\rangle, i = 1, \ldots, 4\}$ is then obtained through the change of basis [54]

$$\begin{aligned}
|z_1\rangle &= \tfrac{1}{2}\left(e^{i\phi_1}|x_1\rangle + e^{i\phi_2}|x_2\rangle + e^{i\phi_3}|x_3\rangle + e^{i\phi_4}|x_4\rangle\right), \\
|z_2\rangle &= \tfrac{1}{2}\left(e^{i\phi_1}|x_1\rangle + e^{i\phi_2}|x_2\rangle - e^{i\phi_3}|x_3\rangle - e^{i\phi_4}|x_4\rangle\right), \\
|z_3\rangle &= \tfrac{1}{2}\left(e^{i\phi_1}|x_1\rangle - e^{i\phi_2}|x_2\rangle + e^{i\phi_3}|x_3\rangle - e^{i\phi_4}|x_4\rangle\right), \\
|z_4\rangle &= \tfrac{1}{2}\left(e^{i\phi_1}|x_1\rangle - e^{i\phi_2}|x_2\rangle - e^{i\phi_3}|x_3\rangle + e^{i\phi_4}|x_4\rangle\right),
\end{aligned} \tag{3.94}$$

where the angles $\phi_1, \ldots, \phi_4$ are chosen so that $\sum_{j=1}^{4} e^{2i\,\phi_j}\lambda_j = 0$, which is always possible since $\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4 < 0$. One easily checks that all states $|z_i\rangle$ $(i = 1, \ldots, 4)$ have a zero 2-qubit concurrence, and are thus separable.

From this separable decomposition, we can deduce that the unitary matrix

$$U = \frac{1}{2}\begin{pmatrix} e^{i\phi_1} & e^{i\phi_2} & e^{i\phi_3} & e^{i\phi_4} \\ e^{i\phi_1} & -e^{i\phi_2} & e^{i\phi_3} & -e^{i\phi_4} \\ e^{i\phi_1} & e^{i\phi_2} & -e^{i\phi_3} & -e^{i\phi_4} \\ e^{i\phi_1} & -e^{i\phi_2} & -e^{i\phi_3} & e^{i\phi_4} \end{pmatrix} \tag{3.95}$$

hollowises the diagonal matrix $diag(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. The matrix V obtained by squaring each element in U is ensured to satisfy Eq. (3.93) for the vector $(\lambda_1, \ldots, \lambda_4)^T$, as the phases $e^{i\phi_j}$ $(j = 1, \ldots, 4)$ satisfy $\sum_{j=1}^{4} e^{2i\,\phi_j}\lambda_j = 0$. For this solution, the matrix V has identical rows and has thus rank 1. This corresponds to the simplest solution as, even though the condition $\det(V) = 0$ prevents V from having maximal rank, V could still have rank 2 or 3.

This procedure for building a unitary matrix hollowising an hollowisable diagonal matrix can straightforwardly be generalized to any dimension that is a power of 2. Choosing a sufficiently large dimension and discarding potential unnecessary columns, we can then use it to find hollowising unitaries for preconcurrence matrices corresponding to arbitrary multiqudit systems. As we already mentioned, this is however a simple solution, with few degrees of freedom, and it is unfortunately unlikely that such a solution helps solving the simultaneous hollowisation problem.

Chapter 4

Separable decompositions of PPT symmetric multiqubit states

Just like entanglement, separability is a property that is difficult to characterize. For instance, even when a state is known to be separable, it is in general difficult to obtain one separable decomposition. This emblematic feature of separable states (the fact that they admit at least one separable decomposition) remains poorly known. For instance, given a separable state ρ, one does in general not know its length, i.e. the minimal number of product state required in a separable decomposition of ρ, or the multiplicity of decompositions with such minimal cardinality. Concerning these two features of separable states, several specific results have nevertheless been obtained. Using arguments concerning facial structures of the convex set of separable states, it has for instance been shown that, in the set of bipartite separable states of length k acting on the Hilbert space $\mathbb{C}^m \otimes \mathbb{C}^n$, the subset of separable states with unique separable decomposition is dense and open if $k \leq \max(m, n)$ [71]. Using similar arguments, separable states with unique separable decomposition have also been found in multipartite systems [72]. Concerning the length of separable states, general results have been obtained for mixed states of ranks 2 and 3 [70].

As a byproduct of our research about the separability problem, we already obtained some results about separable decompositions of separable states in Chapter 3. In Theorem 3.5, we indeed showed that, given a mixed state ρ, the existence of a separable decomposition of ρ is equivalent to the existence of a unitary matrix allowing the simultaneous hollowisation of all the preconcurrence matrices of ρ (or their extensions). For separable states of rank 2, we provided a simple way to compute a separable decomposition over two product states and also demonstrated the unicity of this decomposition.

For separable states of rank 3, we gave an algorithm allowing to efficiently compute a separable decomposition over three product states.

In this chapter, we follow a different approach and use properties of the partial transposition operation to search for separable decompositions of separable states. In Section 4.1, we present an algorithm proposed in Ref. [73] to constructively check the separability of bipartite PPT states and show how to extend this algorithm to multipartite states. We then use this algorithm in Section 4.2 to prove general results about the separable decompositions of symmetric states of 2, 3 and 4 qubits.

4.1 The rank reduction algorithm

Although it is neither a common nor an easy approach to solve the separability problem, trying to explicitly reconstruct a separable decomposition can be a way of proving that a given state is separable. In Ref. [73], a constructive algorithm was proposed to reconstruct separable decompositions of bipartite PPT states acting on the space $\mathbb{C}^2 \otimes \mathbb{C}^M$. Given a PPT mixed state ρ acting on this space, the principle of this algorithm, that we call *rank reduction algorithm*, is to subtract projectors onto product states from ρ in order to decrease its rank (and the rank of its partial transposes[1]) while keeping the resulting mixed state PPT. If one can decrease the rank of ρ up to zero with this method, then ρ is obviously separable and the set of projectors that have been subtracted from ρ provides a separable decomposition of this state.

This rank reduction algorithm is mathematically based upon two lemmas shown in Ref. [73], that we briefly recall here. Given a bipartite PPT density operator ρ and a product state $|e, f\rangle$, let us define, as in Ref. [73]:

$$\tilde{\rho}(\rho, |e, f\rangle, \lambda) = \rho - \lambda |e, f\rangle\langle e, f|, \tag{4.1}$$

$$\lambda_0(\rho, |e, f\rangle) = \frac{1}{\langle e, f|\rho^{-1}|e, f\rangle}, \tag{4.2}$$

$$\overline{\lambda}_0(\rho, |e, f\rangle) = \frac{1}{\langle e^*, f| \left(\rho^{T_A}\right)^{-1} |e^*, f\rangle}, \tag{4.3}$$

where $|e^*\rangle$ denotes the complex conjugate of the state $|e\rangle$ in the computational basis, ρ^{T_A} denotes the partial transpose of ρ with respect to the first party and σ^{-1} denotes the pseudoinverse of the density operator σ, i.e. $\sigma^{-1} = \sum_{i=1}^{r} 1/\lambda_i \, |v_i\rangle\langle v_i|$ with r the rank of σ, λ_i $(i = 1, \ldots, r)$ its nonzero eigenvalues and $|v_i\rangle$ the associated eigenvectors. The operation transforming the product state $|e, f\rangle$ into $|e^*, f\rangle$ is a *partial conjugation*, performed here on the first party. Using a notation reminding the one used for the partial transposition, we also denote this operation by $(|e, f\rangle)^{C_A} \equiv |e^*, f\rangle$. The partial

[1] As the partial transposes of ρ with respect to the two parties (often called A and B in the case of bipartite systems) are related by a (full) transposition, they have the same spectrum, and thus the same rank. We can therefore restrict ourselves to consider one partial transpose, for example the one performed over party A, and only look at the rank of this partial transpose.

conjugation naturally extends to multipartite states, where it can be performed with respect to any subset of the parties.

On the one hand, denoting by $\mathcal{R}(\rho)$ the *range* of the density operator ρ, the condition under which the operator $\tilde{\rho}(\rho, |e, f\rangle, \lambda)$ is PPT reads:

Lemma 4.1 (Kraus *et al.* [73]). *$\tilde{\rho}(\rho, |e, f\rangle, \lambda)$ is PPT if and only if $|e, f\rangle \in \mathcal{R}(\rho)$, $|e^*, f\rangle \in \mathcal{R}(\rho^{T_A})$ and $\lambda \leq \min\Big(\lambda_0(\rho, |e, f\rangle), \overline{\lambda}_0(\rho, |e, f\rangle)\Big)$.*

On the other hand, the ranks of $\tilde{\rho}(\rho, |e, f\rangle, \lambda)$ and its partial transpose over party A differ from the ones of ρ and ρ^{T_A} in three situations:

Lemma 4.2 (Kraus *et al.* [73]). *Assuming $|e, f\rangle \in \mathcal{R}(\rho)$, $|e^*, f\rangle \in \mathcal{R}(\rho^{T_A})$, and simply denoting $\tilde{\rho}(\rho, |e, f\rangle, \lambda)$ by $\tilde{\rho}$,*

(i) *if $\lambda = \lambda_0(\rho, |e, f\rangle) < \overline{\lambda}_0(\rho, |e, f\rangle)$, then $r(\tilde{\rho}) = r(\rho) - 1$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A})$,*

(ii) *if $\lambda = \overline{\lambda}_0(\rho, |e, f\rangle) < \lambda_0(\rho, |e, f\rangle)$, then $r(\tilde{\rho}) = r(\rho)$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A}) - 1$,*

(iii) *if $\lambda = \lambda_0(\rho, |e, f\rangle) = \overline{\lambda}_0(\rho, |e, f\rangle)$, then $r(\tilde{\rho}) = r(\rho) - 1$ and $r(\tilde{\rho}^{T_A}) = r(\rho^{T_A}) - 1$.*

Subtracting a projector onto a product state, i.e. a rank-1 density operator, from a density operator ρ can obviously only decrease its rank, or the rank of its partial transpose, by at most one unit. As both ranks must be brought to zero, the success of the algorithm requires at least $\max\big[r(\rho), r(\rho^{T_A})\big]$ subtractions. Lemma 4.2 shows however that the rank of ρ and its partial transpose cannot always be reduced at the same time, explaining why the success of the algorithm may require some extra subtractions.

As a consequence of these lemmas, we can conclude that the central task in the rank reduction algorithm is to find product states $|e, f\rangle$ in the range of the density operator we wish to reduce the rank such that the partially conjugated state $|e^*, f\rangle$ is in the range of the partial transpose (over the first party) of this density operator. The success of the algorithm is however not guaranteed. By successively reducing the rank of a PPT state ρ using this method, one can indeed end up with a PPT state σ for which there exists no product state $|e, f\rangle \in \mathcal{R}(\sigma)$ such that $|e^*, f\rangle \in \mathcal{R}(\sigma^{T_A})$. Because subtracting from them any projector onto a product state always yields an NPT state, such states σ can be seen as lying on "the edge" of the set of PPT states and are therefore called *edge states* [74, 75]. Failure of the algorithm for a given state does however not prove that the state is entangled. The reason of the failure may also be that the set of product states chosen at each step of the algorithm is not part of a separable decomposition of the state.

As shown in Ref. [76], the rank reduction algorithm and the Lemmas 4.1 and 4.2 extend naturally to general bipartite states. We show in the next section that they can even be extended to multipartite states. This extension requires some adaptations, as there are, in the multipartite case, several bipartitions (and thus several partial transpositions) to consider.

4.1.1 Multipartite extension of the algorithm

Let us now consider an N-partite PPT state ρ acting on a Hilbert space $\mathcal{H}$. As in the bipartite case, we want to decrease the rank of ρ and its partial transposes by subtraction of projectors onto product states. Given such a product state $|\phi\rangle \in \mathcal{H}$, we now study the operator $\tilde{\rho}(\rho, |\phi\rangle, \lambda) = \rho - \lambda|\phi\rangle\langle\phi|$. The function $\overline{\lambda}_0(\rho, |e, f\rangle)$ of the bipartite algorithm generalizes, for any bipartition $S|\bar{S}$ of the N parties (with $\bar{S}$ denoting the complement of the subset S), to

$$\lambda_0^S(\rho, |\phi\rangle) = \frac{1}{\langle\phi'| \left(\rho^{T_S}\right)^{-1} |\phi'\rangle}, \tag{4.4}$$

with $|\phi'\rangle = (|\phi\rangle)^{C_S}$.

To obtain the condition under which $\tilde{\rho}(\rho, |\phi\rangle, \lambda)$ is a PPT operator, we just have to apply Lemma 4.1 to all distinct bipartitions of the N parties. This provides the following lemma:

Lemma 4.3. *$\tilde{\rho}(\rho, |\phi\rangle, \lambda)$ is PPT if and only if $|\phi\rangle \in \mathcal{R}(\rho)$, $\lambda \leq \lambda_0(\rho, |\phi\rangle)$ and, for all distinct bipartitions $S|\bar{S}$ of the parties, $(|\phi\rangle)^{C_S} \in \mathcal{R}(\rho^{T_S})$ and $\lambda \leq \lambda_0^S(\rho, |\phi\rangle)$.*

The conditions under which the ranks of $\tilde{\rho}(\rho, |\phi\rangle, \lambda)$ and its partial transposes change can be inferred from Lemma 4.2.

A lower bound on the number of subtractions required in a successful application of the algorithm is now given by the greatest rank among the rank of ρ itself and the ranks of all its partial transposes taken with respect to distinct bipartitions of the parties. For an N-partite state ρ, there are 2^{N-1} such ranks. For convenience, we put them into a (2^{N-1})-tuple called *rank configuration* of ρ.

Although the ideas and lemmas supporting the rank reduction algorithm are easily generalized to the multipartite case, the number of partial transpositions to consider, and thus the number of range conditions to verify, grows exponentially with the number of parties. This makes the algorithm quickly unpractical when the number of parties increases.

As pointed out in Ref. [77], this exponential growth of the number of partial transposes can be replaced by a linear growth when considering symmetric multiqubit states. We detail the adaptation of the rank reduction algorithm to symmetric states in the next section.

4.1.2 Rank reduction of symmetric multiqubit states

We consider now an N-qubit symmetric PPT state ρ_S. The permutation symmetry of ρ_S implies two simplifications in the rank reduction algorithm. First, as the range of ρ_S contains only symmetric states, a product state belonging to the range of ρ_S is necessarily of the form $|e, \ldots, e\rangle \equiv |e\rangle^{\otimes N}$, with $|e\rangle$ a 1-qubit state. Second, for a given subset S of the qubits, if $|e, \ldots, e\rangle \in \mathcal{R}(\rho_S)$ and $(|e, \ldots, e\rangle)^{C_S} \in \mathcal{R}(\rho_S^{T_S})$, then $(|e, \ldots, e\rangle)^{C_{S'}} \in \mathcal{R}(\rho_S^{T_{S'}})$ for all subset S' of the qubits such that $\#S = \#S'$. Instead of considering the partial

transpositions and partial conjugations with respect to all distinct bipartitions, we can thus restrict ourselves to considering partial transpositions and conjugations over the first k qubits, for all $k = 1, \ldots, \lfloor N/2 \rfloor$. We simply denote by $\rho_S^{T_{(k)}}$ the partial transpose of ρ_S over the first k qubits and by $(|e, \ldots, e\rangle)^{C_{(k)}}$ the partial conjugation of $|e, \ldots, e\rangle$ over these k first qubits. These two properties of symmetric states considerably simplify the search for the suitable product states to subtract from ρ_S.

The permutation symmetry also implies $r(\rho_S^{T_S}) = r(\rho_S^{T_{S'}})$ when $\#S = \#S'$. We therefore drop these redundancies in the rank configuration of ρ_S, so that it merely becomes the $(\lfloor N/2 \rfloor + 1)$-tuple constituted by the rank of ρ_S and the ranks of its partial transposes $\rho_S^{T_{(k)}}$, for all $k = 1, \ldots, \lfloor N/2 \rfloor$. Working with symmetric states presents the additional advantage of providing nontrivial upper bounds on all the ranks of their rank configuration. Indeed, as it acts on the symmetric subspace of the N-qubit Hilbert space, ρ_S itself has a rank that is at most equal to $N + 1$. As partial transposition breaks the permutation symmetry of the qubits, any partial transpose $\rho_S^{T_{(k)}}$ does not act on the symmetric subspace and may therefore have a greater rank. The symmetry breaking is however only partial: it is broken across the bipartition $1 \cdots k | k+1 \cdots N$, but the reduced density operators corresponding to the first k qubits and the last $N - k$ ones remain permutation invariant. As a consequence, the partial transpose $\rho_S^{T_{(k)}}$ $(k = 1, \ldots, \lfloor N/2 \rfloor)$ can be considered as a density operator acting on the bipartite Hilbert space $\mathcal{H} = \mathcal{H}_S^{(k)} \otimes \mathcal{H}_S^{(N-k)}$, where $\mathcal{H}_S^{(k)}$ and $\mathcal{H}_S^{(N-k)}$ are the symmetric subspaces corresponding the Hilbert spaces of k- and $(N-k)$-qubit systems. This provides the following upper bound on their ranks [77]

$$r(\rho_S^{T_{(k)}}) \leq (k+1)(N-k+1), \ \forall k = 1, \ldots, \lfloor N/2 \rfloor. \tag{4.5}$$

These bounds show that symmetric states have limited rank configurations. This is interesting as low rank multipartite states appear to have particular separability properties [70]. We review some of these properties in the next section.

4.1.3 Low rank states and optimal separable decompositions

In general, the rank configuration of a separable state reflects the complexity of its separable decompositions. The minimal number of separable states required to build a separable decomposition of a separable state ρ is indeed lower bounded by the greatest rank appearing in its rank configuration, and upper bounded by $r(\rho)^2$ [66]. This minimal number of separable states is often called *length* or *optimal cardinality* of the separable state ρ and denoted by $\mathcal{L}(\rho)$. It also corresponds to the minimal dimension of the extensions of the preconcurrence matrices τ_α^{ext} of a separable state such that these extended preconcurrence matrices are simultaneously hollowisable for all α (see Theorem 3.5).

The length of a separable state is generally hard to determine. Some general values of length are nevertheless known for low rank states [70]. We summarize here some important results about the lengths of low rank states.

In the separability criterion of Theorem 3.7, based on simultaneous hollowisation of 2×2 matrices, we showed that separable states of rank 2 have length 2. This had been previously shown using the PPT criterion:

Theorem 4.1 (Chen & Đokovic [70]). *A density operator ρ of rank 2 is separable if and only if it is PPT, in which case we have also $\mathcal{L}(\rho) = 2$.*

As we show in the following corollary, this completely fixes the rank configuration of PPT states of rank 2.

Corollary 4.1. *An N-partite PPT state ρ has $r(\rho) = 2$ if and only if, for any subset S of the parties, $r(\rho^{T_S}) = 2$.*

Proof. (*Necessary condition*) As a consequence of Theorem 4.1, if ρ is a rank-2 PPT state, then it is separable and has length 2. Since the length of a state must be greater than or equal to any element of its rank configuration, we have thus, for any subset S of the parties, $r(\rho^{T_S}) \leq 2$. Whatever subset S, the rank of ρ^{T_S} can however not be equal to 1, as it would imply that ρ is a separable pure state, in which case it cannot have a rank equal to 2. We have therefore $r(\rho^{T_S}) = 2$ for all subsets S of the parties. (*Sufficient condition*) As ρ is a PPT state, ρ^{T_S} is also PPT. In addition, ρ is nothing but the partial transpose of ρ^{T_S} with respect to the subset S of the parties. Applying the necessary condition to the rank-2 PPT density operator ρ^{T_S} yields therefore $r(\rho) = 2$. □

The PPT criterion turns out to also solve the separability problem for rank-3 states. However, there exist PPT states of rank 3 with a length greater than 3:

Theorem 4.2 (Chen & Đokovic [70]). *A density operator ρ of rank 3 is separable if and only if it is PPT, in which case it has $\mathcal{L}(\rho) \in \{3, 4\}$. Omitting trivial parties of ρ having a rank-1 reduced density operator, $\mathcal{L}(\rho) = 4$ is only possible if ρ is a bipartite state with $r(\mathrm{Tr}_1\, \rho) = r(\mathrm{Tr}_2\, \rho) = 2$.*

This theorem also fixes the rank configuration of PPT states of rank 3. We distinguish two cases depending on their length.

Corollary 4.2. *A rank-3 PPT state has length 4 if and only if it is a bipartite state (when omitting trivial parties with a rank-1 reduced density operator) with rank configuration $(3, 4)$.*

Proof. (*Necessary condition*) As a consequence of Theorem 4.2, if ρ is a rank-3 PPT state with length 4, then (omitting trivial parties with a rank-1 reduced density operator) it is a bipartite state with $r(\mathrm{Tr}_1\, \rho) = r(\mathrm{Tr}_2\, \rho) = 2$. The partial transpose of ρ with respect to the first party cannot have a rank greater than the length of ρ, so $r(\rho^{T_1}) \leq 4$. Let us span the values of $r(\rho^{T_1})$ from 1 to 3 to show that they are incompatible with the rank and length of ρ. If $r(\rho^{T_1}) = 1$, then ρ is a pure product state with $r(\rho) = 1$. If $r(\rho^{T_1}) = 2$, Corollary 4.1 implies $r(\rho) = 2$. Finally, if $r(\rho^{T_1}) = 3$, let us apply the rank

reduction algorithm to show that $\mathcal{L}(\rho) = 3$. As ρ is separable, we can indeed always find a product state $|e, f\rangle \in \mathcal{R}(\rho)$ such that $|e^*, f\rangle \in \mathcal{R}(\rho^{T_1})$. As a consequence of Corollary 4.1, bipartite states with rank configuration $(2, 3)$ or (3,2) do not exist. This implies that when subtracting a projector onto $|e, f\rangle$ from ρ to decrease its rank, the resulting state $\tilde{\rho}(\rho, |e, f\rangle, \lambda)$ with $\lambda = \min\Big(\lambda_0(\rho, |e, f\rangle), \overline{\lambda}_0(\rho, |e, f\rangle)\Big)$ is necessarily a PPT state with rank configuration (2,2). Such a state has length 2 because of Theorem 4.1 and we have thus $\mathcal{L}(\rho) = 3$. The only possible value for $r(\rho^{T_1})$ is therefore 4, which concludes the proof of the necessary condition. (*Sufficient condition*) As a consequence of Theorem 4.2, a PPT state ρ of rank 3 has length 3 or 4. However, $r(\rho^{T_1}) = 4$ implies $\mathcal{L}(\rho) \geq 4$, so that ρ has length 4. □

Corollary 4.3. *Omitting trivial parties having a rank-*1 *reduced density operator, if a PPT state ρ is not a bipartite state with $r(\mathrm{Tr}_1\,\rho) = r(\mathrm{Tr}_2\,\rho) = 2$, then $r(\rho) = 3$ if and only if, for any subset S of the parties, $r(\rho^{T_S}) = 3$.*

Proof. (*Necessary condition*) As a consequence of Theorem 4.2, the rank-3 PPT state ρ must have length 3. This implies, for any subset S of the parties, $r(\rho^{T_S}) \leq 3$. As a consequence of Corollary 4.1, we cannot have $r(\rho^{T_S}) = 2$ as it would imply $r(\rho) = 2$. Similarly, $r(\rho^{T_S}) = 1$ is impossible as it would imply that ρ is a separable pure state, in which case we have $r(\rho) = 1$. The only possibility is therefore $r(\rho^{T_S}) = 3$. (*Sufficient condition*) As ρ is a PPT state, ρ^{T_S} is also PPT. Furthermore, ρ is nothing but the partial transpose of ρ^{T_S} with respect to the subset S of the parties. Applying the necessary condition to the rank-3 PPT density operator ρ^{T_S} yields therefore $r(\rho) = 3$. □

As we show in the next section, these theorems and corollaries complement well the rank reduction algorithm to study optimal separable decompositions (i.e. separable decompositions of a separable state ρ containing $\mathcal{L}(\rho)$ product states) of symmetric multiqubit states.

4.2 Optimal separable decompositions of symmetric multiqubit states

In this section, we show that the rank reduction algorithm and the separability properties of low rank states can be exploited to obtain general results about length and optimal separable decompositions of symmetric multiqubit states. We successively consider 2-qubit, 3-qubit and 4-qubit systems.

4.2.1 2-qubit system

A 2-qubit symmetric separable density operator ρ_S has a rank that is at most equal to 3. Its length depends on its rank and the rank of its partial transpose $\rho_S^{T_1}$, for which the general bound (4.5) reads $\rho^{T_1} \leq 4$. If $r(\rho_S) = 2$, then $\mathcal{L}(\rho_S) = 2$ (Theorem 4.1). If

$r(\rho_S) = 3$, then $\mathcal{L}(\rho_S) = 3$ if $r\left(\rho_S^{T_1}\right) = 3$, and $\mathcal{L}(\rho_S) = 4$ if $r\left(\rho_S^{T_1}\right) = 4$ (Theorem 4.2 and Corollary 4.2). If $r(\rho_S) = 2$, Theorem 3.7 implies that ρ_S has a unique optimal separable decomposition. We now study optimal separable decompositions of 2-qubit symmetric states of rank 3.

Let us consider the most general case of a 2-qubit symmetric separable state ρ_S with rank configuration $(3, 4)$. In this case, any 2-qubit product state $|e, e\rangle$ belongs to $\mathcal{R}(\rho_S)$ and is such that $|e^*, e\rangle \in \mathcal{R}(\rho_S^{T_1})$, since both ranges are maximal. Any symmetric product state can thus be subtracted from ρ_S, while keeping it PPT, as long as the associated weight λ satisfies Lemma 4.1. As a consequence of Corollary 4.1, we cannot have $\lambda_0(\rho_S, |e, e\rangle) \leq \overline{\lambda}_0(\rho_S, |e, e\rangle)$, as the state $\tilde{\rho}\Big(\rho_S, |e, e\rangle, \lambda_0(\rho_S, |e, e\rangle)\Big)$ would either have rank configuration $(2, 3)$ or rank configuration $(2, 4)$, which are both impossible. We must therefore have $\lambda_0(\rho_S, |e, e\rangle) > \overline{\lambda}_0(\rho_S, |e, e\rangle)$ and the state $\tilde{\rho}_1 \equiv \tilde{\rho}\Big(\rho_S, |e, e\rangle, \overline{\lambda}_0(\rho_S, |e, e\rangle)\Big)$ has the rank configuration $(3, 3)$. This means that the kernel[2] of the operator $\tilde{\rho}_1^{T_1}$ has dimension 1 and contains thus 1 state (up to global phase), that we denote by $|\chi\rangle$. A direct computation shows that $\tilde{\rho}_1^{T_1}\left(\rho_S^{T_1}\right)^{-1}|e^*, e\rangle = 0$, which implies that $|\chi\rangle = \left(\rho_S^{T_1}\right)^{-1}|e^*, e\rangle$. As we show now, the permutation symmetry of ρ_S induces constraints on the state $|\chi\rangle$.

In the computational basis, the 2-qubit symmetric states ρ_S has the general form

$$\rho_S = \begin{pmatrix} r_1 & c_1 & c_1 & c_2 \\ c_1^* & r_2 & r_2 & c_3 \\ c_1^* & r_2 & r_2 & c_3 \\ c_2^* & c_3^* & c_3^* & r_3 \end{pmatrix}, \tag{4.6}$$

with $r_1, r_2, r_3 \in \mathbb{R}$ and $c_1, c_2, c_3 \in \mathbb{C}$, and its partial transpose $\rho_S^{T_1}$ reads

$$\rho_S^{T_1} = \begin{pmatrix} r_1 & c_1 & c_1^* & r_2 \\ c_1^* & r_2 & c_2^* & c_3^* \\ c_1 & c_2 & r_2 & c_3 \\ r_2 & c_3 & c_3^* & r_3 \end{pmatrix}. \tag{4.7}$$

The pseudoinverse operator ρ_S^{-1} keeps the same structure as ρ_S in terms of real and complex elements. By contrast, the pseudoinverse operator $\left(\rho_S^{T_1}\right)^{-1}$ loses one symmetry

[2]We remind that the kernel of a density operator ρ acting on a Hilbert space $\mathcal{H}$ is the subspace

$$\mathcal{K}(\rho) = \{|\psi\rangle \in \mathcal{H} \mid \rho|\psi\rangle = 0\}.$$

Denoting by $k(\rho)$ the dimension of $\mathcal{K}(\rho)$, we have $\dim(\mathcal{H}) = r(\rho) + k(\rho)$.

compared to $\rho_S^{T_1}$:

$$\left(\rho_S^{T_1}\right)^{-1} = \begin{pmatrix} r'_1 & c'_1 & (c'_1)^* & r'_2 \\ (c'_1)^* & r'_3 & c'_2 & c'_3 \\ c'_1 & (c'_2)^* & r'_3 & (c'_3)^* \\ r'_2 & (c'_3)^* & c'_3 & r'_4 \end{pmatrix}, \tag{4.8}$$

with $r'_1, r'_2, r'_3, r'_4 \in \mathbb{R}$ and $c'_1, c'_2, c'_3 \in \mathbb{C}$. This structure implies that applying the operator $\left(\rho_S^{T_1}\right)^{-1}$ to a product state of the form $|e^*, e\rangle$ always yields a state $|\chi\rangle$ of the form

$$|\chi\rangle = a|00\rangle + \gamma|01\rangle + \gamma^*|10\rangle + b|11\rangle, \text{ with } a, b \in \mathbb{R} \text{ and } \gamma \in \mathbb{C}. \tag{4.9}$$

The form of $|\chi\rangle$ may suggest that it is the partial conjugation of a symmetric product state. It is however not, as the first and last components are real but not necessarily positive. The state $|\chi\rangle$ is generally an entangled state.

If we want to further decrease the rank of $\tilde{\rho}_1$, we must search a 1-qubit state $|e_2\rangle$ such that $|e_2, e_2\rangle \in \mathcal{R}(\tilde{\rho}_1)$ and $|e_2^*, e_2\rangle \in \mathcal{R}(\tilde{\rho}_1^{T_1})$, which is equivalent to $\langle\chi|e_2^*, e_2\rangle = 0$. Using the simple parametrization $|e\rangle = |0\rangle + \alpha|1\rangle$, with $\alpha \in \mathbb{C}$, we find that the state we are looking for must have

$$\alpha = -\frac{\gamma}{b} + r\, e^{i\theta}, \tag{4.10}$$

with $r = \sqrt{(|\gamma|/b)^2 - a/b}$ and $\theta \in [0, 2\pi[$.

This set of complex numbers α forms a circle into the complex plane. Each point of this circle corresponds to a state $|e_2\rangle$, which (after normalization) can be used to decrease the rank of $\tilde{\rho}_1$ or its partial transpose. Except when $r = 0$, in which case the circle collapses into a point, we thus have some freedom to choose the second separable state of the separable decomposition of ρ_S that we are building using the rank reduction algorithm. We must this time have $\lambda_0(\tilde{\rho}_1, |e_2, e_2\rangle) = \overline{\lambda}_0(\tilde{\rho}_1, |e_2, e_2\rangle)$ as, because of Corollary 4.1, the ranks of $\tilde{\rho}_1$ and its partial transpose must be reduced at the same time. The state $\tilde{\rho}_2 \equiv \tilde{\rho}\Big(\tilde{\rho}_1, |e_2, e_2\rangle, \lambda_0(\tilde{\rho}_1, |e_2, e_2\rangle)\Big)$ is a thus PPT state with rank configuration $(2, 2)$. Such a state is always separable and has length 2. Its unique optimal separable decomposition can be found using Theorem 3.7. Adding the corresponding product states and weights to the 2 states and weights we already subtracted from ρ_S provides a separable decomposition of ρ_S containing 4 states. Such a decomposition is in addition optimal as $\mathcal{L}(\rho_S) = 4$.

In conclusion, we showed that given a 2-qubit separable symmetric state ρ_S with rank configuration $(3, 4)$, the rank reduction algorithm always succeeds in decomposing ρ_S as a sum of projectors onto product states. In addition, the corresponding separable decomposition always contains 4 states and is thus always optimal. As both the ranks of ρ_S and its partial transpose $\rho_S^{T_1}$ are maximal, we also noticed that the symmetric product state chosen in the first step is totally arbitrary. Using the rank reduction algorithm, we can thus build an optimal separable decomposition of ρ_S from any 2-qubit symmetric product state $|e, e\rangle$. This is summarized in the following theorem.

Theorem 4.3. *A 2-qubit symmetric separable state ρ_S with rank configuration $(3,4)$ admits an infinite number of optimal separable decompositions such that any 2-qubit product state $|e,e\rangle$ is part of an optimal separable decomposition of ρ_S.*

In the next section, we study the optimal separable decompositions of symmetric states of 3 qubits.

4.2.2 3-qubit system

A 3-qubit symmetric density operator ρ_S has a rank that is at most equal to 4. Due to the permutation symmetry, we can restrict ourselves to consider only the partial transpose $\rho_S^{T_{(1)}}$ when applying the rank reduction algorithm to ρ_S (as explained in Section 4.1.2). According to the bound (4.5), this partial transpose has a rank satisfying $r(\rho_S^{T_{(1)}}) \leq 6$. It was shown in Ref. [78] that a 3-qubit symmetric state is separable if and only if it is PPT. Using the rank reduction algorithm, we can further determine its length. This is the object of the following theorem.

Theorem 4.4. *A 3-qubit separable symmetric state ρ_S has a length equal to the rank of its partial transpose over the first qubit.*

Proof. Since the state ρ_S is separable, it is necessarily PPT [27] and we can thus apply the rank reduction algorithm to try to reconstruct a separable decomposition of this state. At each step of the algorithm, we keep a symmetric 3-qubit PPT state, hence a separable state [78]. This ensures that we can decrease the rank of ρ_S up to zero, and effectively build a separable decomposition of this state. To see how many steps are required in the algorithm, it is useful to make a list of the possible rank configurations of ρ_S. If the separable state ρ_S has rank 1, it can obviously only have the rank configuration $(1,1)$. If $r(\rho_S) = 2$, then Corollary 4.1 implies that ρ_S has the rank configuration $(2,2)$. Since ρ_S is a symmetric state, its three parties have identical reduced density operators. As a consequence, ρ_S always satisfies the hypotheses of Corollary 4.3, so that if $r(\rho_S) = 3$, then ρ_S has necessarily the rank configuration $(3,3)$. Finally, if ρ_S has maximal rank, i.e. $r(\rho_S) = 4$, then its partial transpose $\rho_S^{T_{(1)}}$ cannot have a rank lower than 4 due to Corollaries 4.1 and 4.3. As a consequence, if ρ_S has maximal rank, its possible rank configurations are $(4,4)$, $(4,5)$ and $(4,6)$.

In any case, we always have $r(\rho_S) \leq r(\rho_S^{T_{(1)}})$, so that the length of the separable state ρ_S is at least equal to $r(\rho_S^{T_{(1)}})$. We now prove that the rank reduction algorithm always provides a separable decomposition of ρ_S containing a number a product states equal to $r(\rho_S^{T_{(1)}})$. Due to the possible rank configurations of ρ_S, it turns out to be impossible to decrease its rank without decreasing also the rank of its partial transpose $\rho_S^{T_{(1)}}$. As a consequence, at any step of the rank reduction algorithm, we must always decrease the rank of $\rho_S^{T_{(1)}}$. If $r(\rho_S^{T_{(1)}}) > 4$, we can only decrease the rank of $\rho_S^{T_{(1)}}$. Otherwise, we must

decrease the ranks of both ρ_S and $\rho_S^{T_{(1)}}$. The rank reduction algorithm has thus a number of steps equal to the rank of $\rho_S^{T_{(1)}}$, implying $\mathcal{L}(\rho_S) = r(\rho_S^{T_{(1)}})$. □

In the proof of this theorem, we showed that the rank reduction algorithm always provides an optimal separable decomposition for 3-qubit PPT symmetric states. When considering a 3-qubit PPT state ρ_S with the maximal rank configuration $(4, 6)$, the first product state of the decomposition can in addition be chosen arbitrarily among all symmetric product states of 3 qubits. This is due to the fact that when the ranges of ρ_S and its partial transpose $\rho_S^{T_{(1)}}$ are maximal, any product state $|e, e, e\rangle$ (with $|e\rangle$ a 1-qubit state) belongs to $\mathcal{R}(\rho_S)$ and is such that $|e^*, e, e\rangle \in \mathcal{R}(\rho_S^{T_{(1)}})$. This shows that Theorem 4.3 extends to symmetric states of 3 qubits:

Theorem 4.5. *A symmetric 3-qubit state ρ_S with the maximal rank configuration $(4, 6)$ admits an infinite number of optimal separable decompositions such that for any 1-qubit state $|e\rangle$, it is always possible to build an optimal separable decomposition of ρ_S containing the product state $|e, e, e\rangle$.*

In the following section, we show that Theorem 4.5 does however not extend to symmetric states of 4 qubits.

4.2.3 4-qubit system

A 4-qubit symmetric density operator ρ_S has a rank that is at most equal to 5. By contrast to the case of symmetric states of 3 qubits, we must here explicitly use the multipartite framework of the rank reduction algorithm, as there are two distinct partial transposes to consider, namely $\rho_S^{T_{(1)}}$ and $\rho_S^{T_{(2)}}$. According to the general bound (4.5), the ranks of these partial transposes satisfy $r(\rho_S^{T_{(1)}}) \leq 8$ and $r(\rho_S^{T_{(2)}}) \leq 9$.

We prove here by a counterexample that for a 4-qubit symmetric separable state ρ_S with the maximal rank configuration $(5, 8, 9)$, any 4-qubit symmetric product state $|e, e, e, e\rangle$ is not necessarily part of an optimal separable decomposition of ρ_S.

We consider the separable state

$$\rho_S = \frac{1}{9} \sum_{j=1}^{3} \sum_{k=0}^{2} \Big(\Big| \psi(j\,\pi/4, k\,2\pi/3) \Big\rangle \Big\langle \psi(j\,\pi/4, k\,2\pi/3) \Big| \Big)^{\otimes 4}, \tag{4.11}$$

with $|\psi(\theta, \phi)\rangle$ the usual Bloch representation of single qubit states, that is

$$|\psi(\theta, \phi)\rangle = \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}\,e^{i\phi}\,|1\rangle. \tag{4.12}$$

This state has the maximal rank configuration $(5, 8, 9)$, which in particular implies that its length is at least equal to 9. Since it is build as a convex sum of 9 projectors onto product states, we can conclude that its length is precisely equal to 9. Due to the fact that

ρ_S has the maximal rank configuration, any 4-qubit symmetric product state $|e,e,e,e\rangle$ belongs to $\mathcal{R}(\rho_S)$ and is such that $|e^*,e,e,e\rangle \in \mathcal{R}(\rho_S^{T_{(1)}})$ and $|e^*,e^*,e,e\rangle \in \mathcal{R}(\rho_S^{T_{(2)}})$. Such a state $|e,e,e,e\rangle$ can therefore always be used to decrease at least one element of the rank configuration of ρ_S.

If we choose this product state to be the state $|0000\rangle$, we have

$$\lambda_0(\rho_S,|0000\rangle) > \lambda_0^{1,2}(\rho_S,|0000\rangle) > \lambda_0^1(\rho_S,|0000\rangle). \tag{4.13}$$

This implies that we can only reduce the rank of $\rho_S^{T_{(1)}}$ by using a projector onto the state $|0000\rangle$. The state

$$\tilde{\rho}_S = \rho_S - \lambda_0^1(\rho_S,|0000\rangle)\,|0000\rangle\langle 0000| \tag{4.14}$$

is thus a PPT state with rank configuration $(5,7,9)$. If it is still a separable state, then by continuing the rank reduction algorithm, we might be able to reconstruct a separable decomposition of ρ_S containing the state $|0000\rangle$. This decomposition can however not be optimal. Indeed, as $r(\tilde{\rho}_S^{T_{(2)}}) = 9$, we have $\mathcal{L}(\tilde{\rho}_S) \geq 9$ and if we succeed in building a separable decomposition of ρ_S containing the state $|0000\rangle$, this decomposition will at least contain 10 product states (which is more than the length of ρ_S).

By contrast, for all the product states $|\psi_{j,k}\rangle \equiv |\psi(j\,\pi/4, k\,2\pi/3)\rangle^{\otimes 4}$, with $j = 1,2,3$ and $k = 0,1,2$, appearing in the separable decomposition (4.11) of ρ_S, we have

$$\lambda_0(\rho_S,|\psi_{j,k}\rangle > \lambda_0^1(\rho_S,|\psi_{j,k}\rangle) > \lambda_0^{1,2}(\rho_S,|\psi_{j,k}\rangle) = \frac{1}{9}. \tag{4.15}$$

It is most likely that such a counterexample can also be found for symmetric states of more than 4 qubits. The freedom we have in building optimal separable decompositions of 2- and 3-qubit symmetric states with maximal rank configuration is essentially due to their low ranks and the fact that the study of their separability requires to consider only one partial transpose.

Chapter 5

Entanglement quantification of symmetric multiqubit states

Quantifying entanglement is a complex task. Since different entanglement measures are often maximized by different entangled states, it is in most systems not possible to establish an absolute hierarchy between entangled states. This is essentially due to the fact that entanglement measures do not quantify entanglement in its entirety but rather quantify a specific feature of entanglement. For instance, the geometric measure of entanglement [43] quantifies the "distance" between an entangled state and the "closest" separable state (measured through the fidelity), the 3-tangle [79] quantifies the amount of tripartite correlations in 3-qubit entangled states and the negativity [80, 81] quantifies how far an entangled state is from having the PPT property. In that regard, the large number of functions that have been proposed to quantify entanglement (see for instance the list given in Ref. [37]) gives a good insight of the diversity of the properties of entangled states.

In this chapter, we focus on the quantification of entanglement properties of symmetric multiqubit states. In Refs. [82, 83], it had been noticed from numerical computations and analytical considerations that symmetric states corresponding to large values of the geometric measure of entanglement have highly scattered Majorana points on the Bloch sphere. In light of this observation, we aim at building a function that would quantify the entanglement of SLOCC-equivalent symmetric states through the distance between their Majorana points on the Bloch sphere.

In Section 5.1, we consider the entanglement quantification within SLOCC classes and show how the special properties of symmetric states under SLOCC can simplify the quantification problem. In Section 5.2, we review the Majorana representation of symmetric states and develop geometrical tools that are useful to study the distribution of the Majorana points on the Bloch sphere. In Section 5.3, we propose a function to quantify the entanglement of SLOCC-equivalent symmetric multiqubit states through

their Majorana points configuration. Finally, in Section 5.3.3, we relate this type of quantification to the mathematical problem that consists in finding the configuration of points on a sphere that minimizes a given potential energy.

5.1 Entanglement quantification in SLOCC classes

Although entanglement characterization tools for multiqubit states can always be particularized to symmetric multiqubit states, it is sometimes also possible to develop characterization methods specifically dedicated to symmetric states. For instance, in the context of the classification of entanglement with respect to local operations, a classification of entanglement specifically dedicated to symmetric states and defined upon their Majorana representation has been proposed in Ref. [25]. In the context of entanglement quantification, it is by contrast not possible to define an entanglement measure that would be specifically dedicated to symmetric multiqubit states. This is due to the fact entanglement measures have to satisfy the monotonicity under LOCC axiom (see Section 1.3.3), while LOCC do not necessarily preserve the permutation symmetry.

To circumvent this pitfall, we use the link between entanglement monotones and homogeneous functions that are invariant under det-1 local operations shown in Ref. [84] to propose a quantification of entanglement inside SLOCC classes. In this context, we then show that the specific properties of symmetric states under SLOCC can be exploited to develop entanglement quantification functions that are exclusively dedicated to symmetric states.

Let us first introduce the following theorem from Ref. [84].

Theorem 5.1 (Eltschka *et al.* [84]). *A positive homogeneous function $\mu(\psi)$ of the pure multiqubit state $|\psi\rangle$ that is invariant under local determinant-1 operations and such that*

$$\mu(\lambda\psi) = \lambda^\eta \mu(\psi), \text{ with } \eta, \lambda > 0,$$

is an entanglement monotone if and only if $\eta \leq 4$.

If $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent N-qubit pure states, then there exist invertible operators $A_1, \ldots, A_N \in \mathrm{GL}(2,\mathbb{C})$ such that $|\psi\rangle = A_1 \otimes \cdots \otimes A_N |\phi\rangle$ [18]. Up to a multiplicative constant, each element of the ILO can be rescaled into a det-1 operator since there exist angles $\theta_i \in [0, 2\pi[$ such that $A_i = \sqrt{|\det(A_i)|}\, e^{i\theta_i} A_i'$ with $\det(A_i') = 1$ for all $i = 1, \ldots, N$. For any entanglement monotone μ satisfying Theorem 5.1, we then have

$$\mu(\psi) = \mu\left(\prod_{i=1}^{N} \sqrt{|\det(A_i)|}\, e^{i\theta_i} \left(A_1' \otimes \cdots \otimes A_N'\, \phi\right)\right) = \left(\prod_{i=1}^{N} \sqrt{|\det(A_i)|}\right)^{\eta} \mu(\phi). \quad (5.1)$$

As a consequence, if μ vanishes for one state of the SLOCC class of the states $|\psi\rangle$ and $|\phi\rangle$, then it must vanish on the whole SLOCC class. By contrast, if μ is nonzero on this SLOCC class, then we can deduce whether the state $|\psi\rangle$ is more entangled than the state

$|\phi\rangle$ (according to the entanglement measure μ) by looking only at the determinant of the ILO connecting these two states, whatever the precise form of the entanglement monotone μ. In addition, this also shows that the degree of the homogeneous function μ has no influence on the entanglement hierarchy between SLOCC-equivalent states induced by the entanglement measure μ.

If we now consider two symmetric SLOCC-equivalent states $|\psi_S\rangle$ and $|\phi_S\rangle$, it is always possible to connect them through a symmetric ILO [35]. As for nonsymmetric states, we could consider quantifying the entanglement of these symmetric states through the value of the determinant of the symmetric ILO connecting them. To stay in the symmetric subspace and quantify the entanglement of symmetric states only, we would however need a function that preserves the permutation symmetry. Based on the previous comments, we make the following observation.

Observation 5.1. *A strictly positive homogeneous function $\tau_{\mathcal{C}}(\psi_S)$ of the pure symmetric multiqubit state $|\psi_S\rangle$ belonging to the SLOCC class $\mathcal{C}$ that is invariant under any* det*-1 symmetric ILO and such that*

$$\tau_{\mathcal{C}}(\lambda\psi_S) = \lambda^{\kappa}\tau_{\mathcal{C}}(\psi_S), \text{ with } \kappa, \lambda > 0,$$

would lead, in the symmetric subspace of the SLOCC class $\mathcal{C}$, to the same quantification of entanglement as any nonzero homogeneous function satisfying Theorem 5.1. Since symmetric ILOs preserve the permutation symmetry, such a function could be defined in the symmetric space only and exploit specific properties of symmetric states to quantify their entanglement.

As a consequence of this observation, we propose to use homogeneous functions that are invariant under det-1 symmetric ILOs to quantify entanglement in the symmetric subspace of SLOCC classes. To build a function that would relate the distribution of the Majorana points of a symmetric state to its entanglement quantity, we first study geometric properties of the Majorana representation.

5.2 Geometric properties of the Majorana representation

The Majorana representation of symmetric N-qubit states exploits the permutation invariance of these states to represent them as collections of N points on the Bloch sphere. We had already introduced this representation in Section 1.2.3 but we review it briefly here as, to simplify upcoming developments, we adopt in this chapter a specific normalization convention for the Majorana representation.

In the Majorana representation, an N-qubit symmetric state is represented as the superposition of the states corresponding to all possible permutations of the single qubit states of an N-qubit product state. Indeed, given an N-qubit symmetric state $|\psi_S\rangle$, there

always exist single qubit states $|\epsilon'_1\rangle, \ldots, |\epsilon'_N\rangle$ such that

$$|\psi_S\rangle = \frac{1}{\mathcal{N}} \sum_{\pi \in S_N} |\epsilon'_{\pi(1)}, \ldots, \epsilon'_{\pi(N)}\rangle, \tag{5.2}$$

where S_N is the group of permutations of N elements and $\mathcal{N}$ is a normalization factor. Several conventions exist for this normalization factor, depending on the norm of the single qubit states $|\epsilon'_i\rangle$ $(i = 1, \ldots, N)$. To get an unambiguous parametrization that moreover respects the permutation invariance, these single qubit states must all have the same norm, but this norm does not necessarily have to be 1. We choose here to work with the convention in which the parameter $\mathcal{N}$ corresponds to the norm of the superposition of all the permutations of the tensor product of the normalized single qubit states, i.e.

$$\mathcal{N} = \sqrt{\left(\sum_{\pi \in S_N} \frac{\langle \epsilon'_{\pi(1)}|}{||\epsilon'_{\pi(1)}||} \otimes \cdots \otimes \frac{\langle \epsilon'_{\pi(N)}|}{||\epsilon'_{\pi(N)}||} \right) \left(\sum_{\pi' \in S_N} \frac{|\epsilon'_{\pi'(1)}\rangle}{||\epsilon'_{\pi'(1)}||} \otimes \cdots \otimes \frac{|\epsilon'_{\pi'(N)}\rangle}{||\epsilon'_{\pi'(N)}||} \right)}. \tag{5.3}$$

The norm of $|\psi_S\rangle$ is then stored into the single qubit states $|\epsilon'_i\rangle$, yielding the following parametrization:

$$|\psi_S\rangle = \frac{1}{\mathcal{N}} \sum_{\pi \in S_N} |\epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}\rangle, \tag{5.4}$$

with

$$|\epsilon_i\rangle = \frac{|\epsilon'_i\rangle}{||\epsilon'_i||} ||\psi_S||^{1/N}. \tag{5.5}$$

In this parametrization, if the state $|\psi_S\rangle$ is normalized (which is usually the case), all the states $|\epsilon_i\rangle$ $(i = 1, \ldots, N)$ are normalized as well. Each normalized single qubit state $|\epsilon_i\rangle$ can (up to a global phase) always be written

$$|\epsilon_i\rangle = \cos(\theta_i/2)\, |0\rangle + \sin(\theta_i/2)\, e^{i\,\phi_i}\, |1\rangle, \tag{5.6}$$

with $\theta_i \in [0, \pi]$ and $\phi_i \in [0, 2\pi[$. Using those angles, we can equivalently represent the state $|\psi_S\rangle$ as a collection of N points (called Majorana points) on the Bloch sphere.

5.2.1 Distance between Majorana points on the Bloch sphere

Given two single qubit states $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$, let us first characterize the (great-circle) distance $\Delta\sigma$ between the points representing them on the Bloch sphere (see Fig. 5.1).

The Bloch sphere having a radius equal to 1, the great-circle distance between two points on the sphere is equal to the central angle between them. This central angle can be expressed as a function of the spherical coordinates of the two points using the haversine formula of spherical trigonometry. Using our conventions of Bloch sphere coordinates (as

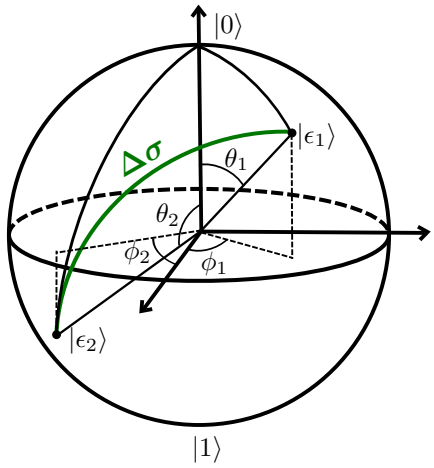


Figure 5.1: Representation of the great-circle distance $\Delta\sigma$ on the Bloch sphere between two points with Bloch sphere coordinates (θ_1, ϕ_1) and (θ_2, ϕ_2), corresponding to the states $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$, respectively.

shown in Fig. 5.1), this yields:

$$\Delta\sigma = 2\arcsin\sqrt{\sin^2\left(\frac{\theta_2-\theta_1}{2}\right) + \sin\theta_1\sin\theta_2\sin^2\left(\frac{\phi_2-\phi_1}{2}\right)}. \tag{5.7}$$

Using trigonometric identities, this formula is easily shown to be equivalent to

$$\Delta\sigma = 2\arcsin\left|\cos\left(\frac{\theta_1}{2}\right)\sin\left(\frac{\theta_2}{2}\right)e^{i\phi_2} - \cos\left(\frac{\theta_2}{2}\right)\sin\left(\frac{\theta_1}{2}\right)e^{i\phi_1}\right|. \tag{5.8}$$

In this second formulation, we can directly identify the computational basis components of $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$, expressed in the Bloch representation (5.6). Renaming these as

$$|\epsilon_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \text{ and } |\epsilon_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle, \tag{5.9}$$

we simply get

$$\Delta\sigma = 2\arcsin|\alpha_1\beta_2 - \alpha_2\beta_1|. \tag{5.10}$$

Instead of the great-circle distance, we can also consider the Euclidean distance to quantify the separation between two points on the Bloch sphere. The Euclidean distance between the points representing the states $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ on the Bloch sphere, that we denote by $d(|\epsilon_1\rangle, |\epsilon_2\rangle)$, is given by the chord length of the central angle $\Delta\sigma$. We thus have

$$d(|\epsilon_1\rangle, |\epsilon_2\rangle) = 2\sin\left(\frac{\Delta\sigma}{2}\right) = 2|\alpha_1\beta_2 - \alpha_2\beta_1|. \tag{5.11}$$

Whereas the great-circle distance $\Delta\sigma$ ranges from 0 (when $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ are identical) to π (when $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ correspond to antipodal points on the Bloch sphere), the Euclidean distance d ranges from 0 to 2. This function can also be expressed as twice the modulus of the overlap between $|\epsilon_1\rangle$ and $|\epsilon_2^\perp\rangle$, a state that is orthogonal to $|\epsilon_2\rangle$:

$$d(|\epsilon_1\rangle, |\epsilon_2\rangle) = 2\left|\langle\epsilon_2^\perp|\epsilon_1\rangle\right|. \tag{5.12}$$

This shows in particular that orthogonal states are always represented by antipodal points on the Bloch sphere. In the following section, we use these geometrical tools to quantify the entanglement of symmetric multiqubit states through the distribution of their Majorana points.

5.3 Entanglement quantification upon Majorana points distribution

In the symmetric subspace of any SLOCC class $\mathcal{C}$ containing symmetric states with only nondegenerated Majorana points on the Bloch sphere, we propose the function

$$\tau_{\mathcal{C}}(|\psi_S\rangle) = \frac{\delta_{\mathcal{C}}}{\mathcal{N}} \prod_{1\leq i<j\leq N} d(|\epsilon_i\rangle, |\epsilon_j\rangle)^{\frac{1}{N-1}}, \tag{5.13}$$

where $\delta_{\mathcal{C}}$ is a (strictly positive) normalization constant, to quantify the entanglement of any symmetric state $|\psi_S\rangle \in \mathcal{C}$ with Majorana representation

$$|\psi_S\rangle = \frac{1}{\mathcal{N}} \sum_{\pi\in S_N} |\epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}\rangle. \tag{5.14}$$

We now show that this function satisfies the hypotheses of Observation 5.1. This function is obviously positive, and it is nonzero for all symmetric states that have only nondegenerated Majorana points on the Bloch sphere. It is also homogeneous. Indeed, for any $\lambda > 0$, the state $\lambda|\psi_S\rangle$ has a Majorana representation with the same norm parameter as $|\psi_S\rangle$ and single qubit states $|\epsilon_i'\rangle$ reading $|\epsilon_i'\rangle = \lambda^{\frac{1}{N}}|\epsilon_i\rangle$ for all $i = 1, \ldots, N$. Since $d(\lambda^{\frac{1}{N}}|\epsilon_i\rangle, \lambda^{\frac{1}{N}}|\epsilon_j\rangle) = \lambda^{\frac{2}{N}} d(|\epsilon_i\rangle, |\epsilon_j\rangle)$, we have $\tau_{\mathcal{C}}(\lambda|\psi_S\rangle) = \lambda\,\tau_{\mathcal{C}}(|\psi_S\rangle)$, meaning that $\tau_{\mathcal{C}}$ is an homogeneous function of degree 1. There remains to be shown that $\tau_{\mathcal{C}}$ is invariant under any det-1 symmetric ILO. Let A be a det-1 operator. We have

$$A^{\otimes N}|\psi_S\rangle = \frac{1}{\mathcal{N}} \sum_{\pi\in S_N} A|\epsilon_{\pi(1)}\rangle \otimes \cdots \otimes A|\epsilon_{\pi(N)}\rangle. \tag{5.15}$$

Since the ILO $A^{\otimes N}$ does not necessarily preserve the norm of $|\psi_S\rangle$, the right-hand side of Eq. (5.15) does however not necessarily respect our normalization convention for the Majorana representation of $A^{\otimes N}|\psi_S\rangle$. According to this convention, the actual Majorana

representation of this state reads instead

$$A^{\otimes N}|\psi_S\rangle = \frac{1}{\mathcal{N}'}\sum_{\pi\in S_N}\frac{A|\epsilon_{\pi(1)}\rangle}{||A|\epsilon_{\pi(1)}\rangle||}||A^{\otimes N}|\psi_S\rangle||^{1/N}\otimes\cdots\otimes\frac{A|\epsilon_{\pi(N)}\rangle}{||A|\epsilon_{\pi(N)}\rangle||}||A^{\otimes N}|\psi_S\rangle||^{1/N} \tag{5.16}$$

with

$$\mathcal{N}' = \sqrt{\left(\sum_{\pi\in S_N}\frac{\langle\epsilon_{\pi(1)}|A^\dagger}{||A|\epsilon_{\pi(1)}\rangle||}\otimes\cdots\otimes\frac{\langle\epsilon_{\pi(N)}|A^\dagger}{||A|\epsilon_{\pi(N)}\rangle||}\right)\left(\sum_{\pi'\in S_N}\frac{A|\epsilon_{\pi'(1)}\rangle}{||A|\epsilon_{\pi'(1)}\rangle||}\otimes\cdots\otimes\frac{A|\epsilon_{\pi'(N)}\rangle}{||A|\epsilon_{\pi'(N)}\rangle||}\right)} \tag{5.17}$$

and

$$||A^{\otimes N}|\psi_S\rangle|| = \frac{\mathcal{N}'\prod_{i=1}^N||A|\epsilon_i\rangle||}{\mathcal{N}}. \tag{5.18}$$

From Eq. (5.11), which expresses the distance $d(|\epsilon_i\rangle,|\epsilon_j\rangle)$ in terms of the computational basis components of $|\epsilon_i\rangle$ and $|\epsilon_j\rangle$, we find $d(A|\epsilon_i\rangle,A|\epsilon_j\rangle) = |\det(A)|\,d(|\epsilon_i\rangle,|\epsilon_j\rangle)$. As A is a det-1 operation, we have

$$\tau_{\mathcal{C}}(A^{\otimes N}|\psi_S\rangle) = \frac{\delta_{\mathcal{C}}}{\mathcal{N}'}\prod_{1\le i<j\le N} d\left(\frac{||A^{\otimes N}|\psi_S\rangle||^{1/N}}{||A|\epsilon_i\rangle||}A|\epsilon_i\rangle,\frac{||A^{\otimes N}|\psi_S\rangle||^{1/N}}{||A|\epsilon_j\rangle||}A|\epsilon_j\rangle\right)^{\frac{1}{N-1}} \tag{5.19}$$

$$= \frac{\delta_{\mathcal{C}}}{\mathcal{N}'}\prod_{1\le i<j\le N}\left(\frac{||A^{\otimes N}|\psi_S\rangle||^{2/N}}{||A|\epsilon_i\rangle||\,||A|\epsilon_j\rangle||}\right)^{\frac{1}{N-1}} d(A|\epsilon_i\rangle,A|\epsilon_j\rangle)^{\frac{1}{N-1}} \tag{5.20}$$

$$= \frac{\delta_{\mathcal{C}}||A^{\otimes N}|\psi_S\rangle||}{\mathcal{N}'\prod_{k=1}^N||A|\epsilon_k\rangle||}\prod_{1\le i<j\le N} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^{\frac{1}{N-1}} \tag{5.21}$$

$$= \tau_{\mathcal{C}}(|\psi_S\rangle). \tag{5.22}$$

This finally proves that $\tau_{\mathcal{C}}$ does effectively satisfy the hypotheses of Observation 5.1. By definition, $\tau_{\mathcal{C}}$ can only be used to quantify entanglement in SLOCC classes containing symmetric states with only nondegenerated Majorana points on the Bloch sphere, i.e. in the SLOCC classes of the entanglement family $\mathcal{D}_{1,\ldots,1}$ of Ref. [25]. Fortunately, this family contains all generic symmetric states and, in systems of at least 4 qubits, it includes an infinite number of SLOCC classes [25], in which we can nontrivially quantify entanglement.

In the entanglement quantification function $\tau_{\mathcal{C}}$, the term involving the product of the Euclidean distances between all pairs of Majorana points is obviously larger for symmetric states that have highly scattered Majorana points on the Bloch sphere. By contrast, the influence of the Majorana points configuration on the norm parameter $\mathcal{N}$ is not so evident. We figure out how to express it as a function of the distances between the Majorana points in the next section.

5.3.1 Geometric interpretation of the norm parameter

Following our convention, the norm parameter defined in Eq. (5.3) corresponds to the norm of a superposition of tensor products of normalized single qubit states. In the following, we drop the normalization factor of the single qubit states to simplify the notations. The norm parameter $\mathcal{N}$ is then given by

$$\mathcal{N} = \sqrt{\left(\sum_{\pi\in S_N} \langle \epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}|\right)\left(\sum_{\pi'\in S_N} |\epsilon_{\pi'(1)}, \ldots, \epsilon_{\pi'(N)}\rangle\right)} \tag{5.23}$$

$$= \sqrt{\sum_{\pi\in S_N}\sum_{\pi'\in S_N}\Big(\langle \epsilon_1, \ldots, \epsilon_N|\Big)\Big(|\epsilon_{\pi\circ\pi'(1)}, \ldots, \epsilon_{\pi\circ\pi'(N)}\rangle\Big)}, \tag{5.24}$$

where $\pi \circ \pi'$ denotes the composition of the permutations π and π'. Since the action of any permutation on its permutation group gives the group itself, the first sum gives the same result for all permutations $\pi \in S_N$ and we have

$$\mathcal{N} = \sqrt{N! \sum_{\pi'\in S_N}\Big(\langle \epsilon_1, \ldots, \epsilon_N|\Big)\Big(|\epsilon_{\pi'(1)}, \ldots, \epsilon_{\pi'(N)}\rangle\Big)}. \tag{5.25}$$

To get intuition on how to express this equation as a function of the distance between the Majorana points, we consider explicitly the cases of symmetric states of 2 to 4 qubits. We then extrapolate the general case.

Case of 2 qubits

We begin with the simplest case: $N = 2$. Throughout these explicit computations of the norm parameter $\mathcal{N}$ (to which we add a subscript specifying the number of qubits it corresponds to), we use cycle notations for the elements of the symmetric group S_N and omit cycles of length 1 for simplicity. In this case, we have

$$\mathcal{N}_2 = \sqrt{2!\left(\langle \epsilon_1, \epsilon_2|\ \Big(\mathbb{1} + (12)\Big)|\epsilon_1, \epsilon_2\rangle\right)} \tag{5.26}$$

$$= \sqrt{2\left(1 + |\langle \epsilon_2|\epsilon_1\rangle|^2\right)} \tag{5.27}$$

Let $|\epsilon_2^\perp\rangle$ denote a state orthonormal to $|\epsilon_2\rangle$. In the orthonormal basis $\{|\epsilon_2\rangle, |\epsilon_2^\perp\rangle\}$, we have, for any normalized state $|\epsilon_1\rangle$,

$$|\langle \epsilon_2|\epsilon_1\rangle|^2 + |\langle \epsilon_2^\perp|\epsilon_1\rangle|^2 = 1. \tag{5.28}$$

As shown in Eq. (5.12), the second term of the sum is nothing but $d(|\epsilon_1\rangle, |\epsilon_2\rangle)^2/4$. Inserting this identity into Eq. (5.27) gives

$$\mathcal{N}_2 = \sqrt{2}\sqrt{2 - \frac{1}{4}d(|\epsilon_1\rangle, |\epsilon_2\rangle)^2}. \tag{5.29}$$

Case of 3 qubits

For a 3-qubit symmetric state, the norm parameter $\mathcal{N}_3$ contains 6 permutations:

$$\mathcal{N}_3 = \sqrt{3!\left(\langle\epsilon_1, \epsilon_2, \epsilon_3|\ \Big(\mathbb{1} + (12) + (23) + (13) + (123) + (132)\Big)|\epsilon_1, \epsilon_2, \epsilon_3\rangle\right)}. \tag{5.30}$$

From the $N = 2$ case, we can deduce the result for the cycles of length 2:

$$\langle\epsilon_1, \epsilon_2, \epsilon_3|(ij)|\epsilon_1, \epsilon_2, \epsilon_3\rangle = 1 - \frac{1}{4}d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2, \quad \forall\, i, j \in \{1, 2, 3\},\ i \neq j. \tag{5.31}$$

For the last two terms, we have

$$\langle\epsilon_1, \epsilon_2, \epsilon_3|\Big((123) + (132)\Big)|\epsilon_1, \epsilon_2, \epsilon_3\rangle = 2\,\Re(\langle\epsilon_1|\epsilon_2\rangle\langle\epsilon_2|\epsilon_3\rangle\langle\epsilon_3|\epsilon_1\rangle), \tag{5.32}$$

where $\Re(c)$ denotes the real part of the complex number c. This part of the norm factor involving a product of three scalar products is more difficult to express as a function of Euclidean distances. When expressing each single qubit state $|\epsilon_i\rangle$ $(i = 1, 2, 3)$ into the Bloch parametrization (5.6), the explicit computation of the scalar products yields

$$2\,\Re(\langle\epsilon_1|\epsilon_2\rangle\langle\epsilon_2|\epsilon_3\rangle\langle\epsilon_3|\epsilon_1\rangle) = \frac{1}{2}\Big(1 + \sum_{1\leq i<j\leq 3} \cos\theta_i \cos\theta_j + \sin\theta_i \sin\theta_j \cos(\phi_i - \phi_j)\Big). \tag{5.33}$$

The great-circle distance $\Delta\sigma_{ij}$ between the points representing the states $|\epsilon_i\rangle$ and $|\epsilon_j\rangle$ on the Bloch sphere appears explicitly in this last formula from the spherical law of cosines. When applied to the spherical triangle formed by the points representing the states $|\epsilon_i\rangle$ and $|\epsilon_j\rangle$ on the Bloch sphere and an auxiliary point on either the north or the south pole of the Bloch sphere, the spherical law of cosines gives indeed

$$\Delta\sigma_{ij} = \arccos\Big(\cos\theta_i \cos\theta_j + \sin\theta_i \sin\theta_j \cos(\phi_i - \phi_j)\Big). \tag{5.34}$$

Combining this formula with the trigonometric identity $\cos\alpha = 1 - 2\sin^2(\alpha/2)$, we get

$$2\,\Re(\langle\epsilon_1|\epsilon_2\rangle\langle\epsilon_2|\epsilon_3\rangle\langle\epsilon_3|\epsilon_1\rangle) = 2 - \frac{1}{4}\sum_{1\leq i<j\leq 3} d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2. \tag{5.35}$$

Gathering the terms corresponding to all the permutations yields finally

$$\mathcal{N}_3 = \sqrt{3!}\sqrt{6 - \frac{1}{2}\sum_{1\leq i<j\leq 3} d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2}. \tag{5.36}$$

Case of 4 qubits

For a 4-qubit symmetric state, we have 24 permutations to consider in the norm factor $\mathcal{N}_4$. The terms with cycles of length up to 3 can be deduced from the previous cases, so that we only have to analyze the cycles of length 4 and the compositions of disjoint *transpositions* (i.e. cycles of length 2). As the length of the cycle increases, an explicit computation like in Eq. (5.33) becomes harder to perform. For this reason, we present now another approach, based on the matrix representation of the permutation operators. In this approach, we consider the sum over all permutations as a single operator and try to express its action onto the product state $|\epsilon_1, \ldots, \epsilon_N\rangle$ as a sum of compositions of disjoint transpositions.

Let us denote by Σ the matrix corresponding to the sum of all the matrices representing permutations of N qubits in the N-qubit computational basis. This matrix can obviously only couple states of the computational basis with the same number of excitations (i.e. the same number of qubits in the state $|1\rangle$). Since the action of S_N on itself is regular, all the computational basis states with k excitations have the same orbit under the action of the group. This imply that rows of Σ associated to computational basis states with a given number k of excitations are all equal to each other. Since the matrices representing permutations are orthogonal, the matrix Σ must in addition be symmetric (in the sense $\Sigma = \Sigma^T$). This can easily be seen by grouping each permutation with its inverse in the sum constituting Σ. As a consequence, the columns of Σ associated to computational basis states with a given number k of excitations must also be equal to each other, so that all the elements in these rows and columns have the same value. This value is simply given by the total number of permutations, divided by the number of computational states with k excitations. We thus have

$$(\Sigma)_{ij} = \frac{N!}{\binom{N}{E(i-1)}}\delta_{E(i-1),E(j-1)}, \tag{5.37}$$

where $\delta_{a,b}$ is the Kronecker symbol between a and b and $E(n)$ gives the number of digits 1 in the binary representation of the natural number n.

Given a computational basis state with k excitations, any permutation on its qubits can equivalently be realized by the composition of up to $\min(k, N-k)$ transpositions over disjoint couples of qubits. We thus want to decompose the matrix Σ as a sum of permutations corresponding to the composition of up to $\lfloor N/2 \rfloor$ disjoint transpositions. As Σ contains all the permutations, we expect all the compositions of k disjoint transpositions to have the same weight in the sum, for all $k = 1, \ldots, \lfloor N/2 \rfloor$. Denoting by Σ_k the matrix corresponding to the sum of the matrices representing, in the computational basis, all

the compositions of k disjoint transpositions of the qubits, such a decomposition of Σ is possible if there exist integer numbers $x_0, x_1, \ldots, x_{\lfloor N/2 \rfloor}$ such that

$$\Sigma = x_0 \mathbb{1} + x_1 \Sigma_1 + \cdots + x_{\lfloor N/2 \rfloor} \Sigma_{\lfloor N/2 \rfloor}. \tag{5.38}$$

We now search for such a decomposition in the case $N = 4$. To see if the matrix equation (5.38) admits a solution, we decompose it into blocks of rows and columns corresponding to computational basis states with the same number of excitations. In each block, all the rows and columns are thus identical. We arbitrarily choose one row, corresponding to a particular computational basis state, and decompose, as in Eq. (5.38), all the permutations of the qubits of this state into three components corresponding to $\mathbb{1}$, Σ_1 and Σ_2. By solving the corresponding equation, we get the values of the coefficients x_0, x_1 and x_2 of Eq. (5.38), for the corresponding block. We then check whether the coefficients corresponding to the decompositions of the other blocks are identical, in which case we have the confirmation that the matrix decomposition of Eq. (5.38) is possible. The block corresponding to computational basis states with k excitations being identical to the block corresponding to computational basis states with $N - k$ excitations, we only consider the blocks associated to computational basis states with at most 2 excitations. We begin with the block corresponding to computational basis states with 2 excitations.

Given a computational basis state with 2 excitations, such as the state $|0011\rangle$, we can distinguish, in the corresponding row of Σ, 3 classes of computational basis states this state can be transformed into by permutation. A permutation can indeed either leave the state unchanged, induce one swap between excited and non-excited states or induce two swaps between the excited and non-excited states. For the different components of the decomposition (5.38), we have:

- The 3 compositions of disjoint transpositions transform the state $|0011\rangle$ once into itself and twice into the state $|1100\rangle$, i.e. the only state with 2 swaps.
- The 6 transpositions transform the state $|0011\rangle$ twice into itself, and once into the states $|1001\rangle$, $|1010\rangle$, $|0101\rangle$ and $|0110\rangle$, i.e. once into each state with 1 swap.
- The identity naturally transforms the state $|0011\rangle$ into itself.

In the left hand-side of Eq. (5.38), all the nonzero elements of Σ corresponding to this row must be identical and equal to $4!/\binom{4}{2} = 4$. For the different states of this row, the Equation (5.38) can thus be put into the linear system

$$\begin{array}{c} \\ \text{2 swaps} \\ \text{1 swap} \\ \text{0 swap} \end{array} \begin{array}{c} \begin{array}{ccc} \mathbb{1} & \Sigma_1 & \Sigma_2 \end{array} \\ \begin{pmatrix} 0 & 0 & 2 \\ 0 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \end{array} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \\ 4 \end{pmatrix}. \tag{5.39}$$

This system admits the solution $x_0 = -6, x_1 = 4$ and $x_2 = 2$. We must now verify that this solution also holds for the other rows and columns of Σ. For the rows and

columns corresponding to computational basis states with 1 excitation, such as the state $|0001\rangle$, the permutations cannot correspond to 2 swaps. They can only correspond to 1 or 0 swap, giving the following system:

$$\begin{array}{c} \\ \text{1 swap} \\ \text{0 swap} \end{array} \begin{array}{c} \begin{array}{ccc} \mathbb{1} & \Sigma_1 & \Sigma_2 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 3 & 0 \end{pmatrix} \end{array} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 6 \\ 6 \end{pmatrix}. \tag{5.40}$$

We check easily that the solution of the previous system is compatible with this one. Finally, we have to consider states with 0 excitation. There is only one such state, namely $|0000\rangle$. Any permutation of its qubits leaves it unchanged. The Equation (5.38) for the corresponding row simply reads

$$\begin{array}{c} \\ \text{0 swap} \end{array} \begin{array}{c} \begin{array}{ccc} \mathbb{1} & \Sigma_1 & \Sigma_2 \end{array} \\ \begin{pmatrix} 1 & 6 & 3 \end{pmatrix} \end{array} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 24. \tag{5.41}$$

The solution $x_0 = -6, x_1 = 4$ and $x_2 = 2$ being also solution of this system, we can conclude that the matrix Σ can indeed be decomposed into the identity, transpositions and compositions of two disjoint transpositions as

$$\Sigma = -6\,\mathbb{1} + 4\,\Sigma_1 + 2\,\Sigma_2. \tag{5.42}$$

This allows a simple computation of the norm factor:

$$\mathcal{N}_4 = \sqrt{4!\Big(-6 + 4\sum_{\{i,j\}\subset\mathcal{S}_4} |\langle\epsilon_i|\epsilon_j\rangle|^2 + 2\sum_{\text{disjoint pairs } \{i,j\},\{k,l\}\subset\mathcal{S}_4} |\langle\epsilon_i|\epsilon_j\rangle|^2|\langle\epsilon_k|\epsilon_l\rangle|^2\Big)}, \tag{5.43}$$

with $\mathcal{S}_4$ the set $\{1,2,3,4\}$ containing the 4 qubits. Replacing the squared overlaps using the identity $|\langle\epsilon_i|\epsilon_j\rangle|^2 = 1 - \frac{1}{4}d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2$, we finally obtain the norm parameter

$$\mathcal{N}_4 = \sqrt{4!}\sqrt{24 - \frac{3}{2}\sum_{\{i,j\}\subset\mathcal{S}_4} d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2 + \frac{1}{8}\sum_{\substack{\text{disjoint pairs} \\ \{i,j\},\{k,l\} \text{ in } \mathcal{S}_4}} d(|\epsilon_i\rangle, |\epsilon_j\rangle)^2\, d(|\epsilon_k\rangle, |\epsilon_l\rangle)^2}. \tag{5.44}$$

General case

Following a development similar to the one detailed in the previous section, we can try to find, in systems of $N > 4$ qubits, a decomposition of the matrix $\Sigma^{(N)}$ into the identity and $\Sigma_k^{(N)}$ matrices, for $k = 1, \ldots, \lfloor N/2 \rfloor$ (for clarity, we add a superscript to the matrices Σ, $\mathbb{1}$ and Σ_k, to specify the number of qubits they correspond to). For instance,

for systems of 5 to 7 qubits, such a decomposition can indeed be found and we have

$$\Sigma^{(5)} = -30\,\mathbb{1}^{(5)} + 6\,\Sigma_1^{(5)} + 6\,\Sigma_2^{(5)}, \tag{5.45}$$

$$\Sigma^{(6)} = -90\,\mathbb{1}^{(6)} - 6\,\Sigma_1^{(6)} + 18\,\Sigma_2^{(6)} + 6\,\Sigma_3^{(6)}, \tag{5.46}$$

$$\Sigma^{(7)} = -120\,\Sigma_1^{(7)} + 48\,\Sigma_2^{(7)} + 24\,\Sigma_3^{(7)}. \tag{5.47}$$

This allows a simple computation of the corresponding norm factors:

$$\mathcal{N}_5 = \sqrt{5!}\sqrt{120 - 6\sum_{\{i,j\}\subset\mathcal{S}_5} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 + \frac{3}{8}\sum_{\substack{\text{disjoint pairs}\\ \{i,j\},\{k,l\}\subset\mathcal{S}_5}} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2\, d(|\epsilon_k\rangle,|\epsilon_l\rangle)^2}, \tag{5.48}$$

$$\mathcal{N}_6 = \sqrt{6!}\left(720 - 30\sum_{\{i,j\}\subset\mathcal{S}_6} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 + \frac{3}{2}\sum_{\substack{\text{disjoint pairs}\\ \{i,j\},\{k,l\}\subset\mathcal{S}_6}} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 d(|\epsilon_k\rangle,|\epsilon_l\rangle)^2 - \frac{3}{32}\sum_{\substack{\text{disjoint pairs}\\ \{i,j\},\{k,l\},\{m,n\}\subset\mathcal{S}_6}} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 d(|\epsilon_k\rangle,|\epsilon_l\rangle)^2 d(|\epsilon_m\rangle,|\epsilon_n\rangle)^2\right)^{1/2}, \tag{5.49}$$

$$\mathcal{N}_7 = \sqrt{7!}\left(5040 - 180\sum_{\{i,j\}\subset\mathcal{S}_7} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 + \frac{15}{2}\sum_{\substack{\text{disjoint pairs}\\ \{i,j\},\{k,l\}\subset\mathcal{S}_7}} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 d(|\epsilon_k\rangle,|\epsilon_l\rangle)^2 - \frac{3}{8}\sum_{\substack{\text{disjoint pairs}\\ \{i,j\},\{k,l\},\{m,n\}\subset\mathcal{S}_7}} d(|\epsilon_i\rangle,|\epsilon_j\rangle)^2 d(|\epsilon_k\rangle,|\epsilon_l\rangle)^2 d(|\epsilon_m\rangle,|\epsilon_n\rangle)^2\right)^{1/2}, \tag{5.50}$$

where $\mathcal{S}_N$ $(N = 5, 6, 7)$ denotes the set made of the N qubits. Extrapolating these expressions to an arbitrary number of qubits, we conjecture that the decomposition (5.38) can be performed for any number N of qubits, yielding the norm factor

$$\mathcal{N}_N = \sqrt{N!}\sqrt{N! + \sum_{k=1}^{\lfloor N/2\rfloor}\left(\frac{-1}{4}\right)^k (N-k)! \sum_{\substack{k\text{ disjoint pairs}\\ \{i_1,i_2\},\ldots,\{i_{2k-1},i_{2k}\}\subset\mathcal{S}_N}} d(|\epsilon_{i_1}\rangle,|\epsilon_{i_2}\rangle)^2 \ldots d(|\epsilon_{i_{2k-1}}\rangle,|\epsilon_{i_{2k}}\rangle)^2}. \tag{5.51}$$

We checked this formula numerically, up to $N = 12$. This gives strong indications that the entanglement quantification function $\tau_{\mathcal{C}}$ only depends on the Euclidean distances between the Majorana points of symmetric states.

The maximization of $\tau_{\mathcal{C}}$ requires to minimize the norm parameter $\mathcal{N}$. Due to the factorial term in front of the sum in formula (5.51), the minimization of the norm pa-

rameter requires a large value of the (negative) term corresponding to $k = 1$ in the sum. Indeed, a low value for this term implies a low value for the other terms, so that there is nothing to balance the $N!$ term. The term $k = 1$ of the sum corresponds to the sum of the Euclidean distances between all pairs of Majorana points. In the numerator of $\tau_{\mathcal{C}}$ we have the product of all these distances. The inequality between the arithmetic mean and the geometric mean suggests then that, in order to maximize both terms (and thus maximize $\tau_{\mathcal{C}}$), the points should be homogeneously distributed on the sphere.

This intuition is in accordance with the observation, made in Refs. [82, 83], that symmetric states corresponding to large values of the geometric measure of entanglement have highly scattered Majorana points on the Bloch sphere. This can also be checked numerically. We show in the next section how to efficiently compute the entanglement quantification function $\tau_{\mathcal{C}}$.

5.3.2 Numerical computation of the norm parameter

Although it is useful to understand how the entanglement quantification function $\tau_{\mathcal{C}}$ quantifies the entanglement of a symmetric state through its Majorana point configuration, the general formula (5.51) is not the most efficient way to numerically compute the norm parameter $\mathcal{N}$ of the Majorana representation of a symmetric state $|\psi_S\rangle$. This is due to the sums over all possible disjoint transpositions among the N qubits. Although these sums contain less terms than in the general formula (5.25), where one had to consider all the possible permutations of the N qubits, they still become difficult to evaluate when the number of qubits increases. As we show here, the computation of all these sums can be circumvented by using the equivalence between the Majorana and Dicke representations of symmetric states (which we had already introduced in Section 1.2.3).

Let us consider an N-qubit symmetric state $|\psi_S\rangle$ with Majorana representation

$$|\psi_S\rangle = \frac{1}{\mathcal{N}} \sum_{\pi \in S_N} |\epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}\rangle, \tag{5.52}$$

where

$$|\epsilon_i\rangle = \cos(\theta_i/2)\, |0\rangle + \sin(\theta_i/2)\, e^{i\,\phi_i}\, |1\rangle, \tag{5.53}$$

with $\theta_i \in [0, \pi]$ and $\phi_i \in [0, 2\pi[$ for all $i = 1, \ldots, N$. We choose here to order the single qubit states $|\epsilon_i\rangle$ $(i = 1, \ldots, N)$ in descending order of the associated angles θ_i and denote by K $(0 \leq K \leq N)$ the number of angles θ_i satisfying $\theta_i \neq 0$. The coefficients d_k $(k = 0, \ldots, N)$ of the Dicke representation of $|\psi_S\rangle$ can be deduced from the polynomial [25]

$$P(z) = \sum_{k=0}^{K} (-1)^k \sqrt{\binom{N}{k}}\, d_k\, z^k, \tag{5.54}$$

which is a degree K polynomial whose complex roots $z_1, \ldots, z_K$ are related to the angles characterizing the Majorana states (5.53) of $|\psi_S\rangle$ through the relation $z_i = \cot(\theta_i) e^{-i\,\phi_i}$

for all $i = 1, \ldots, K$. We thus have the identification

$$P(z) = \sum_{k=0}^{K} (-1)^k \sqrt{\binom{N}{k}}\, d_k\, z^k = \alpha \prod_{i=1}^{K} (z - z_i), \tag{5.55}$$

where α is a multiplicative constant that can be chosen to fix the norm of the state with Dicke coefficients d_k.

To compute the value of the norm parameter $\mathcal{N}$, we now adjust α to compute the Dicke representation of the state

$$|\psi'_S\rangle = \sum_{\pi \in S_N} |\epsilon_{\pi(1)}, \ldots, \epsilon_{\pi(N)}\rangle, \tag{5.56}$$

as the norm of this state is precisely equal to $\mathcal{N}$. To do so, we compare the components of $|\psi'_S\rangle$ and the state with Dicke coefficients d_k satisfying Eq. (5.55) on one particular computational basis state. Among all computational basis components, the one that is the easiest to identify is probably the first, i.e. the component on the computational basis state $|0 \cdots 0\rangle$. For the state $|\psi'_S\rangle$, this component is simply given by

$$\langle 0 \cdots 0 | \psi'_S \rangle = (N!) \prod_{i=1}^{N} \cos(\theta_i/2). \tag{5.57}$$

For the state with the Dicke components d_k of Eq. (5.55), since $|0 \cdots 0\rangle$ is nothing but the Dicke state $|D_N^{(0)}\rangle$, the component on the first computational basis state is simply d_0. From Eq. (5.55), we have

$$d_0 = (-1)^K \alpha \prod_{i=1}^{K} z_i. \tag{5.58}$$

Unless $\theta_1 = \pi$, in which case $z_1 = 0$ and Eqs. (5.57) and (5.58) both vanish, we can use these equations to compute α. Inserting the value of α into Eq. (5.55), we can then compute all the Dicke coefficient d_k, for $k = 0, \ldots, K$, and finally compute the norm parameter, which simply reads $\mathcal{N} = \sqrt{\sum_{k=0}^{K} |d_k|^2}$.

When $\theta_1 = \pi$, we could try to compare another computational basis component between the Dicke representation of $|\psi_S\rangle$ and the unnormalized Majorana representation of $|\psi'_S\rangle$ but we can also follow a more practical solution. It is indeed easier to apply a symmetric LU operation $U^{\otimes N}$, where U is a 2×2 unitary matrix, on the state $|\psi_S\rangle$, so as to make sure that the Majorana states of the resulting state $U^{\otimes N}|\psi_S\rangle$ are all different from the state $|1\rangle$. Such a symmetric LU operation induces a rigid rotation of the N Majorana points representing the state $|\psi_S\rangle$ on the Bloch sphere [85] and a random unitary operation U is generically sufficient to obtain a state $U^{\otimes N}|\psi_S\rangle$ without Majorana state $|1\rangle$. Since an LU operation does not change the norm parameter $\mathcal{N}$ of the Majorana representation of a symmetric state, this parameter can be computed using the state $U^{\otimes N}|\psi_S\rangle$ instead of $|\psi_S\rangle$ in the previous development. We have this time the guarantee that the

state $U^{\otimes N}|\psi_S\rangle$ has a nonzero component on the computational basis state $|0\cdots0\rangle$, so that $\mathcal{N}$ can effectively be computed from this component. This potential LU transformation, that we presented, for explanatory purposes, as a solution to an issue that could occur in a first execution of the procedure can naturally be implemented at the beginning of the procedure, to prevent any failure of the computation of α. In any case, this method provides a fast and efficient way to compute the norm parameter $\mathcal{N}$ of any symmetric multiqubit state.

In the next section, we consider the problem of finding Majorana points configurations optimizing the entanglement quantification function $\tau_{\mathcal{C}}$.

5.3.3 Majorana points configuration with maximal entanglement

The entanglement quantification function $\tau_{\mathcal{C}}$ can be rescaled, so that its maximal value is 1, by computing, in each SLOCC class $\mathcal{C}$ of the family $\mathcal{D}_{1,\ldots,1}$, the normalization constant

$$\delta_{\mathcal{C}} = \left[\sup_{|\psi_S\rangle\in\mathcal{C}} \tau'_{\mathcal{C}}(\psi_S)\right]^{-1}, \tag{5.59}$$

where $\tau'_{\mathcal{C}}$ merely corresponds to $\tau_{\mathcal{C}}$ with $\delta_{\mathcal{C}} = 1$.

We show now that the optimization problem for $\tau'_{\mathcal{C}}$ can be rephrased into the well established framework (see for instance Ref. [86]) of the study of distributions of points on a sphere minimizing a certain potential energy. In 1904, J. J. Thompson considered the problem of finding the configuration of N electrons constrained on the surface of a sphere that minimizes their electrostatic potential energy [87]. Mathematically, Thompson's problem is equivalent to searching the N points $x_1, \ldots, x_N$ on the sphere S^2 minimizing the potential energy

$$E(x_1, \ldots, x_N) = \sum_{1\le i<j\le N} |x_i - x_j|^{-1}, \tag{5.60}$$

where $|x_i - x_j|$ denotes the Euclidean distance between the points x_i and x_j.

This problem was then generalized [86] to the minimization of the potential energy

$$E(s; x_1, \ldots, x_N) = \sum_{1\le i<j\le N} |x_i - x_j|^{-s}, \tag{5.61}$$

for arbitrary values of $s > 0$. In the limit $s \to \infty$, we recover the so-called Tammes problem [88], in which the minimal distance between all pairs of points has to be maximized. In the opposite limit $s \to 0$, one minimizes the logarithmic energy

$$E(0; x_1, \ldots, x_N) = -\sum_{1\le i<j\le N} \ln\left(|x_i - x_j|\right), \tag{5.62}$$

which is equivalent [89] to maximizing the product

$$\prod_{1\leq i<j\leq N} |x_i - x_j|. \tag{5.63}$$

Up to the norm factor $1/\mathcal{N}$ and the exponent (which has no influence on the maximization), this is precisely the problem we are concerned with. The potential energy that must be minimized in order to maximize the entanglement quantification function $\tau'_{\mathcal{C}}$ is thus

$$E'(0; x_1, \ldots, x_N) = -\sum_{1\leq i<j\leq N} \ln\left(\frac{|x_i - x_j|}{\mathcal{N}^{\frac{2}{N}}}\right)^{\frac{1}{(N-1)}}, \tag{5.64}$$

with the additional constraint that $x_1, \ldots, x_N$ correspond to Majorana points of a state of the SLOCC class $\mathcal{C}$. It has been established in Ref. [90] that an ILO between two SLOCC-equivalent symmetric states can be interpreted as a Moebius transformation on the roots of the polynomial P defined in Eq. (5.54), which are related to the Bloch sphere coordinates of the Majorana points. This provides a clue to implement the SLOCC equivalence constraint, but it further complicates the original problem. In fact, even without this additional constraint, the minimization of such potential energies on a sphere is a very challenging task. These functions are indeed known to have many saddle points, leading to many local minima [89]. Even though the entanglement quantification function $\tau_{\mathcal{C}}$ provides a simple way to quantify entanglement within SLOCC classes of symmetric states, it is, as many entanglement measures, difficult to maximize.

Chapter 6

Entanglement robustness against particle loss

The intensive research undertaken in the past decades to better characterize quantum entanglement revealed non only its theoretical complexity, but also its potential for innovative experimental protocols (see for example Ref. [26, 91] and references therein). The practical realization of theoretical protocols involving entangled states constitutes however a considerable challenge as it requires to solve experimental issues such as decoherence. In this context, the robustness of entanglement was introduced by Vidal and Tarrach [19], as a measure to quantify how resilient an entangled state is to the presence of local noise.

Entanglement robustness can also be defined with respect to particle loss [18]. In that case, an entangled multipartite state is said to be robust (or in contrast fragile) for the loss of a given subset of its particles if the reduced density operator corresponding to the remaining particles is an entangled (respectively separable) state. The Greenberger-Horne-Zeilinger [92] state of 3 qubits $|\mathrm{GHZ}_3\rangle \equiv 1/\sqrt{2}\,(|000\rangle + |111\rangle)$ is an emblematic example of fragile entangled state as, though highly entangled as a 3-qubit state, it loses all entanglement with the loss of any of its qubits [18]. By contrast, the so-called W state of 3 qubits $|\mathrm{W}_3\rangle \equiv 1/\sqrt{3}\,(|001\rangle + |010\rangle + |100\rangle)$, which captures the other type of genuine 3-qubit entanglement [18], has the highest robustness of entanglement against particle loss in the sense that the average entanglement of its 2-qubit reduced density operators reaches the highest value among all 3-qubit states [18]. This property of maximal bipartite entanglement (as measured by the mean concurrence of the 2-qubit reduced density operators) was quickly generalized to W states of an arbitrary number of qubits [93].

In Ref. [94], the relationship between robustness against particle loss and permutation symmetry was studied for specific 3-qubit pure states. Up to now, entanglement robustness and fragility properties have mainly been considered in the extreme case where all the particles but 2 are lost (see for example Refs. [95, 93, 96]). The reason for this is

that the concurrence can then be used as a true entanglement measure on the resulting 2-qubit reduced density operator.

In this chapter, we use different tools to investigate the entanglement robustness against particle loss, which enables us to consider a more general framework. In Section 6.1, we identify exhaustively all fragile multiqubit states for the loss of any single of their qubits. The extension of this result to multiqudit systems is considered in Section 6.2. In Section 6.3, we investigate the influence of permutation invariance on entanglement fragility. We show in particular that symmetric entangled states that are fragile for the loss of 1 qubit are all SLOCC-equivalent and belong the SLOCC class of the GHZ state. We also identify SLOCC classes containing only symmetric robust states.

Some of the results of this chapter have been published in Ref. [97]. To make them better fit in the construction of this chapter, some of the proofs we give here differ from the ones given in Ref.[97]. These proofs are naturally equivalent.

6.1 Fragility for the loss of 1 particle in multiqubit systems

The concepts of entanglement robustness and fragility against particle loss making only sense for N-particle systems of at least 3 particles, we always assume $N \geq 3$ in the following. In an N-particle system, an entangled pure state $|\psi\rangle$ is said to be fragile (resp. robust) against the loss of its particle k if $\rho_{\neg k} \equiv \mathrm{Tr}_k(|\psi\rangle\langle\psi|)$ is separable (resp. entangled).

We first prove a simple lemma showing the incompatibility between biseparability for the bipartition $k|1\cdots\not{k}\cdots N$ and fragility for the loss of the k-th qubit.

Lemma 6.1. *Let $|\psi\rangle$ be an N-qubit entangled pure state. If $|\psi\rangle$ is fragile for the loss of its k-th qubit, then $|\psi\rangle$ cannot be biseparable for the bipartition $k|1\cdots\not{k}\cdots N$.*

Proof. We prove this lemma by contradiction. Assuming that the state $|\psi\rangle$ is fragile for the loss of its k-th qubit, if it is in addition biseparable for the bipartition $k|1\cdots\not{k}\cdots N$, then $|\psi\rangle$ is necessarily fully separable. This is however impossible as it contradicts our hypothesis about the entanglement of $|\psi\rangle$. □

Even though we consider here the case in which only one qubit is lost, we can imagine several fragility scenarios. In the simplest scenario, the process leading to particle loss only affects one of the qubits, say qubit k. In this scenario, an entangled multiqubit state $|\psi\rangle$ is robust if it remains entangled after the loss of its qubit k. In another scenario, all the qubits are affected by the process inducing particle loss. In that case, the state $|\psi\rangle$ is robust if it remains entangled after the loss of any one of its qubits, i.e. if $\rho_{\neg i}$ is entangled for all $i = 1, \ldots, N$. In the most general scenario (which covers the previous ones), the process leading to particle loss affects all the qubits belonging to a given subset $\mathcal{A}$ of the qubits and $|\psi\rangle$ is robust if $\rho_{\neg i}$ is entangled for all $i \in \mathcal{A}$. We successively treat these 3 scenarios in the following sections.

6.1.1 Fragility for the loss of a given qubit

In this section, we study the conditions under which an entangled multiqubit state $|\psi\rangle$ is fragile for the loss of its k-th qubit. According to Lemma 6.1, such a fragile state cannot be biseparable for the bipartition $k|1\cdots\not{k}\cdots N$. As a consequence, the Schmidt number [91] of $|\psi\rangle$ for the bipartition $k|1\cdots\not{k}\cdots N$ must be strictly greater than 1. Since $|\psi\rangle$ is a multiqubit state, its Schmidt number for this bipartition cannot be greater than 2, and is thus precisely equal to 2. This implies that the reduced density operator $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$, which is separable since $|\psi\rangle$ is fragile for the loss of its k-th qubit, has a rank equal to 2. As a separable density operator of rank 2 has a length[1] equal to 2 [70], we can always write $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ as a convex sum of two distinct projectors onto product states:

$$\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right) = p_1\,|\mathbf{e}_{\neg k}\rangle\langle\mathbf{e}_{\neg k}| + p_2\,|\mathbf{e}'_{\neg k}\rangle\langle\mathbf{e}'_{\neg k}|, \tag{6.1}$$

with $p_1, p_2 > 0$ such that $p_1 + p_2 = 1$ and

$$|\mathbf{e}_{\neg k}\rangle = \bigotimes_{\substack{i=1\\ i\neq k}}^{N} |e_i\rangle \text{ and } |\mathbf{e}'_{\neg k}\rangle = \bigotimes_{\substack{i=1\\ i\neq k}}^{N} |e'_i\rangle, \tag{6.2}$$

where $|e_i\rangle$ and $|e'_i\rangle$ $(i \neq k)$ are normalized 1-qubit states such that $|\langle\mathbf{e}_{\neg k}|\mathbf{e}'_{\neg k}\rangle| < 1$.

Let λ_1 and λ_2 be the two nonzero eigenvalues of $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ and $|v_1\rangle, |v_2\rangle$ the associated eigenvectors. We denote by U the 2×2 unitary matrix connecting the separable decomposition (6.1) of $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ to its eigendecomposition [21]. This unitary satisfies

$$\begin{pmatrix} \sqrt{\lambda_1}\,|v_1\rangle \\ \sqrt{\lambda_2}\,|v_2\rangle \end{pmatrix} = U \begin{pmatrix} \sqrt{p_1}\,|\mathbf{e}_{\neg k}\rangle \\ \sqrt{p_2}\,|\mathbf{e}'_{\neg k}\rangle \end{pmatrix}. \tag{6.3}$$

According to the Schmidt decomposition [91] of the state $|\psi\rangle$ for the bipartition $k|1\cdots\not{k}\cdots N$, there exist 2 orthonormal 1-qubit states $|a_1\rangle, |a_2\rangle$ such that

$$|\psi\rangle = \sqrt{\lambda_1}\,|v_1\rangle\otimes|a_1\rangle_k + \sqrt{\lambda_2}\,|v_2\rangle\otimes|a_2\rangle_k, \tag{6.4}$$

where we added a subscript to the single qubit states $|a_1\rangle$ and $|a_2\rangle$ to specify which qubit they correspond to.

Using Eq. (6.3), we can then write

$$|\psi\rangle = \sqrt{p_1}\,|\mathbf{e}_{\neg k}\rangle\otimes|\phi_k\rangle_k \;+\; \sqrt{p_2}\,|\mathbf{e}'_{\neg k}\rangle\otimes|\phi'_k\rangle_k, \tag{6.5}$$

where

$$\begin{pmatrix} |\phi_k\rangle \\ |\phi'_k\rangle \end{pmatrix} = U^T \begin{pmatrix} |a_1\rangle \\ |a_2\rangle \end{pmatrix}. \tag{6.6}$$

[1] The length of a separable state ρ corresponds to the minimal number of separable states of any separable decomposition of ρ.

The Equation (6.5) shows that the fragile state $|\psi\rangle$ can always be written as a superposition of two product states. As $|a_1\rangle, |a_2\rangle$ are orthonormal states, the unitary transformation in Eq. (6.6) implies that the states $|\phi_k\rangle$ and $|\phi'_k\rangle$ are orthonormal too. On the other hand, any N-qubit state $|\psi\rangle$ that can be written into the form (6.5) with orthogonal states $|\phi_k\rangle$ and $|\phi'_k\rangle$ is obviously fragile for the loss of its k-th qubit. We can thus conclude the following theorem.

Theorem 6.1. *An entangled N-qubit pure state $|\psi\rangle$ is fragile for the loss of its k-th qubit if and only if it can be written*

$$|\psi\rangle = a|e_1, \ldots, e_N\rangle + b|e'_1, \ldots, e'_N\rangle, \tag{6.7}$$

where $|e_i\rangle$ and $|e'_i\rangle$ $(i = 1, \ldots, N)$ are normalized 1-qubit states such that $\langle e_k|e'_k\rangle = 0$ and $|\langle \mathbf{e}_{\neg k}|\mathbf{e}'_{\neg k}\rangle| < 1$, and where a, b are two nonzero complex numbers such that $|a|^2 + |b|^2 = 1$.

This theorem characterizes all states that are fragile for the loss of a given qubit. We now turn to the scenario in which any particle of the system can be lost.

6.1.2 Fragility for the loss of any one of the qubits

A state $|\psi\rangle$ that is fragile for the loss of any one of its qubits is in particular fragile for the loss of its k-th qubit and can therefore always be written into the form (6.7). The partial trace over the k-th qubit of this state is the separable density operator

$$\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right) = |a|^2\, |\mathbf{e}_{\neg k}\rangle\langle\mathbf{e}_{\neg k}| + |b|^2\, |\mathbf{e}'_{\neg k}\rangle\langle\mathbf{e}'_{\neg k}|. \tag{6.8}$$

On the one hand, the expression (6.7) of $|\psi\rangle$ implies that if $|\langle e_i|e'_i\rangle| = 1$ for some $i \in \{1, \ldots, \not{k}, \ldots, N\}$, then the state $|\psi\rangle$ is biseparable for the bipartition $i|1 \cdots \not{i} \cdots N$. According to Lemma 6.1, this is however incompatible with the fragility for the loss of the i-th qubit. To have a state $|\psi\rangle$ that is fragile for the loss of any of its qubits, we must therefore have $|\langle e_i|e'_i\rangle| < 1$, for all $i \in \{1, \ldots, \not{k}, \ldots, N\}$.

On the other hand, the reduced density operator of $|\psi\rangle$ obtained after partial trace over any other qubit than the k-th, say qubit l $(l \neq k)$, must also be a $(N-1)$-qubit separable mixed state of rank 2. This reduced density operator can always be written

$$\mathrm{Tr}_l\left(|\psi\rangle\langle\psi|\right) = q_1\, |\mathbf{f}_{\neg l}\rangle\langle\mathbf{f}_{\neg l}| + q_2\, |\mathbf{f}'_{\neg l}\rangle\langle\mathbf{f}'_{\neg l}|, \tag{6.9}$$

where $|f_i\rangle$ and $|f'_i\rangle$ $(i \neq l)$ are normalized 1-qubit states such that $|\langle \mathbf{f}_{\neg l}|\mathbf{f}'_{\neg l}\rangle| < 1$, and q_1, q_2 are two positive (nonzero) real numbers satisfying $q_1 + q_2 = 1$.

Following a development similar to the one of the previous section, but this time for the l-th qubit, we find

$$|\psi\rangle = \sqrt{q_1}\, |\mathbf{f}_{\neg l}\rangle \otimes |\phi_l\rangle_l + \sqrt{q_2}\, |\mathbf{f}'_{\neg l}\rangle \otimes |\phi'_l\rangle_l, \tag{6.10}$$

with $|\phi_l\rangle$ and $|\phi'_l\rangle$ two orthonormal 1-qubit states.

The expressions (6.8) and (6.9) being two reduced density operators from the same state, they must fulfill some compatibility conditions. For instance, for any $m \in \{1, \ldots, N\}$ with $m \neq k, l$, the 1-qubit reduced density operator $\mathrm{Tr}_{\neg m}\left[\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)\right]$ (in which $\mathrm{Tr}_{\neg m}$ means that all the qubits are traced out except the m-th), which reads

$$\mathrm{Tr}_{\neg m}\left[\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)\right] = |a|^2|e_m\rangle\langle e_m| + |b|^2|e'_m\rangle\langle e'_m|, \tag{6.11}$$

has to be consistent with the 1-qubit reduced density operators obtained from tracing out first the l-th qubit and then all the qubits except the m-th, i.e. with the reduced density operator

$$\mathrm{Tr}_{\neg m}\left[\mathrm{Tr}_l\left(|\psi\rangle\langle\psi|\right)\right] = q_1|f_m\rangle\langle f_m| + q_2|f'_m\rangle\langle f'_m|. \tag{6.12}$$

Since the expressions (6.11) and (6.12) must correspond to the same density operator, these two decompositions must be related by a unitary transformation [21]. Not taking into account unphysical global phases, this implies that there exist two complex numbers γ, δ, satisfying $|\gamma|^2 + |\delta|^2 = 1$ and such that

$$\begin{pmatrix} \sqrt{q_1}\,|f_m\rangle \\ \sqrt{q_2}\,|f'_m\rangle \end{pmatrix} = \begin{pmatrix} \gamma & \delta \\ -\delta^* & \gamma^* \end{pmatrix} \begin{pmatrix} |a|\,|e_m\rangle \\ |b|\,|e'_m\rangle \end{pmatrix}. \tag{6.13}$$

We can check the compatibility between Eqs. (6.11) and (6.12) by computing expectation values of projectors chosen so as to exploit the relation (6.13) between the two decompositions of the reduced density operator corresponding to the m-th qubit. We choose here the projectors

$$A = \mathbb{1}_2^{\otimes N-3} \otimes |e_k\rangle_k\langle e_k| \otimes |\phi_l\rangle_l\langle\phi_l| \otimes |e_m^\perp\rangle_m\langle e_m^\perp|, \tag{6.14}$$

and

$$B = \mathbb{1}_2^{\otimes N-3} \otimes |e'_k\rangle_k\langle e'_k| \otimes |\phi_l\rangle_l\langle\phi_l| \otimes |(e'_m)^\perp\rangle_m\langle(e'_m)^\perp|, \tag{6.15}$$

where the notation $|a^\perp\rangle$ is used to denote a state that is orthogonal to the state $|a\rangle$. Computing the expectation values of these projectors for the expressions (6.7) and (6.10) of $|\psi\rangle$ yields

$$\begin{cases} \langle\psi|A|\psi\rangle = 0 = |b|^2\,|\delta|^2\,|\langle e'_m|e_m^\perp\rangle|^2\,|\langle f_k|e_k\rangle|^2 \\ \langle\psi|B|\psi\rangle = 0 = |a|^2\,|\gamma|^2\,|\langle e_m|(e'_m)^\perp\rangle|^2\,|\langle f_k|e'_k\rangle|^2 \end{cases}. \tag{6.16}$$

As $|e_m\rangle$ and $|e'_m\rangle$ cannot be proportional to each other, the only solutions of System (6.16) are $\delta = 0$ and $|\langle f_k|e'_k\rangle| = 0$ or $\gamma = 0$ and $|\langle f_k|e_k\rangle| = 0$. Up to swapping the primed and non-primed vectors, these two solutions lead to the same situation, where $|\langle e_m|f_m\rangle| = 1$, $|\langle e'_m|f'_m\rangle| = 1$ and, more interestingly, $|\langle e_k|f_k\rangle| = 1$. Using similar projectors, we can also prove that the states $|e'_k\rangle$ and $|f'_k\rangle$ must be proportional to each other, as well as the states $|e_l\rangle$ and $|\phi_l\rangle$, and $|e'_l\rangle$ and $|\phi'_l\rangle$. Since this is valid for all $m \neq k, l$, the expressions (6.7) and (6.10) of $|\psi\rangle$, resulting from its fragility for the loss of the qubits k and l, respectively, are only compatible if they have the same single qubit states in each term of the sum, with orthogonal states for the qubits l and k. To have a state $|\psi\rangle$ that is fragile for the

loss of any one of its qubits, this orthogonality condition must obviously be replicated on each pair of 1 qubit states. This proves the following theorem.

Theorem 6.2. *An entangled N-qubit state $|\psi\rangle$ is fragile for the loss of any single qubit if and only if it can be written*

$$|\psi\rangle = a|e_1,\ldots,e_N\rangle + b|e_1^\perp,\ldots,e_N^\perp\rangle, \tag{6.17}$$

where $|e_i\rangle$ and $|e_i^\perp\rangle$ are normalized 1-qubit states such that $\langle e_i|e_i^\perp\rangle = 0$ for all $i = 1,\ldots,N$ and where a, b are two nonzero complex numbers such that $|a|^2 + |b|^2 = 1$.

The state $|\mathrm{GHZ}_N\rangle \equiv 1/\sqrt{2}(|0\cdots0\rangle + |1\cdots1\rangle)$ is an emblematic example among states that are fragile for the loss of any one of their qubits. For this state, we have $|e_i\rangle = |0\rangle$ and $|e_i^\perp\rangle = |1\rangle$ for all $i = 1,\ldots,N$, and $a = b = 1/\sqrt{2}$. Any state $|\psi\rangle$ of the form (6.17) is in fact SLOCC-equivalent to the state $|\mathrm{GHZ}_N\rangle$. Indeed, as the states $|e_i\rangle$ and $|e_i^\perp\rangle$ are orthonormal, there exist unitary matrices U_i $(i = 1,\ldots,N)$ such that $U_i\,|e_i\rangle = |0\rangle$ and $U_i\,|e_i^\perp\rangle = |1\rangle$, $\forall i = 1,\ldots,N$. Adding a 2×2 diagonal matrix D to balance the weights, we find:

$$|\mathrm{GHZ}_N\rangle = \left(\bigotimes_{i=1}^{N} D\,U_i\right)|\psi\rangle, \tag{6.18}$$

with

$$D = \begin{pmatrix} (\sqrt{2}a)^{-1/N} & 0 \\ 0 & (\sqrt{2}b)^{-1/N} \end{pmatrix}. \tag{6.19}$$

This shows that the states $|\psi\rangle$ and $|\mathrm{GHZ}_N\rangle$ can be transformed into each other through an invertible local operation (the invertibility of D is ensured by the fact that both a and b are nonzero). These states are thus SLOCC-equivalent [18]. Naturally, there are states that are SLOCC-equivalent to the state $|\mathrm{GHZ}_N\rangle$ but that cannot be transformed into the state $|\mathrm{GHZ}_N\rangle$ through an ILO of the form (6.18). As a consequence, the SLOCC class of the state $|\mathrm{GHZ}_N\rangle$ contains also states that are robust for the loss of any one of their qubits. From this particular SLOCC equivalence, we can conclude the following corollary of Theorem 6.2:

Corollary 6.1. *The entangled N-qubit states that are fragile for the loss of any one of their N qubits belong all to the same SLOCC class, namely that of the state $|\mathrm{GHZ}_N\rangle$ state, but this class contains also robust states.*

6.1.3 Fragility for the loss of one qubit among a given subset of the qubits

The last case we still need to address to get a full characterization of the fragility for the loss of 1 qubit is the fragility for the loss of one qubit among a given subset $\mathcal{A}$ of the qubits. This case can be deduced from the previous one through a few adaptations.

We can for instance use a similar development to show that a state that consists in the superposition of two separable states in which the single qubit states corresponding to all the qubits in the subset $\mathcal{A}$ are pairs of orthogonal states is fragile for the loss of any qubit of $\mathcal{A}$. In the previous case (or in other words when $\mathcal{A}$ contains all the qubits), the unicity of the solution (6.17) was guaranteed by the fact that the fragile state could not be biseparable, for any bipartition. In this case though, we have to reconsider this assumption about the possible biseparability of the state. As a consequence of Lemma 6.1, the states $|\psi\rangle$ we are looking for cannot present a biseparability of the form one qubit versus the rest for any qubit belonging to subset $\mathcal{A}$. This is however not forbidden for the other qubits and this can provide new solutions.

In system (6.16), we can indeed find a different solution if the states $|e_m\rangle$ and $|e'_m\rangle$ correspond to a qubit (the m-th in that case) that do not belong to the subset $\mathcal{A}$ and are proportional to each other. Since the same system can be written for any qubit that does not belong to $\mathcal{A}$, another solution can be found only if the state $|\psi\rangle$ is biseparable for the bipartition $\mathcal{A}$ versus the rest and such that the state corresponding to the complement of $\mathcal{A}$ is fully separable. In this case, the qubit states corresponding to the complement of $\mathcal{A}$ can always be factored out of any partial trace and do not influence the separability of the global state. The fragility problem of the global state is then equivalent to the fragility problem of the state corresponding to the qubits in $\mathcal{A}$ only. We already know, from Theorem 6.2, the solution of this problem if $\mathcal{A}$ contains at least 3 qubits. If $\mathcal{A}$ contains only 2 qubits, however, the partial trace of the global state over any of the 2 qubits in $\mathcal{A}$ always yields a separable mixed because of the separability of the state corresponding to the qubits belonging to the complement of $\mathcal{A}$. As a consequence, for any subset $\mathcal{A}$ containing 2 qubits, any N-qubit state $|\psi\rangle$ of the form

$$|\psi\rangle = |\phi_e\rangle_{\mathcal{A}} \otimes |\phi_s\rangle_{\bar{\mathcal{A}}}\,, \tag{6.20}$$

with $|\phi_e\rangle_{\mathcal{A}}$ an entangled state of the 2 qubits of $\mathcal{A}$ and $|\phi_s\rangle_{\bar{\mathcal{A}}}$ a product state of the remaining $N-2$ qubits, is an entangled state that is fragile for the loss of any qubit in $\mathcal{A}$.

The Schmidt decomposition [91] of the bipartite state $|\phi_e\rangle$ implies that there always exist pairs of orthonormal states $|e_1^{(1)}\rangle$, $|e_2^{(1)}\rangle$ and $|e_1^{(2)}\rangle$, $|e_2^{(2)}\rangle$, such that

$$|\phi_e\rangle = \sum_{i=1}^{2} \lambda_i |e_i^{(1)}\rangle \otimes |e_i^{(2)}\rangle, \tag{6.21}$$

with λ_1, λ_2 two nonzero real numbers satisfying $\lambda_1^2 + \lambda_2^2 = 1$. In the end, the fragile state (6.20) can thus also be written as a superposition of two product states in which the qubits of $\mathcal{A}$ correspond to pairs of orthogonal states. This turns out to be the unique, general form of fragility for the loss of one qubit belonging to any subset $\mathcal{A}$ of the qubits. We summarize this in the following theorem.

Theorem 6.3. *An entangled N-qubit pure state $|\psi\rangle$ is fragile for the loss of any qubit belonging to a given subset $\mathcal{A}$ of the qubits if and only if it can be written*

$$|\psi\rangle = a|e_1, \ldots, e_N\rangle + b|e'_1, \ldots, e'_N\rangle, \tag{6.22}$$

where $|e_i\rangle$, $|e'_i\rangle$ $(i = 1, \ldots, N)$ are normalized 1-qubit states such that $\langle e_k|e'_k\rangle = 0$ for all $k \in \mathcal{A}$ and, if $\#\mathcal{A} = 1$, there exists at least one $j \in \{1, \ldots, N\} \setminus \mathcal{A}$ such that $|e_j\rangle$ and $|e'_j\rangle$ are not proportional to each other, and where a, b are two nonzero complex numbers satisfying $|a|^2 + |b|^2 = 1$.

This theorem concludes our general study of entanglement fragility for the loss of a single qubit in multiqubit systems. In the next section, we consider the extension of these results to multiqudit systems.

6.2 Fragility for the loss of 1 particle in multiqudit systems

We first consider the extension of Theorem 6.1 to multiqudit systems and search the conditions under which an N-qudit pure state $|\psi\rangle$ is fragile for the loss of its k-th qudit. In the proof of Theorem 6.1, the dimension of the subsystems (which was 2 in the multiqubit case) was only used once, to get an upper bound on the rank of the reduced density operator obtained after tracing out the k-th particle. Indeed, as a consequence of the Schmidt decomposition for the bipartition $k|1 \cdots \not{k} \cdots N$, the partial trace over the k-th particle of a pure state $|\psi\rangle$ has a rank that is equal to the local rank associated to the k-th particle. When $|\psi\rangle$ was a multiqubit state, the rank of $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$ was thus at most equal to 2. If $|\psi\rangle$ is now a multiqudit state, the rank of $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$ can take values up to d.

We show now that this maximal rank has a critical impact from the perspective of extending the proof of Theorem 6.1 to multiqudit systems. Given an entangled N-qudit pure state $|\psi\rangle$ that is fragile for the loss of its k-th qudit, the reduced density operator $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$ must be separable and have a rank strictly greater than 1 (as a consequence of Lemma 6.1). In the generic case, the separable $(N-1)$-qudit state $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$ has rank d. Following the proof of Theorem 6.1, we should now exploit a separable decomposition of $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$, generalizing Eq. (6.5). Unlike in the multiqubit case, we do here not know the length l of the separable state $\mathrm{Tr}_k(|\psi\rangle\langle\psi|)$. In the multiqubit case, we had indeed used the fact that separable states of rank 2 have a length equal to 2 [70], but, to our knowledge, this result has not been generalized to separable states of arbitrary rank d.

Up to the fact that we cannot relate the length of $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ to its rank, we can still perform a development similar to the one that allowed us to prove Theorem 6.1. To

begin with, we can write the separable state $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ of rank d and length l as

$$\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right) = \sum_{j=1}^{l} p_j |\mathbf{e}_{\neg k}^{(j)}\rangle\langle\mathbf{e}_{\neg k}^{(j)}|, \tag{6.23}$$

with $p_j > 0\ \forall j = 1, \ldots, l$ satisfying $\sum_{j=1}^{l} p_j = 1$, and

$$|\mathbf{e}_{\neg k}^{(j)}\rangle = \bigotimes_{\substack{i=1 \\ i\neq k}}^{N} |e_i^{(j)}\rangle, \tag{6.24}$$

where $|e_i^{(j)}\rangle$ $(i = 1, \ldots, N, i \neq k$ and $j = 1, \ldots, l)$ are normalized 1-qubit states such that $|\mathbf{e}_{\neg k}^{(j)}\rangle$ and $|\mathbf{e}_{\neg k}^{(j')}\rangle$ are not proportional for all $1 \leq j < j' \leq l$.

Let λ_i $(i = 1, \ldots, d)$ be the d nonzero eigenvalues of $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ and $|v_i\rangle$ the associated eigenvectors. We denote by U the $d \times l$ "unitary" matrix (whose rows are d orthonormal vectors of $\mathbb{C}^l$) connecting the separable decomposition (6.23) of $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ to its eigendecomposition [21]. This unitary satisfies

$$\begin{pmatrix} \sqrt{\lambda_1}\,|v_1\rangle \\ \vdots \\ \sqrt{\lambda_d}\,|v_d\rangle \end{pmatrix} = U_{d\times l} \begin{pmatrix} \sqrt{p_1}\,|\mathbf{e}_{\neg k}^{(1)}\rangle \\ \vdots \\ \sqrt{p_l}\,|\mathbf{e}_{\neg k}^{(l)}\rangle \end{pmatrix}. \tag{6.25}$$

According to the Schmidt decomposition [91] of the state $|\psi\rangle$ for the bipartition $k|1\cdots\not{k}\cdots N$, there exist d orthonormal 1-qudit states $|a_i\rangle$ $(i = 1, \ldots, d)$ such that

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\ |v_i\rangle \otimes |a_i\rangle_k, \tag{6.26}$$

where we add subscripts to the single qudit states $|a_i\rangle$ to specify which qudit they correspond to.

Using Eq. (6.25), we can then write

$$|\psi\rangle = \sum_{j=1}^{l} \sqrt{p_j}\,|\mathbf{e}_{\neg k}^{(j)}\rangle \otimes |\phi_k^{(j)}\rangle_k, \tag{6.27}$$

where

$$\begin{pmatrix} |\phi_k^{(1)}\rangle \\ \vdots \\ |\phi_k^{(l)}\rangle \end{pmatrix} = \left(U_{d\times l}\right)^T \begin{pmatrix} |a_1\rangle \\ \vdots \\ |a_d\rangle \end{pmatrix}. \tag{6.28}$$

The length of a separable state cannot be smaller than its rank and l is thus either equal to d or strictly greater than d. If it is equal to d, U is a usual unitary matrix and

the unitary matrix U^T transforms the orthonormal states $|a_1\rangle, \ldots, |a_d\rangle$ into orthonormal states $|\phi_k^{(1)}\rangle, \ldots, |\phi_k^{(d)}\rangle$. In this case, we can thus write the fragile state $|\psi\rangle$ as a superposition of d product states in which the qudit states associated to the k-th particle are orthogonal to each other. By contrast, if $l > d$, then the matrix U^T is made of l non-orthonormal rows and it transforms the orthonormal states $|a_1\rangle, \ldots, |a_d\rangle$ into non normalized nor orthogonal states $|\phi_k^{(1)}\rangle, \ldots, |\phi_k^{(l)}\rangle$. In this case, with the loss of the orthogonality between the qudit states associated to the k-th particle, we also lose the sufficient condition of fragility for the loss of the k-th qudit of the state (6.27). As a consequence, we can only extend the proof of Theorem 6.1 to qudit systems if $l = d$. Although we cannot guarantee it in the general case, we can exploit the results of Ref. [70] concerning the length of mixed states of rank 3 to study the qutrit case.

Let $|\psi\rangle$ be an entangled N-qutrit state that is fragile for the loss of its k-th qutrit. In this case, the separable reduced density operator $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ has either rank 2 or rank 3 (rank 1 being impossible because of Lemma 6.1). If it has rank 2, it has necessarily a length equal to its rank. If $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ has rank 3, then it has also length 3, except in the special case where the $(N-1)$-particle state $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ has $(N-3)$ particles with rank-1 reduced density operators and 2 particles with rank-2 reduced density operators, in which case it can also have length 4 [70]. When $|\psi\rangle$ does not have the local rank configuration of the special case, the separable density operator $\mathrm{Tr}_k\left(|\psi\rangle\langle\psi|\right)$ has a length equal to its rank. Using the previous development, we can thus conclude the following fragility criterion for the loss of 1 particle, for almost all N-qutrit states (the special case is not generic).

Proposition 6.1. *Let $|\psi\rangle$ be an entangled N-qutrit state. Given one of the qutrit, say the k-th, if $|\psi\rangle$ has not the special local rank configuration in which the k-th qutrit is the only one that has local rank 3, $N-3$ qutrits have local rank 1, and the two remaining ones have local rank 2, then $|\psi\rangle$ is fragile for the loss of its k-th qutrit if and only if it can be written*

$$|\psi\rangle = \sum_{j=1}^{l} \sqrt{p_j}\, |e_1^{(j)}, \ldots, e_N^{(j)}\rangle,, \tag{6.29}$$

where $l \in \{2,3\}$ is the local rank of the k-th qutrit, $|e_i^{(j)}\rangle$ ($i = 1, \ldots, N$ and $j = 1, \ldots, l$) are single qutrit states such that $\langle e_k^{(j)} | e_k^{(j')}\rangle = 0$ and $|\mathbf{e}_{\neg k}^{(j)}\rangle$ is not proportional to $|\mathbf{e}_{\neg k}^{(j')}\rangle$ for $j \neq j'$, and $p_1, \ldots, p_l$ are strictly positive numbers such that $\sum_{j=1}^{l} p_j = 1$.

For all the states for which we can apply Theorem 6.1 or Proposition 6.1, fragility for the loss of a given qubit is not a generic property. This is essentially due to the orthogonality relations required when writing the pure fragile state as a superposition of product states, which are not met by generic states. As mentioned earlier, states which, after the loss of a given particle, have a reduced density that (if separable) can have a length greater than its rank, do not have to meet these orthogonality conditions to be fragile. As we show now, this can, in some particular systems, dramatically change the proportion of states that are fragile for the loss of one particle.

In a hybrid system composed of one qutrit and two qubits, the reduced density operator obtained after having traced out the qutrit is a mixed state that has generically rank 3 but that could, if separable, have length 4. Out of 1000 random[2] pure states of this system, we could always find a non-negligible fraction of fragile states (from 20 repetitions of the numerical simulation, the mean fraction of fragile state was about 0.088, with a standard deviation of 0.009), showing that generic states of this system have a nonzero probability of being fragile for the loss of the qutrit. By contrast, out of all the simulations that were performed, none of these random states were fragile for the loss of one of the two qubits, which is not surprising as this kind of fragility is characterized by Proposition 6.1.

6.3 Robustness against particle loss in the symmetric subspace

Due to their permutation invariance, the reduced density operators of a symmetric multiqubit state corresponding to a given number of qubits are all equal, whatever subset of the qubits is traced out. This implies that if a symmetric state is fragile (respectively robust) for the loss of some k-tuple of its qubits, it is also fragile (respectively robust) for the loss of any other k-tuple of its qubits.

In light of this observation, we first revisit the results we obtained in the previous section about the fragility for the loss of 1 qubit for the special case of symmetric states. We investigate then the fragility of symmetric states for the loss of several qubits and consider in particular the states belonging to the SLOCC classes of the Dicke states.

6.3.1 Symmetric states fragile for the loss of 1 qubit

Due to their permutation invariance, symmetric states that are fragile for the loss of a given qubit must be also fragile for the loss of any other qubit. As a consequence, symmetric states that are fragile for the loss of 1 qubit must necessarily satisfy Theorem 6.2. In the following corollary, we particularize this theorem in order to get a necessary and sufficient condition for the fragility for the loss of one qubit of symmetric states.

Corollary 6.2. *A symmetric entangled N-qubit state $|\psi_S\rangle$ is fragile for the loss of any single qubit if and only if it can be written*

$$|\psi_S\rangle = a|e,\ldots,e\rangle + b|e^\perp,\ldots,e^\perp\rangle, \tag{6.30}$$

where $|e\rangle$ and $|e^\perp\rangle$ are normalized 1-qubit states such that $\langle e|e^\perp\rangle = 0$ and a, b are 2 nonzero complex numbers such that $|a|^2 + |b|^2 = 1$.

[2]For this random generation of pure states, the real and imaginary parts of the 12 complex components of the states in the (hybrid) computational basis were chosen uniformly at random on the unit sphere in $\mathbb{R}^{24}$ using G. Marsaglia's method given in Ref. [98].

Proof. States of the form (6.30) constitute a particular case, obviously symmetric, of the general case of states $|\psi\rangle$ that are fragile for the loss of any one of their qubits, which can always be written (see Theorem 6.2)

$$|\psi\rangle = a|e_1, \ldots, e_N\rangle + b|e_1^\perp, \ldots, e_N^\perp\rangle. \tag{6.31}$$

We now prove that this is the only possible form for a symmetric state satisfying the desired fragility property. Let us assume that, in Eq. (6.31), there are at least two unproportional states $|e_k\rangle$ and $|e_l\rangle$ for some $k, l \in \{1, \ldots, N\}, k \neq l$. Since the single qubit states appearing in Eq. (6.31) are normalized, we have $\langle e_1, \ldots, e_N|\psi\rangle = a$. If $|\psi\rangle$ is a symmetric state, it must remain invariant under any permutation of the qubits, thus in particular under the permutation of the qubits k and l. However, denoting by P_{kl} the operator permuting the qubits k and l, we have $\langle e_1, \ldots, e_N|P_{kl}|\psi\rangle = a|\langle e_k|e_l\rangle|^2$. As a consequence, $|\psi\rangle$ cannot be symmetric if $|e_k\rangle$ and $|e_l\rangle$ are not proportional to each other. The state $|\psi\rangle$ can thus only be symmetric if all the single qubit states $|e_1\rangle, \ldots, |e_N\rangle$ of Eq. (6.31) are proportional to each other, in which case $|\psi\rangle$ can always be written into the form (6.30). □

As a consequence of corollary 6.1, any symmetric state that is fragile for the loss of one of its qubits is SLOCC-equivalent to the state $|\mathrm{GHZ}_N\rangle$. In the symmetric subspace, the fragility for the loss of one qubit is thus limited to a single SLOCC class. As we show now this fragility property of symmetric states can be related to a particular symmetry of their Majorana points. The state $|\mathrm{GHZ}_N\rangle$ is known to have a highly symmetrical Majorana representation, with Majorana points forming a regular N-sided polygon on the equatorial plane of the Bloch sphere (see Fig. 6.1). Surprisingly, this polygonal symmetry of the Majorana points turns out to be a necessary and sufficient condition for the fragility for the loss of any single qubit of symmetric multiqubit states. This is the object of the following Theorem.

Theorem 6.4. *A symmetric entangled N-qubit pure state $|\psi_S\rangle$ is fragile for the loss of any one of its qubits if and only if its Majorana points are the vertices of a regular N-sided polygon in any plane intersecting the Bloch sphere.*

Proof. It was shown in Ref. [99] that point-group symmetries of the Majorana points of a multiqubit symmetric state induce constraints on the coefficients of the symmetric state in the Dicke basis. In particular, the results of Ref. [99] imply that an N-qubit symmetric state has N distinct Majorana points exhibiting the symmetries of a regular N-sided polygon if and only if it is equivalent through a symmetric LU operation to a state of the form

$$|\phi_S\rangle = a'|0, \ldots, 0\rangle + b'|1, \ldots, 1\rangle, \tag{6.32}$$

where a' and b' are two nonzero complex numbers such that $|a'|^2 + |b'|^2 = 1$.

As the single qubit states $|0\rangle$ and $|1\rangle$ are orthonormal, a unitary operation always transforms them into a pair of orthonormal states. As a consequence, a symmetric LU

operation always transforms a state of the form (6.32) into a state of the form (6.30) and corollary 6.2 concludes the proof. □

As illustrated in Fig. 6.1, this proposition gives a direct geometrical interpretation of the fragility for the loss of one qubit in the symmetric subspace.

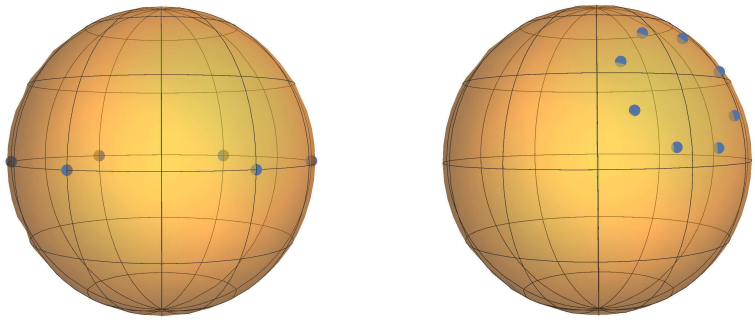


Figure 6.1: Illustration of the Majorana representations of two symmetric multiqubit states that are fragile for the loss of one qubit. As shown in Theorem 6.4, these states necessarily have Majorana points forming a regular polygon inscribed into a circle of the Bloch sphere. This circle can be a great circle (as in the left figure), in which case it corresponds to a state LU-equivalent to the state $|\mathrm{GHZ}_N\rangle$, or any circle that is not degenerated into a point (as in the right figure).

6.3.2 Symmetric states fragile for the loss of multiple qubits

In the previous section, we showed that symmetric states that are fragile for the loss of one qubit belong all to the same SLOCC class. This is however not true for states that are fragile for the loss of at least 2 qubits. We illustrate this with symmetric states of 4 qubits. As explained in Section 1.3.2, symmetric multiqubit states can be classified into families [25] based on the degeneracy list of the 1-qubit states appearing in their Majorana representation. In this classification, symmetric 4-qubit states with 4 distinct 1-qubit states in their Majorana representation belong to the family $\mathcal{D}_{1,1,1,1}$, which contains an infinite number of different SLOCC classes [25]. In Ref. [100], it was shown that each SLOCC class in the family $\mathcal{D}_{1,1,1,1}$ is unambiguously represented, for a given value of the complex number μ in the set (see Fig. 6.2)

$$\mathcal{S} = \{\mu \in \mathbb{C} : \mathrm{Re}(\mu), \mathrm{Im}(\mu) \geq 0,\ \mu < \sqrt{2/3} \text{ if } \mathrm{Im}(\mu) = 0 \\ \text{and } |\mu - \sqrt{2/3}| < \sqrt{8/3} \text{ if } \mu \neq \sqrt{2}\, i\}, \quad (6.33)$$

by the state

$$|\psi_\mu\rangle = \frac{1}{\sqrt{2+|\mu|^2}}\Big(|D_4^{(0)}\rangle + \mu|D_4^{(2)}\rangle + |D_4^{(4)}\rangle\Big), \quad (6.34)$$

where, $|D_4^{(k)}\rangle$ denotes the k excitations Dicke state of 4 qubits. In their respective SLOCC class, the states $|\psi_\mu\rangle$ are in addition the unique maximally entangled states (up to LU operations) in the sense that their 1-qubit reduced density operators are maximally mixed [100]. To estimate their robustness for the loss of 1 or 2 qubit(s), we use the negativity [81]. Given a subset $\mathcal{A}$ of the qubits, the negativity, denoted by $\mathcal{N}$, is an entanglement measure defined for any state ρ as

$$\mathcal{N}(\rho) = \frac{||\rho^{T_\mathcal{A}}||_1 - 1}{2}, \tag{6.35}$$

where $||\rho||_1 = \mathrm{Tr}(\sqrt{\rho\rho^\dagger})$ and $\rho^{T_\mathcal{A}}$ is the partial transpose of ρ with respect to the qubits of $\mathcal{A}$. After the loss of 1 or 2 qubit(s), the states $|\psi_\mu\rangle$ become symmetric mixed states of 3 or 2 qubits. For such states, the negativities corresponding to all the possible subsets of the qubits yield the same value. For this reason, we only consider the negativity relative to the first qubit. For symmetric mixed states of 3 or 2 qubits, the PPT criterion, and thus the vanishing of the negativity, is in addition a necessary and sufficient condition of separability [78]. A state $|\psi_\mu\rangle$ is then fragile for the loss of 1 or 2 qubits if and only if the negativity of the corresponding reduced density operator is equal to zero.

For the loss of 1 qubit, there is only one fragile state $|\psi_\mu\rangle$, namely the state $|\psi_0\rangle$, which is nothing but the $|\mathrm{GHZ}_4\rangle$ state. By contrast, there is a continuous set of state $|\psi_\mu\rangle$ that are fragile for the loss of 2 qubits, corresponding to values of μ belonging to the set (see Fig. 6.2)

$$\mathcal{F} = \mathcal{S} \cap \left\{ \mu \in \mathbb{C} : \mathrm{Im}(\mu) \geq \sqrt{\left(\sqrt{6} - \mathrm{Re}(\mu)\right) \mathrm{Re}(\mu)} \right\}. \tag{6.36}$$

Since the states $|\psi_\mu\rangle$ are SLOCC-inequivalent for different values of μ in S, this shows that the fragility of multiqubit symmetric entangled states for the loss of more than one qubit is not restricted to a single SLOCC class (by contrast to the fragility for the loss of a single qubit).

6.3.3 Robustness in the Dicke states SLOCC classes

Up to now, we mainly focused on the characterization of states that are fragile for the loss of some of their qubits. In this section, we identify symmetric SLOCC classes containing only robust states.

As mentioned in the introduction, the robustness of entanglement against particle loss of the state $|\mathrm{W}_3\rangle$ was first shown in Ref. [18]. This state can naturally be generalized in systems of $N > 3$ qubits, in which it coincides with the 1 excitation Dicke state $|D_N^{(1)}\rangle$. As a natural extension, we can thus study the robustness properties of all Dicke states.

It was shown in Ref. [101] that the 2-qubit reduced density operators of all the entangled Dicke state (which excludes the cases $k = 0$ and $k = N$) are entangled states. As separable states (of at least 3 particles) remain separable after particle loss, this also implies that the entangled Dicke states are robust for the loss of any number $t \in \{1, \ldots, N-2\}$ of their qubits. Another way to prove this is to compute the negativity (for the first qubit)

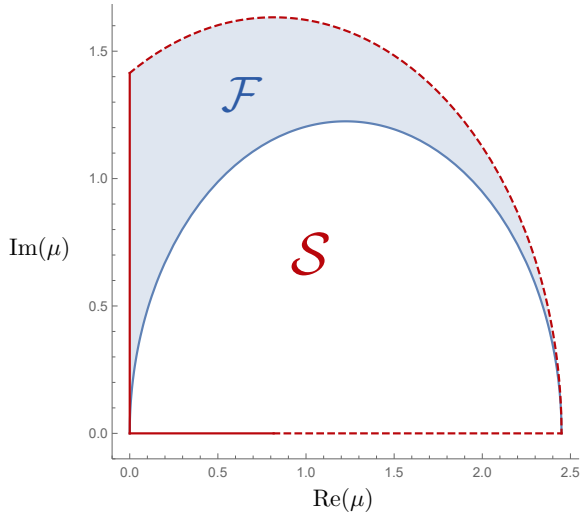


Figure 6.2: Representation of the set $\mathcal{S}$ (area inside the red borders, with the dashed borders excluded) in the complex plane corresponding the values of the parameter μ for which the states $|\psi_\mu\rangle$ are SLOCC-inequivalent. The blue area $\mathcal{F}$ corresponds to the values of μ for which the states $|\psi_\mu\rangle$ are fragile for the loss of 2 qubits.

of the reduced density operator obtained after partial trace of t qubits. This computation gives

$$\mathcal{N}\left(\mathrm{Tr}_{1,\ldots,t}|D_N^{(k)}\rangle\langle D_N^{(k)}|\right) = \frac{1}{2\binom{N}{k}}\sum_{i=1}^{t+1}\left(-x_N^{(k)}(i)+\sqrt{\left(x_N^{(k)}(i)\right)^2+4y_N^{(k)}(i)}\right), \tag{6.37}$$

with

$$x_N^{(k)}(i) = \binom{t}{i-2}\binom{N-t-1}{k-i+1}+\binom{t}{i}\binom{N-t-1}{k-i}, \tag{6.38}$$

and

$$y_N^{(k)}(i) = \binom{N-t-1}{k-i}\binom{N-t-1}{k-i+1}\left(\binom{t}{i-1}^2-\binom{t}{i-2}\binom{t}{i}\right), \tag{6.39}$$

where $\binom{a}{b}$ is the binomial coefficient with the usual convention $\binom{a}{b}=0$ if $b>a$ or $b<0$. As $x_N^{(k)}(i)$ and $y_N^{(k)}(i)$ are always positive numbers for any $N\geq 3$, $k=1,\ldots,N-1$ and $y_N^{(k)}(i)$ is different from zero for at least one value of i between 1 and $t+1$, we can conclude that $\mathcal{N}\left(\mathrm{Tr}_{1,\ldots,t}|D_N^{(k)}\rangle\langle D_N^{(k)}|\right)>0$, $\forall\ N\geq 3, 1\leq k\leq N-1$ and $1\leq t\leq N-2$. This confirms the robustness property of the entangled Dicke states.

We conjecture that this robustness property is not limited to the entangled Dicke states but extends to their whole SLOCC classes. We present now analytical and numerical results supporting this conjecture. Let us first note that if a state $|\psi\rangle$ is robust for the loss of a subset $\mathcal{A}$ of its particles, then any state equivalent to $|\psi\rangle$ under LU operations is

also robust for the loss of the particles of the subset $\mathcal{A}$. In other words, the robustness (or fragility) against particle loss is an LU-invariant property. This is due to the fact that the local unitaries acting on the particles that are traced out can be seen as a change of basis and do not affect the partial trace operation, as well as the local unitaries acting on the remaining qubits do not change the separability property of the corresponding reduced density operator. As a consequence, we can restrict ourselves to study the robustness of one representative state per LU class.

In the symmetric subspace of an N-qubit system, the Dicke states $|D_N^{(i)}\rangle$ and $|D_N^{(j)}\rangle$ for $i,j \in \{0,\ldots,N\}, i \neq j$ are SLOCC-inequivalent if and only if $i + j \neq N$. The Dicke states thus belong to $\lfloor N/2 \rfloor$ different SLOCC classes, that we denote by $\mathcal{D}_{N-k,k}$ ($k = 1,\ldots,\lfloor N/2 \rfloor$) following the notations of Ref. [25]. Any symmetric state belonging to the SLOCC class $\mathcal{D}_{N-k,k}$ has only 2 different single qubit states in its Majorana representation, degenerated $N-k$ and k times, respectively. Using LU operations, it is always possible to bring the $N-k$ times degenerated state onto the state $|0\rangle$ state and to make real the two computational basis components of the other qubit state. As a consequence, any state in a SLOCC class $\mathcal{D}_{N-k,k}$ is LU-equivalent, for some parameter $u \geq 0$, to the state

$$|\psi_N^{(k)}(u)\rangle = \sqrt{A_N^{(k)}(u)} \sum_{\pi} |0\rangle^{\otimes N-k} \otimes (u\,|0\rangle + |1\rangle)^{\otimes k}, \tag{6.40}$$

with

$$A_N^{(k)}(u) = \left(\sum_{i=0}^{k} \frac{\binom{k}{i}^2}{\binom{N}{i}} u^{2(k-i)} \right)^{-1}. \tag{6.41}$$

Tracing out all qubits but 2, we get the reduced density operator $\tilde{\rho}_N^{(k)}(u) = \mathrm{Tr}_{\neg 1,2}(|\psi_N^{(k)}(u)\rangle\langle\psi_N^{(k)}(u)|)$, which is given by

$$\tilde{\rho}_N^{(k)}(u) = A_N^{(k)}(u) \begin{pmatrix} f_N^{(k)}(u,0,0) & f_N^{(k)}(u,1,0) & f_N^{(k)}(u,1,0) & f_N^{(k)}(u,2,0) \\ f_N^{(k)}(u,1,0) & f_N^{(k)}(u,1,1) & f_N^{(k)}(u,1,1) & f_N^{(k)}(u,2,1) \\ f_N^{(k)}(u,1,0) & f_N^{(k)}(u,1,1) & f_N^{(k)}(u,1,1) & f_N^{(k)}(u,2,1) \\ f_N^{(k)}(u,2,0) & f_N^{(k)}(u,2,1) & f_N^{(k)}(u,2,1) & f_N^{(k)}(u,2,2) \end{pmatrix}, \tag{6.42}$$

with

$$f_N^{(k)}(u,j,j') = \frac{1}{\binom{N}{k}^2} \sum_{i=0}^{k} \binom{N-i-j}{k-i-j} \binom{N-i-j'}{k-i-j'} \binom{N-2}{i} u^{2(k-i)-j-j'}. \tag{6.43}$$

Showing that the reduced density operator $\tilde{\rho}_N^{(k)}(u)$ is entangled shows that the state $|\psi_N^{(k)}(u)\rangle$ is robust for the loss of any number of its qubits (up to $N-2$). To prove that $\tilde{\rho}_N^{(k)}(u)$ is indeed entangled, it is sufficient to show that the determinant of its partial transpose over the first qubit is negative, since this implies that the state is NPT [27].

For the simplest case $k = 1$ (which corresponds to considering the states in the SLOCC class of the state $|\mathrm{W}_N\rangle$), the determinant is simply given by

$$\det\left[\left(\tilde{\rho}_N^{(1)}(u)\right)^{T_1}\right] = -\left(A_N^{(1)}(u)\right)^4, \tag{6.44}$$

which shows that all the states that are SLOCC-equivalent to the state $|\mathrm{W}_N\rangle$ are robust for the loss of any number of their qubits (up to $N-2$).

For $k > 1$, only strong numerical evidences for a similar conclusion can be given. In Fig. 6.3, we see that for a fixed number N of qubits (here set to 10) the determinant of the partial transpose of $\tilde{\rho}_N^{(k)}(u)$ gets more and more negative for increasing values of k. The behavior for increasing number of qubits and $k = 2$ is shown in Fig. 6.4. In this case, the determinant flattens with increasing number of qubits, coming from the negative side closer to the flat zero curve. This suggests that extrapolating to any value of N and $k = 2, \ldots, \lfloor N/2 \rfloor$, we would always have strictly negative values for the determinant and that all symmetric states in the remaining Dicke state SLOCC classes $\mathcal{D}_{N-k,k}$ ($k = 2, \ldots, \lfloor N/2 \rfloor$) would be robust with respect to the loss of any number t of qubits ($t \leq N-2$).

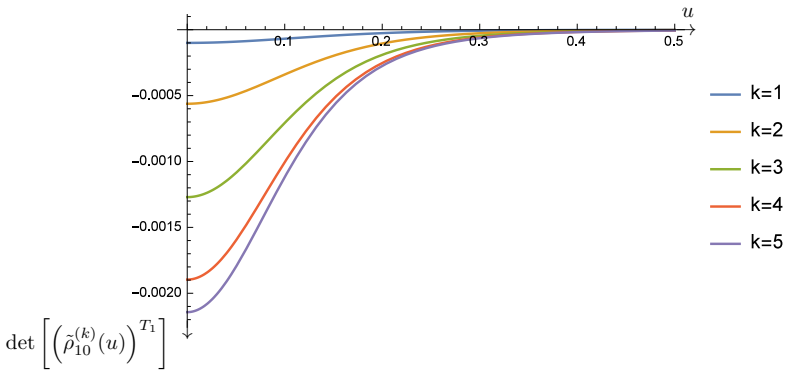


Figure 6.3: Plot of the determinant of the partial transpose (over the first qubit) of the 2-qubit reduced density operator $\tilde{\rho}_N^{(k)}(u)$ as a function of the parameter u for all the possible values of k (N being set here to 10).

Finding states that are robust with respect to the loss of an arbitrary number of qubits is particularly interesting as this property is not generic. When translated into the context and notations of this paper, the results of Refs. [102, 103, 104] imply that N-qubit pure states chosen uniformly at random (according to the natural Fubini-Study measure in the N-qubit Hilbert space) have a probability close to 1 to be fragile for the loss of any t-tuple of their qubits for the largest values of t. By contrast, for the smallest values of t, random states have a probability close to 1 to be robust for the loss of any t-tuple of their qubits. There is a transition region between generic robustness and generic fragility,

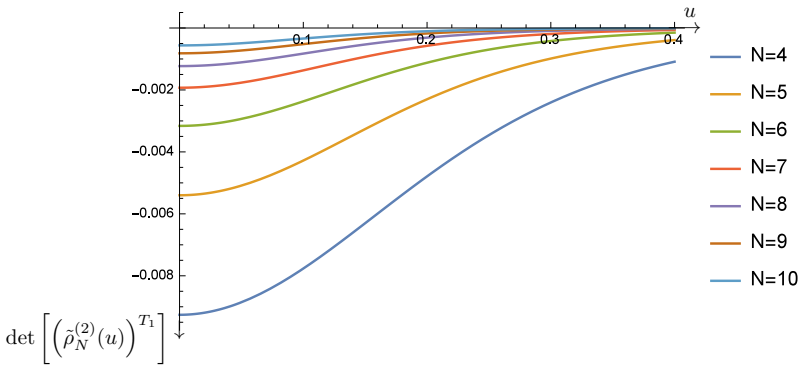


Figure 6.4: Plot of the determinant of the partial transpose (over the first qubit) of the 2-qubit reduced density operator $\tilde{\rho}_N^{(k)}(u)$ as a function of the parameter u for increasing values of N, from 4 to 10 (k being set here to 2).

corresponding to the values of t for which both fragile and robust states with respect to the loss of t qubits can be found with nonnegligible probability. In this region of the t parameter space, the probability of being robust for the loss of any t qubits was shown to decrease exponentially with t, from both numerical simulations [102, 103] and theoretical arguments [104], making the transition region surprisingly sharp. For N-qubit systems, it was numerically estimated to lie somewhere between $N/3$ and $N/2$ [103].

Conclusion

The aim of this thesis was to contribute to a better understanding of quantum entanglement in multipartite systems. Quantum entanglement is a complex property, with countless distinct features that must generally be characterized independently. In this work, we focused on the detection of entanglement, its characterization under local operations, its quantification and its robustness against particle loss. We always considered quantum systems associated to a Hilbert space of finite dimension, such as the celebrated multiqubit systems, or the more general multiqudit systems. We also frequently took a closer look at the case of the symmetric multiqubit states (i.e. states that remain invariant under any permutation of their qubits).

In Chapter 1, we reviewed basic notions of quantum information theory that were used throughout this thesis. We first introduced quantum systems associated to finite dimensional Hilbert spaces and described the formalisms used to treat pure and mixed states. We also defined symmetric states and detailed the Dicke and Majorana representations for these states. We then introduced elementary notions of entanglement characterization. More specifically, we considered entanglement detection, the operational classification of entanglement through local operations and entanglement quantification.

In Chapter 2, we studied fidelity optimization within operational classes containing symmetric states. When computing the maximal fidelity between a symmetric state and all the states of an operational class containing symmetric state, it is interesting to determine whether the maximal fidelity is always obtained for a symmetric state or not. We specifically studied a conjecture stating that this question always admits a positive answer for the SLOCC class of the state $|\mathrm{W}_N\rangle$. On the one hand, we showed that stabilizers of the state $|\mathrm{W}_N\rangle$ can be used to decrease the number of parameters needed in any fidelity optimization within its SLOCC class. On the other hand, we computed the most general stabilizer of the state $|\mathrm{W}_N\rangle$.

In Chapter 3, we studied the general separability problem, which consists in determining whether a given state ρ is separable or not. We first tackled the separability problem of pure states using the concept of generalized concurrences. We showed that the existing methods for generating generalized concurrences produce an overcomplete set, containing redundant generalized concurrences, and proposed an optimized method for generating only the independent ones. This new set contains the minimal number of generalized

concurrences providing a necessary and sufficient condition of separability for pure states. We then used the preconcurrence matrix formalism to address the separability of mixed states. We showed that the general separability problem can be reformulated into a pure matrix analysis problem that consists in determining whether a set of symmetric matrices can be simultaneously hollowised, i.e. simultaneously transformed by unitary congruence into matrices with a diagonal only composed of zeroes. Although this mathematical problem is to date still open, it provides a new angle to tackle the separability problem and it should pave the way toward new research in this field. We initiated research in this direction with the study of the simultaneous hollowisation problem for 2×2 and 3×3 symmetric matrices. In the 2×2 case, we found a criterion of simultaneous hollowisation and showed how to convert it into a general separability criterion for mixed states of rank 2. Even though there exist other separability criteria for mixed states of rank 2, our criterion has the advantage to provide a separable decomposition over two product states for any separable state of rank 2 and it further allowed us to prove that such a decomposition is unique. In the 3×3 case, we showed how to transform the simultaneous hollowisation problem into a set of equations involving only one real parameter. These equations being easily solved numerically, we proposed an algorithm to efficiently solve the separability problem for mixed states of rank 3. This algorithm has also the advantage of providing a separable decomposition of minimal cardinality for all separable states of rank 3.

In Chapter 4, we set aside entangled states to study optimal separable decomposition properties of symmetric separable states. By contrast to Chapter 3, we used methods based on the partial transposition operation to characterize separability. We first showed how to extend an algorithm that had been proposed for trying to reconstruct separable decompositions of PPT bipartite states to the general multipartite case. We also showed that this algorithm could be drastically simplified for symmetric multiqubit states, increasing its tractability for large numbers of parties. We then used this algorithm to study optimal separable decompositions (i.e. separable decompositions containing the lowest possible number of product states) of symmetric states of 2 to 4 qubits. For symmetric states of 2 and 3 qubits, we showed that any mixed state ρ_S of maximal rank, and such that its partial transposes with respect to all possible bipartitions have also a maximal rank, admits an infinite number of optimal separable decompositions, such that any symmetric product state of the system is part of an optimal separable decomposition of ρ_S. For symmetric states of 4 qubits, we presented a counterexample showing that any symmetric product state is not necessarily part of an optimal separable decomposition of a mixed state with such maximal rank properties.

In Chapter 5, we studied the entanglement quantification of symmetric multiqubit states within SLOCC classes. Exploiting the link between det-1 invariant homogeneous positive functions and entanglement monotones, we proposed an homogeneous function invariant under symmetric det-1 local operations to quantify entanglement in the symmetric subspace of the SLOCC classes belonging to the entanglement family $\mathcal{D}_{1,\ldots,1}$. We showed that this function depends only on the Euclidean distances between all pairs of Majorana points representing a symmetric state on the Bloch sphere, which illustrates the

relationship between the geometric configuration of the Majorana points of a symmetric state and its amount of entanglement. We finally related the maximization of this entanglement monotone to a longstanding mathematical and physical problem that consists in minimizing the energy, for a given potential, of particles constrained onto the surface of a sphere.

In Chapter 6, we studied the robustness of entanglement against particle loss of multipartite entangled states. We first characterized multiqubit entangled states that are fragile for the loss of a given qubit and gave a canonical form for any state having this fragility property. We then extended our characterization to entangled states that are fragile for the loss of any one of their qubits and also treated the most general case of the fragility for the loss of any qubit among a given subset of the qubits. We also found a canonical form for the states that present this general form of fragility for the loss of one qubit. Unfortunately, we showed that the lack of general results about the length of separable states with given rank prevents us from extending our results for multiqudit systems. We could nevertheless give a canonical form of fragility for the loss of a given qubit for generic multiqutrit states. We then focused on the entanglement robustness properties of symmetric multiqubit states. We showed that all the symmetric states that are fragile for the loss of one qubit are SLOCC-equivalent and in particular SLOCC-equivalent to the state $|\mathrm{GHZ}\rangle$. We showed however that for the loss of at least two qubits, symmetric fragile states are not necessarily SLOCC-equivalent. We also found SLOCC classes of N-qubit symmetric states in which all the states are robust for the loss of any number of their qubits, between 1 and $N-2$.

Bibliography

[1] E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] J. S. Bell, Physics **1**, 195 (1964).

[4] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982).

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers Systems and Signal Processing **175**, 8 (1984).

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[8] R. Jozsa and N. Linden, Proc. R. Soc. Lond. A **459**, 2011 (2003).

[9] A. S. Sørensen and K. Mølmer, Phys. Rev. Lett. **86**, 4431 (2001).

[10] G. Tóth, Phys. Rev. A **85**, 022322 (2012).

[11] A. F. Abouraddy, B. E. Saleh, A. V. Sergienko, and M. C. Teich, Phys. Rev. Lett. **87**, 123602 (2001).

[12] W. Wieczorek, R. Krischek, N. Kiesel, Ch. Schmid, and H. Weinfurter, Proc. SPIE 7608, Quantum Sensing and Nanophotonic Devices VII, 76080P (2010).

[13] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).

[14] D. Gross, S. T. Flammia, and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).

[15] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[16] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[17] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2000).

[18] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

[19] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).

[20] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[21] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).

[22] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[23] R. H. Dicke, Phys. Rev. **93**, 99 (1954).

[24] E. Majorana, Il Nuovo Cimento **9**, 43 (1932).

[25] T. Bastin, S. Krins, P. Mathonet, M. Godefroid, L. Lamata, and E. Solano, Phys. Rev. Lett. **103**, 070503 (2009).

[26] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[27] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[28] M. Horodecki, P. Horodecki, and Horodecki R., Open Syst. Inf. Dyn. **13**, 103 (2006).

[29] P. Wocjan and M. Horodecki, Open Syst. Inf. Dyn. **12**, 331 (2005).

[30] M. Seevinck and J. Uffink, Phys. Rev. A **78**, 032101 (2008).

[31] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[32] B. M. Terhal, J. Theor. Comp. Science **287**, 313 (2002).

[33] O. Gühne and G. Tóth, Phys. Rep. **474**, 1–75 (2009).

[34] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998).

[35] P. Mathonet, S. Krins, M. Godefroid, L. Lamata, E. Solano, and T. Bastin, Phys. Rev. A **81**, 052315 (2010).

[36] P. Migdał, J. Rodriguez-Laguna, and M. Lewenstein, Phys. Rev. A **88**, 012335 (2013).

[37] M. B. Plenio and S. Virmani, Quant. Inf. Comput. **7**, 1 (2007).

[38] A. Neven, P. Mathonet, O. Gühne, and T. Bastin, Phys. Rev. A **94**, 052332 (2016).

[39] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[40] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[41] D. J. C. Bures, Trans. Am. Math. Soc. **135**, 199 (1969).

[42] M. Hübner, Phys. Lett. A **163**, 239 (1992); **179**, 226 (1993).

[43] T.-C. Wei and P. M. Goldbart, Phys. Rev. A **68**, 042307 (2003).

[44] S. Niekamp, M. Kleinmann, and O. Gühne, Phys. Rev. A **82**, 022322 (2010).

[45] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. A **87**, 040401 (2001).

[46] Y. Huang, New J. Phys. **16**, 033027 (2014).

[47] R. Hübener, M. Kleinmann, T.-C. Wei, C. González-Guillén, and O. Gühne, Phys. Rev. A **80**, 032324 (2009).

[48] R. A. Horn and C. R. Johnson, *Matrix analysis*, second ed., Cambridge University Press, New York (2013).

[49] P. Horodecki, Phys. Lett. A **232**, 333–339 (1997).

[50] O. Rudolph, Quantum Inf. Proc. **4**, 219 (2005).

[51] K. Chen and L.-A. Wu, Quantum Inf. Comp. **3**, 193 (2003).

[52] O. Rudolph, Phys. Rev. A **67**, 032312 (2003).

[53] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[54] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[55] K. Audenaert, F. Verstraete, and B. De Moor, Phys. Rev. A **64**, 052304 (2001).

[56] C.-S. Yu and H.-S. Song, Phys. Rev. A **73**, 022325 (2006).

[57] P. Badziąg, P. Deuar, M. Horodecki, P. Horodecki, and R. Horodecki, J. Mod. Opt. **49**, 1289 (2002).

[58] J. T. Barreiro *et al.*, Nature Physics **6**, 943946 (2010).

[59] M. Guţă, T. Kypraios, and I. Dryden, New J. Phys. **14**, 105002 (2012).

[60] A. Neven and T. Bastin, J. Phys. A: Math. Theor. **51**, 315305 (2018).

[61] J. J. Sakurai, *Modern quantum mechanics*, revised ed., edited by San Fu Tuan (1994).

[62] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).

[63] J. Gillet, *Contribution to entanglement theory, applications in atomic systems and cavity QED*, Ph.D. thesis, Université de Liège (2011).

[64] T.G. Kolda and B.W. Bader, SIAM Rev. **51**, 455–500 (2009).

[65] R. C. Thompson, Linear Algebr. Appl. **26**, 65 (1979).

[66] A. Uhlmann, Open Syst. Inf. Dyn. **5**, 209–227 (1998).

[67] Yu. A. Al'pin and Kh. D. Ikramov, Dokl. Akad. Nauk **437**, 7–8 (2011) (in Russian) transl. in Dokl. Math. **83** 141–142 (2011).

[68] T. G. Gerasimova, R. A. Horn, and V. V. Sergeichuk, Linear Algebra Appl. **438**, 3829–3835 (2013).

[69] F. D. Murnaghan, *The unitary and rotation groups*, Spartan Books, Washington, D.C. (1962).

[70] L. Chen and D. Đoković, J. Phys. A: Math. Theor. **46**, 275304 (2013).

[71] E. Alfsen and F. Shultz, J. Math. Phys. **51**, 052201 (2010).

[72] K.-C. Ha and S.-H. Kye, J. Phys. A: Math. Theor. **48**, 045303 (2015).

[73] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).

[74] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[75] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, Phys. Rev. A **63**, 044304 (2001).

[76] P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 032310 (2000).

[77] R. Augusiak, J. Tura, J. Samsonowicz, and M. Lewenstein, Phys. Rev. A **86**, 042316 (2012).

[78] K. Eckert, J. Schliemann, D. Bruß, and M. Lewenstein, Ann. Physics **299**, 88–127 (2002).

[79] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[80] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).

[81] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

[82] J. Martin, O. Giraud, P. A. Braun, D. Braun, and T. Bastin, Phys. Rev. A **81**, 062347 (2010).

[83] M. Aulbach, D. Markham, and M. Murao, New J. Phys **12**, 073025 (2010).

[84] C. Eltschka, T. Bastin, A. Osterloh, and J. Siewert, Phys. Rev. A **85**, 022301 (2012).

[85] D. Markham, Phys. Rev. A **83**, 042332 (2011).

[86] E. B. Saff and A. B. J. Kuijlaars, Math. Intelligencer **19**, 5 (1997).

[87] J. J. Thompson, Philosophical Magazine **7**, 237 (1904).

[88] R. M. L. Tammes, Rec. Trv. Bot. Neerl. **27**, 1 (1930).

[89] C. Beltrán, *The Sate of the Art in Smale's 7th Problem*, in *Foundations of Computational Mathematics, Budapest 2011* (London Mathematical Society Lecture Note Series), Cambridge University Press, UK (2011).

[90] P Ribeiro and R. Mosseri, Phys. Rev. Lett. **106**, 180502 (2011).

[91] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, UK (2000).

[92] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Bell's theorem, quantum theory, and conceptions of the universe*, Ed. M. Kafatos, Kluwer, Dordrecht, pp. 69-72 (1989).

[93] M. Koashi, V. Bužek, and N. Imoto, Phys. Rev. A **62**, 050302(R) (2000).

[94] A. K. Rajagopal and R. W. Rendell, Phys. Rev. A **65**, 032328 (2002).

[95] W. Dür, Phys. Rev. A **63**, 020303(R) (2001).

[96] J. K. Stockton, J. M. Geremia, A. C. Doherty, and H. Mabuchi, Phys. Rev. A **67**, 022112 (2003).

[97] A. Neven, J. Martin, and T. Bastin, preprint arXiv:1809.00622.

[98] G. Marsaglia, Ann. Math. Statist. **43**, 645 (1972).

[99] D. Baguette, F. Damanet, O. Giraud, and J. Martin, Phys. Rev. A **92**, 052333 (2015).

[100] D. Baguette, T. Bastin, and J. Martin, Phys. Rev. A **90**, 032314 (2014).

[101] X. Wang and K. Mølmer, Eur. Phys. J. D **18**, 385 (2002).

[102] V. M. Kendon, K. Nemoto, and W. J. Munro, J. Mod. Opt. **49**, 1709 (2002).

[103] V. M. Kendon, K. Życzkowski, and W. J. Munro, Phys. Rev. A **66**, 062310 (2002).

[104] G. Aubrun, S. J. Szarek, and D. Ye, Comm. Pure Appl. Math. **67**, 129 (2014).

Development of new tools to detect, characterize and quantify quantum entanglement in multipartite systems

Antoine Neven

Abstract: Quantum entanglement is a key property of quantum information theory, that is at the heart of numerous promising applications in fields such as quantum cryptography, quantum computing or quantum sensing. In the past decades, the advent of such innovative technologies has reinforced the need for a better understanding of entanglement. The aim of this thesis is to contribute to this effort through the development of new tools targeting the characterization of several features of entanglement. Concerning the issue of entanglement detection, we present an optimization of the approach that exploits the concept of generalized concurrences to solve the separability problem for pure states. We then reformulate the separability question of mixed states into a matrix analysis problem, from which we obtain general separability criteria for multipartite states of ranks two and three. We also briefly discuss some properties of separable states. In particular, we characterize optimal separable decompositions of symmetric (i.e. permutation invariant) states of two and three qubits with maximal rank properties. Regarding the quantification of entanglement, we propose a function to quantify the entanglement of symmetric multiqubit states within classes of entangled states gathering states that are stochastically equivalent through local operations assisted with classical communication. This function establishes a link between the amount of entanglement of a symmetric state and the distribution of its Majorana points on the Bloch sphere. We finally investigate the robustness of entanglement with respect to particle loss and provide a full description of all multiqubit states that are fragile for the loss of one of their qubits. For symmetric states, the fragility for the loss of one qubit is shown to be related to a particular symmetry of the Majorana points.