University of Calgary

PRISM Repository | https://prism.ucalgary.ca

The Vault | Open Theses and Dissertations

2013-04-09

Quantifying The Asymmetry Properties Of Quantum Mechanical Systems Using Entanglement Monotones

Toloui Semnani, Borzumehr

Toloui Semnani, B. (2013). Quantifying The Asymmetry Properties Of Quantum Mechanical Systems Using Entanglement Monotones (Doctoral thesis, University of Calgary, Calgary, Canada). Retrieved from https://prism.ucalgary.ca. doi:10.11575/PRISM/27501

http://hdl.handle.net/11023/591

Downloaded from PRISM Repository, University of Calgary

UNIVERSITY OF CALGARY

Quantifying The Asymmetry Properties Of Quantum Mechanical Systems Using Entanglement Monotones

by

Borzumehr Toloui Semnani

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

March, 2013

© Borzumehr Toloui Semnani 2013

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled “Quantifying The Asymmetry Properties Of Quantum Mechanical Systems Using Entanglement Monotones” submitted by Borzumehr Toloui Semnani in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY.

Supervisor, Dr. Gilad Gour
Department of Mathematics and Statistics

Dr. Renate Scheidler
Department of Mathematics and Statistics

Co-supervisor, Dr. Barry C. Sanders
Department of Physics and Astronomy

Dr. Clifton L. R. Cunningham
Department of Mathematics and Statistics

Dr. David L. Feder
Department of Physics and Astronomy

Dr. Michele Mosca
Department of Combinatorics and Optimization
University of Waterloo

Date

Abstract

Dynamical symmetries in closed systems lead to conservation laws and to selection rules that are based on those conservation laws. However, conservation laws are not applicable to open systems that undergo irreversible transformations. More general selection rules are needed to determine whether, given two states, the transition from one state to the other is possible. Characterizing the asymmetry properties of quantum states using quantum information theoretical tools and methods is particularly fruitful for this purpose.

This thesis is concerned with the problem of finding new general selection rules that hold for both open and closed systems. The usual approach to this problem relies heavily on group theory and involves a detailed study of the structure of the symmetry group. In this thesis, we approach the problem in a completely new way. Our approach is to use entanglement to investigate the asymmetry properties of quantum states. In order to do that, we embed the system's Hilbert space in a larger tensor product Hilbert space, whereby all symmetric states are mapped to separable states, asymmetric states are mapped to entangled states, and the symmetric transformations between two states are replaced by local operations on their bipartite images.

Our method is not restricted to only a specific group but applies, in general, to all symmetries that are associated with semi-simple compact Lie groups and their associated Lie algebras. The mapping of the original states to bipartite states that act on the larger Hilbert space enables us to use the well studied theory of entanglement to investigate the consequences of dynamic symmetries. For example, the monotonicity condition on measures of entanglement provide us with new selection rules. Under reversible transformations, the entanglement of the bipartite image states becomes a conserved quantity. These entanglement-based conserved quantities are new and different from the conserved

quantities based on expectation values of the Hamiltonian symmetry generators.

Acknowledgements

I would like to thank my supervisor, Dr. Gilad Gour, and my co-supervisor, Dr. Barry C. Sanders , for all their help and support. I've learned a lot from them and I am grateful for their support and guidance. Working with them has been both a great privilege and a great pleasure.

I have also been very fortunate to work with and learn from Dr. Damian Markham and his team at CNRS - Télécom ParisTech. I also like to thank the Collaborative student training in Quantum Information Processing project, the EU-Canada Programme for Cooperation in Higher Education, Training and Youth, Université Paris-Sud and the Institute for Quantum Information Science (IQIS) for making the visit to France possible.

Special thanks goes to my colleagues and collaborators, Michael Skotiniotis, Varun Narasimhachar, Iman Marvian, Vlad Gheorghiu, Yuval Sanders, Ben Fortescue and Alexander Hentschel. I am grateful to Dr. Robert W. Spekkens and Dr. Peter Turner, Dr. Aidan Roy and Dr. Eleni Diamanti for all that I have learned from them.

The Institute for Quantum Information Science and the department of Physics and Astronomy at the University of Calgary provided valuable assistance throughout the course of my degree, for which I am appreciative. In particular, I thank Lucia Wang, Nancy Lu and Tracy Korsgaard.

I would also like to acknowledge Alberta Innovates, the Natural Sciences and Engineering Research Council, General Dynamics Canada, and the Canadian Centre of Excellence for Mathematics of Information Technology and Complex Systems (MITACS) for their support.

Most importantly, I would like to thank my family, my mother, father, my sister Moujan, my dear late grandmother Azardokht Kamkar and my aunt Mahgooneh Ghahraman, and specially my little niece Anousha.

Finally, I dedicate this work to the memory of my dear dear grandmother, Azardokht Kamkar, who although no longer with us, will continue to live in my heart until the end.

Table of Contents

Approval Page . . . ii
Abstract . . . iii
Acknowledgements . . . v
Table of Contents . . . vii
List of Figures . . . ix
1 Introduction . . . 1
1.1 Background and motivation . . . 1
1.2 Symmetry in physics . . . 4
1.2.1 Symmetry and reference frames . . . 6
1.2.2 Superselection rules . . . 9
1.3 An overview of resource theories . . . 12
1.3.1 Entanglement as a resource . . . 15
1.4 The resource theoretic approach to the study of dynamical symmetries . . . 18
1.5 A review of previous work . . . 24
1.6 The original contributions of the thesis . . . 29
2 Preliminaries . . . 32
2.1 Group representation theory . . . 32
2.1.1 Group-invariant measures and group averages . . . 34
2.1.2 Representations of groups and algebras . . . 36
2.2 Symmetric transformations . . . 44
2.2.1 The collective representation . . . 47
2.3 Entanglement as a quantum resource . . . 49
2.3.1 Composite systems . . . 49
2.3.2 Quantum operations . . . 50
2.3.3 Generalized measurements and POVMs . . . 51
2.3.4 Local operations with classical communication (LOCC) . . . 53
2.3.5 Pure state entanglement . . . 53
2.4 Monotones in resource theories . . . 57
3 Constructing monotones for quantum phase references in totally dephasing channels . . . 62
3.1 Covariant transformations for the symmetry group U(1) and the lack of shared phase references . . . 63
3.1.1 U(1)-asymmetry and phase references . . . 64
3.2 Pure-state monotones . . . 67
3.3 Mapping to bipartite states . . . 71
3.4 Applications . . . 75
3.4.1 Frameness of formation . . . 82
3.4.2 Explicit concurrence of frameness and U(1)-asymmetry of formation of a qubit . . . 85
4 Simulating symmetric transformations with local operations . . . 87

4.1 Simulating G-covariant transformations 90
4.1.1 The main isometry 91
4.1.2 A complete set of LOCC-simulating isometries 95
4.2 Constructing Asymmetry Monotones From Entanglement Monotones . . 99
4.2.1 Unitary Transformation 101
5 Applications and examples 102
5.1 The pure-state standard form 102
5.2 Entanglement-based asymmetry monotones 104
5.2.1 The negativity of entanglement as a measure of asymmetry 104
5.3 Measures based on distance 105
5.3.1 The Relative Entropy of Asymmetry 107
5.3.2 Comparison with G-asymmetry 107
5.4 Case study: Entanglement-based asymmetry monotones versus information-based asymmetry measures 110
5.5 Case study: Vidal monotones and inequivalent pure-state asymmetry resources 112
5.6 Case study: Bounds on G-covariant state discrimination 114
6 Other entanglement-based selection rules and conservation laws 117
6.1 $\mathcal{L}$ is not a LOCC-simulating isometry 118
6.2 Necessary conditions for the manipulation of asymmetric states 119
6.3 Conserved quantities 123
7 Concluding Remarks 127
7.1 Summary of results 127
7.2 Discussion 128
7.3 Open Questions and future Work 132
A The generalized Wigner-Eckart theorem 135
A.0.1 The Set of Isometries $\{\mathcal{C}_g\}$ 135
A.0.2 The Isometry $\mathcal{L}$ 136
B Abelian Lie groups 139
Bibliography 142

List of Figures

1.1 The state of the system and the physical reference frame can be expressed relative to an external idealized frame and then averaged over all possible alignments of the external reference frame. 7

1.2 Teleportation of a qubit can be regarded as a conversion of one ebit of entanglement, which is a static noiseless quantum resource, into a noiseless quantum channel, which is a dynamic noiseless quantum resource [34]. . . 13

1.3 Superdense coding can be regarded as a conversion of one ebit of entanglement, which is a static noiseless quantum resource, to a noiseless classical channel, which is a dynamic noiseless classical resource capable of transmitting to 2 cbits or classical bits [34]. 14

1.4 Alice can include a non-invariant state with the target state through the channel. The relational degrees of freedom are not affected by the effective decoherence in the channel. Bob performs a joint operation on the two states that he receives and recovers the original target state aligned with his reference frame. 22

1.5 Simulating a covariant transformation $\mathcal{E}_{\rm cov}$ by a LOCC transformation $\tilde{\mathcal{E}}_{\rm local}$. 30

2.1 G-covariant transformations are those transformations $\mathcal{E}$ such that $U(g)\mathcal{E}(\rho)U^\dagger(g) = \mathcal{E}\left(U(g)\rho U^\dagger(g)\right)$. 45

4.1 Simulating a covariant transformation $\mathcal{E}_{\rm cov}$ by a LOCC transformation $\tilde{\mathcal{E}}_{\rm local}$. 87

5.1 A schematic depiction of the space of bipartite states. SEP_s is the intersection of the set of separable states, SEP, with the image of the $\mathcal{C}_s$-isometry denoted here as $\mathcal{C}_s[\mathscr{H}]$. The image of the set of G-invariant states under $\mathcal{C}_s$, denoted as $\mathcal{C}_s[\text{INV}]$, is a strict subset of SEP_s. 108

Chapter 1

Introduction

1.1 Background and motivation

Symmetries arise in all contexts and all facets of life. They are essential to aesthetics, art and mathematics. Symmetry also plays an important role in physics. Some of the deepest results in physics are linked to symmetries in nature [87]. For example, arguments based on symmetries of space and time play a vital role in development of the theory of special relativity [73, 87]. The exact solutions to Einstein's field equations of general relativity also use space-time symmetries extensively [73]. Symmetries are also effectively employed in high energy physics, especially the symmetry associated with the group SU(3) that is at the heart of the Standard Model [26]. Supersymmetry, an extension of the symmetries of standard quantum field theories, forms the basis of the efforts to unify quantum mechanics and general relativity [17, 27].

Recognizing the symmetries of a given situation, together with the dynamical consequences that follow from them, is an important step towards a full understanding of the problem and its eventual solution. In many situations where the detailed dynamical laws are not yet discovered, studying the symmetries usually provides the first clues to a deeper and more detailed understanding of the phenomenon. The discovery of the details of the respective dynamical law usually comes only afterwards.

Even in cases where the laws are in principle known, taking advantage of the existing symmetries can immensely simplify the calculations involved. In many cases, it can even render an otherwise computationally intractable task feasible [25, 56, 72, 112]. The fact is that the evolution of most quantum systems is simply too complicated to be solved analytically or even to be simulated numerically in an efficient way, at least in the absence of powerful quantum computers [22,28,52,56,72,83,106,112,113]. Many realistic situations involve either open dynamical systems, or closed systems with Hamiltonians that contain numerous parameters, so that determining how they vary with time is at the present time not computationally tractable [28, 56, 64, 83, 106, 108, 113]. In all such cases, symmetry-based approaches are powerful substitutes for actual detailed analysis of the complex dynamics involved.

A key result concerning dynamical symmetries is the theorem by Emmy Noether that relates the underlying symmetries to conservation laws and to respective conserved quantities [68, 69, 107]. Noether's theorem plays a central role in the study of dynamical symmetries of closed systems in classical mechanics [69]. Equivalent theorems in quantum mechanics play a similarly important role. The classical theorem, as well as its quantum-mechanical counterparts, states that a closed system undergoing reversible and symmetric time evolution is always accompanied by a corresponding conservation law [107].

In quantum mechanics, in particular, this conclusion is straightforward. A symmetric Hamiltonian implies that the expectation value of the operators that represent the generators of the symmetry group are conserved quantities. Yet, closed systems undergoing reversible time evolution are not the most general case appearing in nature. The detailed state of the environment and its interactions with the system under study cannot always be accounted for. Hence, the more general case must also involve open systems and irreversible transformations. In fact, open systems are far more ubiquitous than closed systems. The time evolution of open systems, even when the dynamics satisfies a symmetry, can be very different from the unitary evolution governed by symmetry preserving Hamiltonians. Generally, no conserved quantities are associated with symmetric dynamics of open systems, and thus, the consequences of dynamical symmetries cannot always be reduced to selection rules based on conservation laws [60]. In fact, it was realized recently that even for closed systems, the conservation laws that arise from the quantum mechanical equivalents of Noether's theorem do not capture all the consequences of the symmetry in question [59, 61]. It is therefore necessary to look beyond conservation laws in order to determine how states evolve under symmetric dynamics.

The goal of the present thesis is to find new and more general conditions for deciding when transitions between states are possible, assuming that the dynamical evolution satisfies a symmetry associated with a semi-simple compact Lie group. We refer to such conditions as selection rules. The key idea in our approach involves embedding the system within a larger space comprised of two-party states. We show that symmetric time evolutions can be regarded as a strict subset of local operations. This, in turn, enables us to directly apply the theory of quantum entanglement to the problem of symmetric dynamics. We introduce new selection rules derived from entanglement theory, and in particular, we show how entanglement measures can act as conserved quantities for reversible temporal evolutions. This leads to new conservation laws emerging out of entanglement theory. Our results are reported in two published papers [85, 86].

As an introduction, we first provide a background review of symmetries in physics in Section 1.2. In Section 1.3, we discuss the general features of resource theories as studied in the field of quantum information science. Then, we present an overview of entanglement as a quantum informational resource in Section 1.3.1. We also present the study of dynamical symmetry from the point of view of resource theories in Section 1.4. We present a short review of the relevant literature in Section 1.5. Finally, in Section 1.6, we outline, in more detail, our original contributions to the study of asymmetry and its significance.

1.2 Symmetry in physics

By symmetry, we mean invariance under a set of transformations [102]. The subject of symmetry can be a physical system, the state of a physical system, the Hamiltonian, or in general, the dynamical laws under which a system evolves. When the symmetry belongs to the dynamical evolution of the system, it is referred to as dynamical symmetry. In any case, the transformations that leave the respective structure unchanged form a group. Thus, every symmetry is identified with a group of transformations, or more specifically, by a representation of that group. We denote the symmetry group as G for the rest of the thesis.

Nature exhibits various symmetries that are reflected in the laws of physics. Symmetries that the laws of physics preserve include spatial-translation symmetry, time-displacement symmetry, rotational symmetry and boost symmetry. Together, they form the Galilei group of continuous transformations in the non-relativistic regime or the Poincaré group in the relativistic regime.

Besides the continuous symmetries, there are also discrete symmetries. The main discrete transformations in physics include space inversion (parity flip, P), momentum inversion (time reversal, T) and inversion of charge or baryon number (charge conjugation, C). Today, we realize that the discrete symmetries are not individually respected in nature. So far as we know, nature is always invariant under combinations of the three, known as the CPT transformation. In other words, all Hamiltonians are believed to remain invariant under the combination CPT, but need not remain invariant under each individual discrete transformation [82].

Classically, the evolution of a closed system can be expressed in terms of an action functional defined as the time integral of the system's Lagrangian function. The laws of motion can be derived from minimizing the system's action, known as the principle of least action. Noether's first theorem deals with actions that satisfy a differentiable symmetry and vanish on the boundary of the region of space-time over which the Lagrangian is being integrated. In such cases, the theorem states that a function of the system's parameters exist that remains conserved throughout the time period during which the system's evolution is determined by that action [68, 69].

In classical mechanics, an alternative description of closed system dynamics is in terms of the system's Hamiltonian and the Poisson brackets. The Hamiltonian H is a function of position, q, and momentum, p. In the Hamiltonian framework, Noether's theorem is straightforward: To every continuous symmetry of a Hamiltonian system, there corresponds a conserved quantity. By a continuous symmetry of a Hamiltonian, we mean a vector field that generates a one-parameter family of transformations that preserve the Hamiltonian under the Poisson brackets [15].

In quantum mechanics, the dynamics of a closed system undergoing a reversible transformation is described by a Hamiltonian operator, and the role of the Poisson bracket is replaced with the commutator of operators. In the presence of a symmetry associated with the group G, the Hamiltonian commutes with the group action, *i.e.* with every element of the representation of the group carried by the system's Hilbert space. For example, a Hamiltonian with rotational symmetry commutes with every rotation operator representing an element of the group $SO(3)$. In the general case of an open system interacting with the environment, no Hamiltonian can be attributed to the system alone. Only the joint system comprised of the original open system together with the environment can be regarded as an isolated closed system with a well-defined Hamiltonian. The dynamics of the system alone is determined by tracing out the terms associated with the environment from the Hamiltonian. In the absence of prior entanglement between the system and the environment, *i.e.* when the environment carries no prior memory of the system, the resulting transformation is, in general, a trace preserving completely positive (CP)-map. The symmetric time evolution of an open system implies that the CP-map describing the evolution of the system must commute with the representation of the group. Such a map is known as a G-covariant map [8].

1.2.1 Symmetry and reference frames

Symmetry in physics is closely linked to the notion of reference frames. Reference frames are usually treated as idealized frameworks external to the system under study. Ideal reference frames do not undergo any temporal dynamical evolution. However, in practice, all reference frames are in fact physical systems. A physical system acts as a reference frame for some physical degree of freedom, like the angular momentum, if its states, associated with different values of that degree of freedom, are distinct and distinguishable, in the sense that a measurement exists whose outcomes distinguish the different states. Thus, a frame of reference is a system with an inherent asymmetry with respect to a particular set of transformations, such as rotations in space. Also, one must be able to jointly measure the state of the reference frame together with a given system in order to determine the value of the respective degree of freedom for that given system.

In classical systems, distinct states are automatically completely distinguishable. Hence, a classical system whose states remain distinct, and is stable during the dynamical evolution of the system under study, is a good approximation to the idealized external reference frame. For example, solid rods are usually envisioned as physical substitutes for a coordinate axis, albeit one of bounded size. A sphere, on the other hand, does not qualify as such because it is rotationally symmetric. Its states with respect to different angles of rotation are completely indistinguishable.

In quantum theory, distinct states are not necessarily fully distinguishable. Fully distinguishable states are only those that are mutually orthogonal. For degrees of freedom that transform under continuous groups, the states of a perfect reference frame, in the

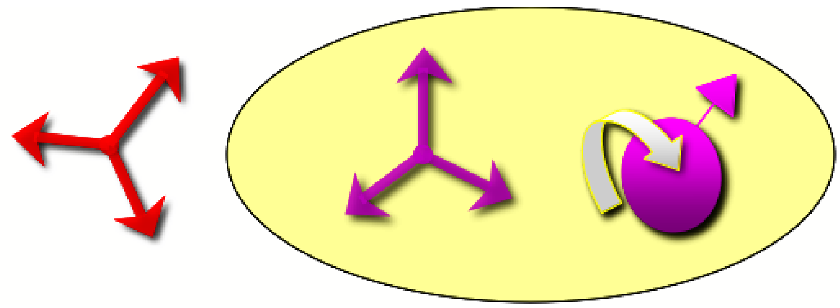

Figure 1.1: The state of the system and the physical reference frame can be expressed relative to an external idealized frame and then averaged over all possible alignments of the external reference frame.

above sense, must therefore act on an infinite-dimensional Hilbert space. The dimension of the Hilbert space on which the states of a system act is a good candidate for the "size" of the quantum system. Hence, in the case of continuous groups, no system of finite size can be a perfect reference frame [9]. Unlike the classical case, the finite size of the reference frame in the quantum regime leads directly to a lack of complete distinguishability of the reference states as the Lie group has infinitely many members, and introduces errors even within the finite range of the reference frame's applicability. More importantly, a quantum reference frame must interact with the system under study, and must ultimately be measured jointly with that system when the respective degree of freedom of the system is measured. Therefore an efficient finite-sized quantum reference frame has inevitably a limited lifespan [6].

Once we treat the reference frame as a physical system with its own dynamics, it must be possible to express the joint state of a system $\mathcal{S}$ with the reference frame $\mathcal{R}$ solely in terms of their relative internal degrees of freedom without referring to any other system [9]. The dynamic system acting as a reference frame in this description is also known as an internalized reference frame, or, alternatively and more succinctly, an internal reference frame [8, 9].

As the reference frame is now internalized and must be assigned a state, we need yet another external reference frame in the background relative to whose alignment the state of the reference system can be determined (see Figure 1.1). On the other hand, as said before, we want ultimately to be able to describe the relative state of the system and the internal reference frame without having to refer to any specific alignment of the background frame. To this end, we first describe their joint state relative to the frame in the background, and then average uniformly over all possible alignments of the background frame (see Figure 1.1). The uniform averaging is a reflection of a complete lack of knowledge of the actual relative alignment of the internal and the background reference frames, so that all alignments are equally likely. If some alignments are more likely than others, then the uniform averaging is replaced with a weighted averaging with more likely alignments having higher weights associated with them than the less likely ones [8, 9].

Let ρ_S denote the state of the system $\mathcal{S}$ relative to the external reference frame and σ_R denote the state of the quantum system acting as the internal reference frame[1]. The passive transformation of the external reference frame is equivalent to an active transformation of the joint state $\rho_S \otimes \sigma_R$ via a representation of the symmetry group $U_S \otimes U_R$, where U_S is a unitary representation carried by the Hilbert spaces of system $\mathcal{S}$, and U_R is a unitary representation carried by the Hilbert spaces of system $\mathcal{R}$. The averaging over the alignments of the external reference frame is known as 'twirling' or the 'twirling operation' [8, 9]

Let us denote the averaging with the superoperator $\mathcal{G}$, known as the twirling super-

[1]In Chapter 2, we will go through in more detail the technical definitions of the concepts used in the present chapter. However, the technical subtleties are not necessary to follow the line of arguments presented in this chapter.

operator:

$$\mathcal{G}\left(\rho_S \otimes \sigma_R\right) = \int \mathrm{d}\mu_g \, U_S(g)\rho_S U_S^\dagger(g) \, \otimes \, U_R(g)\sigma_R U_R^\dagger(g), \tag{1.1}$$

where the integration is done uniformly over the group with $\mathrm{d}\mu_g$ denoting the group-invariant (Haar) measure[2].

The twirling operation destroys coherence between certain subspaces of the Hilbert space $\mathscr{H}$ of the joint systems and imposes a direct sum structure on the Hilbert space,

$$\mathscr{H} = \bigoplus_q \mathscr{H}_q, \tag{1.2}$$

where $\mathscr{H}_q$ are so-called 'charge' sectors, labelled by the index q, each carrying an inequivalent representation of G. Moreover, the index q is a conserved quantity under the corresponding symmetry. For example, the group $SO(3)$ of spatial rotations is usually parametrized by two angles. Similarly, in order to include the spin degrees of freedom as well, we can consider the group $SU(2)$ (with the same algebra) instead. In this case, the parameter q in (1.2) labels the total angular momentum of the system. Physically, the above mathematical structure is equivalent to a "superselection rule" (SSR) [8]. We now briefly go over the notion of a superselection rule and its historical development.

1.2.2 Superselection rules

Historically, superselection rules were introduced as new extra axioms laying out additional overall restrictions on the laws of quantum mechanics [105]. Previously, it was posited that there exists a one-to-one correspondence between all Hermitian operators on the one hand, and the physical observables of measurable quantities on the other [98]. The new axioms limited the quantum observables to a strict subset of all Hermitian operators. In particular, they stated that some observables in quantum mechanics, like

[2] For a more detailed discussion of Haar measures and the twirling operation see Sections 2.1.1 and 2.2 respectively.

charge, boson number or parity, must satisfy superselection rules, *i.e.* their observables must have a direct sum structure [105].

Superselection rules were initially understood as arising due to an overall symmetry in the laws of nature. Not only does the particular Hamiltonian of a system commute with the superselected observable (and the symmetry transformations associated with that observable's degree of freedom), but *all* other observables of the system have to commute with the superselected observable as well and remain invariant under the respective symmetry transformations. This, in turn, implies that for any observable O, the cross term $\langle e_i|O|e_j\rangle = 0$, where $|e_n\rangle$ denotes the eigenstates of the superselected observable A, and where $|e_i\rangle$ and $|e_j\rangle$ are assumed to have *different* eigenvalues. The line of reasoning is as follows: $\langle e_i|OA|e_j\rangle = \langle e_i|AO|e_j\rangle$, and thus $e_j \langle e_i|O|e_j\rangle = e_i^* \langle e_i|O|e_j\rangle$. It follows that $\langle e_i|O|e_j\rangle = 0$, as $e_i \neq e_j$ by assumption.

A "selection rule" determines when the cross terms of a given Hamiltonian H of a system vanishes between two states, $\langle e_i|H|e_j\rangle = 0$, due to that Hamiltonian's particular symmetry. The terminology for a "superselection" rule was thus chosen for the cases where the cross terms of not only the Hamiltonian but every other observable O of the system vanish between two such states, $\langle e_i|O|e_j\rangle = 0$.

Consequently, no physical observable can distinguish between coherent superpositions of the form

$|\psi_\omega\rangle = c_1|e_i\rangle + e^{\imath\omega}c_2|e_j\rangle$, $c_1, c_2 \in \mathbb{C}^+$, for different phases ω, as

$$\langle\psi_\omega|O|\psi_\omega\rangle = |c_1|^2\langle e_i|O|e_i\rangle + |c_2|^2\langle e_j|O|e_j\rangle \tag{1.3}$$

is independent of the phase ω. Similarly, for a mixed state, the cross terms between different basis elements $|e_i\rangle$ vanish in the average $\mathrm{Tr}(O\rho)$ for all observables O. Hence, the interference between different eigenstates of the superselected observable cannot be observed. The situation is, in effect, indistinguishable from the case where states cannot be prepared in coherent superpositions of this form to begin with, which brings us back to the imposed direct-sum structure on the Hilbert space.

The discussion of quantum reference frames in the previous section relates the existence of a superselection rule of an observable to the availability of a suitable reference frame. It implies that superselection rules need not be regarded as axiomatic. Rather, whenever a suitable reference frame for a degree of freedom is hard to come by, an effective superselection rule is in place, whereas degrees of freedom for which many suitable reference frames are naturally formed, or are easily prepared, are not bound by any superselection rules. For example, many objects around us break the rotational symmetry to some extent, and thus can act as Cartesian frames or, at least, as direction indicators. On the other hand, preparing a Bose-Einstein condensate, that can act as a reference frame for the phase associated with particle number, or a superconductor that can be the reference frame for the phase associated with charge number [1], need forming environments with very low temperatures, among other things, and the knowledge to engineer the right circumstances. Consequently, total particle numbers and total charge numbers appear to come naturally with a superselection rule. This possibility was first recognized by Aharonov and Susskind for the charge superselection rule [1]. In later years, a similar observation in the context of quantum optics helped resolve the controversy about whether coherent optical states do in fact exist or are merely suitable fictions [66]. It was realized that the state of an optical system can be treated correctly either as a coherent superposition or an incoherent mixture of different photon-number eigenstates, depending respectively on whether or not it is expressed relative to a background phase reference [7,76]. For a historical account and a more detailed exposition of the controversy see Section 1.5.

What is most relevant to our work is that the superselection rule specifies the general form of restrictions that are imposed by the dynamical symmetry on quantum transformations, or equivalently, on the system's temporal evolution. The symmetry group characterizing the dynamical symmetry is identified with the group of transformations of the reference frame, whose absence is what leads to the superselection rule.

1.3 An overview of resource theories

A resource is anything that enables the performance of a task or allows one to perform the task better or easier. Resources that improve the performance of quantum information processing tasks are known as quantum information resources [13, 53, 58, 67]. Quantum information resources come in different shapes and forms. A resource can be classical or quantum, noisy or noiseless, static or dynamic.

Shared correlation between two parties is an important resource. The correlation between parties can be classical or quantum. If two parties can communicate classically, they can always correlate their actions or their choices of local operations, and prepare states that are correlated classically.

Quantum correlations are known as entanglement [67]. If Alice and Bob, who are spatially separate share a maximally entangled state, like a Bell state, they can use the entanglement in a teleportation protocol to transmit another (in general unknown) quantum state to each other [14]. The entangled state is an example of a static quantum resource. Teleportation can be viewed as a conversion of the static entanglement resource to a noiseless quantum channel which is a dynamic resource (see Figure 1.2). Similarly, superdense coding, whereby Alice and Bob use their shared entanglement to transmit two bits of classical information, converts the static quantum resource of entanglement to a noiseless classical channel that is also a dynamic resource (see Figure 1.3). Entanglement is measured in units of "ebit". An ebit is the amount of entanglement that is contained in a maximally entangled two-qubit state, also known as a Bell state.

Resources can also be noisy. Whereas a pure entangled state is a noiseless quantum resource, a mixed entangled state is a noisy resource. Roughly speaking, a mixed state is a statistical mixture of pure states. A decoherent channel is an example of a noisy dynamic resource.

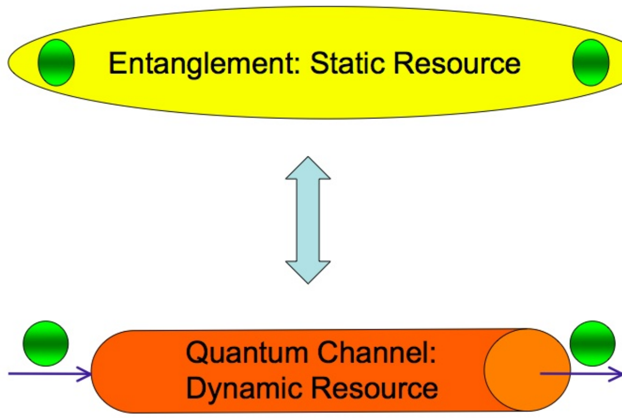

Figure 1.2: Teleportation of a qubit can be regarded as a conversion of one ebit of entanglement, which is a static noiseless quantum resource, into a noiseless quantum channel, which is a dynamic noiseless quantum resource [34].

Resources come in different combinations of classical, quantum, static, dynamic, noisy or noiseless. Thus, there are many types of resources available. In fact in the broadest sense, quantum information theory can be viewed as a theory of interconversion among different resources. In the past two decades, the field of quantum information has amassed powerful tools that can be exploited in order to quantify and categorize asymmetry resources and determine the conditions under which asymmetry resources can be converted to each other, as well as to other types of quantum resources.

A powerful tool for the study of resource theories is the concept of the resource monotones. Monotones are real-valued functions of states that change monotonically as the system undergoes a time evolution permitted by the resource theory's set of restrictions. An example of a resource monotone is the optimal rate of conversion of a given state

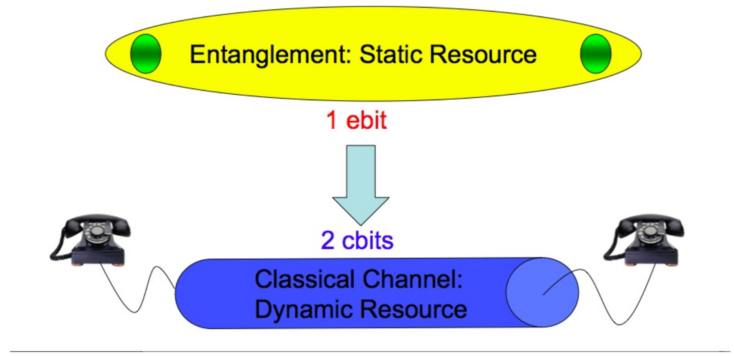

Figure 1.3: Superdense coding can be regarded as a conversion of one ebit of entanglement, which is a static noiseless quantum resource, to a noiseless classical channel, which is a dynamic noiseless classical resource capable of transmitting to 2 cbits or classical bits [34].

to some standard resource. The rate cannot increase as the system evolves, because otherwise, the rate would not have been optimal.

More generally, the motivation for monotones is that they provide operational measures to quantify the strength of resources. If one is faced with a certain task and one wants to know what is the maximum probability with which the task can be performed, or the maximum number of particular states that one can acquire using symmetric operations, the definition of that task already involves an optimization over all allowed operations. It should not be possible to do better by first pre-processing the resource, because the definition of the task assumes that all the preprocessing has already been done. In such cases, a measure of the resource strength cannot increase under restricted transformations. Entanglement monotones are real functions of states that do not increase under deterministic local operations and classical communication (LOCC) or, more generally, functions that do not increase on average under a set of non-deterministic LOCC transformations (see Section 2.4). In the resource theory of asymmetry, we consider functions that are non-increasing under symmetric transformations [35, 37]. Monotones can also be used to determine whether certain states can or cannot be transformed to each other under the restrictions that define the resource theory. A state cannot be transformed to another state with a higher value of the monotone.

1.3.1 Entanglement as a resource

Entanglement plays a central role in quantum information theory. In fact, entanglement was viewed as 'not one but the characteristic trait of quantum mechanics' by Erwin Schrödinger, one of the founders of quantum theory itself [78]. An entangled state, like the state of an EPR-pair introduced in [24], is the state of two or more systems such that the state of each individual system independent of the state of the other system is undefined. Historically, entanglement was first discussed by Albert Einstein, Boris Podolsky and Nathan Rosen in their famous 1935 EPR-paper [24]. Their treatment was in the context of foundations of quantum mechanics, and in particular, the controversy over the interpretation of quantum states. Entanglement was next investigated by Erwin Schrödinger who coined the term in his 1935 papers with Max Born [78] and Paul Dirac [77].

Later in 1964, John Stewart Bell showed that the correlation between two systems that are not entangled cannot be regarded as a "classical" correlation between the values of some hidden variable that the two systems had shared at an earlier time when they were interacting [11]. Bell tacitly assumes it impossible that some form of instantaneous action at the distance updates the correlation at the moment when either one of the two states is measured. The assumption that no action at a distance of this kind is possible is known as "local realism". Bell's result is expressed as an upper bound, known as "Bell's inequality", on the strength of any such classical correlation that adheres to local realism. Bell showed that quantum mechanics breaks this bound. Hence, entanglement denotes correlations that are truly quantum by nature and have no classical counterparts.

The correlations in entangled states can be used as resources for communication, particularly for communication of quantum information. According to the laws of quantum mechanics a qubit can be in any superposition of the two eigenstates of any of its observables. A quantum system whose state is fully expressed as a superposition of eigenstates is said to be in a "superposition state" exhibiting quantum coherence [67]. Of course, at any time, only one of the two eigenstates are obtained after measurement. Based on the observed outcome of a measurement, the state of the qubit, like that of any other quantum system, changes to the corresponding eigenstate[3].

Nevertheless, the amplitudes in the superposition are continuous magnitudes, and thus a full specification of the qubit prior to measurement requires an infinite number of classical bits. It follows that the information required to prepare an arbitrary qubit cannot be passed down classical information channels. Moreover, a qubit in a superposition state is highly susceptible to the effects of the environment that act on it as a source of noise. In an ordinary noisy channel, the environment can be thought of as performing random measurements on the state of the qubit, thus destroying the coherence of the initial state. This process of noise is known as "decoherence". Hence, decoherent channels can, at best, communicate classical information, *i.e.* information that can be stored and accessed in decohered quantum states.

The entanglement of a state can be higher than the entanglement of another state in yet another respect. When one state can be transformed to the other via local operations, but the reverse transformation by local means is not possible, the first state has higher entanglement. Local operations are operations that act on each part of an entangled state separately. This approach involves converting entangled states to each other, which is another instance of the interconversion of resources [95]. Interestingly, the two different ways that the entanglement of a state can be more than another coincide in the case of

[3]that is, unless the qubit was already in one of the eigenstates of the observable being measured prior to the measurement, in which case it will remain there unchanged.

pure states [43]. For example, for a system of two qubits in a pure state, there are four maximally entangled states, also known as Bell states,

$$
\begin{aligned}
|\psi^{\pm}\rangle &:= \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B\right) \\
|\phi^{\pm}\rangle &:= \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B\right). \qquad (1.4)
\end{aligned}
$$

The entanglement of a Bell state is maximal as it can be utilized to perform perfect quantum teleportation and superdense coding, where perfect means that the protocol is successful with probability one. The Bell states are also maximally entangled as they can be transformed with certainty to any other bipartite state using LOCC transformations, but the reverse transformation is not possible with certainty.

Alongside maps between resources that take one entangled state to another via a single transformation, we can also consider asymptotic transformations of states. In an asymptotic transformation many copies of one state are transformed to a state that is 'close' to multiple copies of the final state. Furthermore, the result approaches multiple copies of the final state to any required accuracy in the limit when the number of copies of the initial state tends to infinity. Closeness of the states are determined by various distance measures in quantum theory such as fidelity or the trace distance. The rate of interconversion of the two states is yet another measure of the relative strength of their entanglement, and, in the case of pure states, ordering entangled states in terms of this measure is again consistent with the ordering of entangled states based on the other viewpoint [43, 45, 92].

The most general resource-theoretic view of entanglement can be summed up as follows: Due to the restriction of allowed operations to LOCC, entangled states can no longer be formed out of non-entangled, or separable, states. However, if distant parties share entangled states, they can take advantage of the entanglement that they share to perform operations that are otherwise impossible due to LOCC restrictions. For example, they can be used to teleport separate parts of the state and bring them together, in which case the LOCC restriction becomes irrelevant.

This last view is the one that carries over most naturally to the resource theory of asymmetry. Entanglement satisfies the two essential attributes that separates resources from non-resource states: First, the resource states cannot be prepared from non-resource states under the given restriction. Second, Resource states can be used to circumvent, totally or partially, the respective restriction when they are included along with the target state to undergo joint operations, as in the teleportation protocol where the target state and the pair of entangled states were both acted upon during the teleportation process.

1.4 The resource theoretic approach to the study of dynamical symmetries

We now see that we can treat the resource theory of asymmetry like entanglement. The symmetry, or invariance, of the dynamics imposes a restriction of its own on the allowed quantum transformations.

If a state that breaks the symmetry is available, for example the state might have been prepared before the symmetry was imposed on all systems, it can be used to perform quantum transformations that break the symmetry. When an invariant operation, corresponding to a symmetric time evolution, is performed on the joint states of the target system together with a non-invariant state, the effect of the transformation on the target state alone need not remain symmetric anymore [8]. States that break the symmetry are therefore resources for lifting the symmetry condition.

The situation is similar to how entangled states are used in the teleportation protocol to circumvent the LOCC restrictions due to the lack of a quantum channel. Here, too, if Alice shares a “symmetry channel” with Bob and wants to transmit a quantum system, like a qubit, she can join a non-invariant resource state to the qubit, and send them together through the channel (see Fig 1.4). The channel imposes the symmetry condition on the joint system, but leaves the relative degrees of freedom of the two systems intact. The information of the initial qubit becomes encoded onto these relational degrees as the joint state goes through the channel.

Recall the G-twirling superopertor defined of the joint states of a system and an internal reference frame in Eq. (1.1) of Section 1.2.1. For simplicity, let us assume that the internal reference frame is in a pure state that we denote by $|e\rangle \in \mathscr{H}_R$, where $e \in G$ is the group identity. We similarly denote the states $U_R(g)|e\rangle$ by $|g\rangle$ for every $g \in G$. Let the operator U_R be the representation of G carried by $\mathscr{H}_R$, the Hilbert space of the reference system. The internal reference frame plays the same role as the resource state in the previous discussion, and Alice can send it to Bob together with a target state that she intends for Bob to receive, operate on or measure. A state acting as an internal reference frame is also known as a token of Alice's background reference frame. The two states are twirled as in Eq. (1.1), so the (joint) state that Bob receives is invariant. However, information about a non-invariant target state can be encoded in the joint invariant state.

One can define an encoding map from operators on $\mathscr{H}_S$ to G-covariant operators on $\mathscr{H}_S \otimes \mathscr{H}_R$ [8]:

$$\$: A \mapsto \mathcal{G}\left(A \otimes |e\rangle\langle e|\right), \tag{1.5}$$

and use the map \$ to define the covariant versions of the states and operators as

$$\begin{aligned} \rho_{SR}^{\text{Inv}} &:= \frac{1}{d_R}\$(\rho_S), \\ O_{SR}^{\text{Cov}} &:= \$(O_S), \end{aligned} \tag{1.6}$$

where d_R denotes the dimension of $\mathscr{H}_R$. The state ρ_{SR}^{Inv} is the invariant counterpart of the initial state ρ_S in the sense that the map \$ preserves the statistics of the Born rule and, consequently, all the statistical predictions associated with the original state. In particular, if M_k is a member of a G-covariant measurement[4], we have

$$\mathrm{Tr}_{SR}\left(M_k^{\mathrm{Cov}\dagger} M_k^{\mathrm{Cov}}\,\rho_{SR}^{\mathrm{Inv}}\right) = \mathrm{Tr}_S\left(M_k^\dagger M_k\,\rho_S\right). \tag{1.7}$$

In other words, the probabilities of any outcome of the original measurement and its corresponding covariant version are always the same [8].

Bob then operates on the two systems and recovers the initial qubit. The 'decoding' operation $\mathcal{D}$ is the Hilbert-Schmidt adjoint[5] of the map \$, normalized to be trace preserving [9]. The encoding and decoding maps together yield an effective decoherence of the form

$$(\mathcal{D}\circ \$)\,(\rho_S) = \int \mathrm{d}\mu_g\, p(g)\, U_S(g)\rho_S U_S^\dagger(g), \tag{1.8}$$

where

$$p(g) \propto |\langle e|U_R(g)|e\rangle|^2 \tag{1.9}$$

is a probability distribution [9].

The case of a perfect reference frame corresponds to $p(g) = \delta(g^{-1}e) = \delta\left(g^{-1}\right)$, where $\delta\,(g)$ is the delta function on G defined by $\int \mathrm{d}\mu_g\;\delta(g)f(g) = f(e)$ for any continuous function f of G [8]. In this case, the decoding map completely recovers the original state,

$$(\mathcal{D}\circ \$)\,(\rho_S) = U_S(e)\rho_S U_S^\dagger(e) = \rho_S. \tag{1.10}$$

Since we consider Lie groups in the present thesis, the condition (1.10) for a perfect RF system is satisfied only if the dimension of $\mathscr{H}_R$ is infinite[6]. If we deal with systems of

[4]Measurements and G-covariant measurements are reviewed briefly in Section 2.3.3

[5]The Hilbert-Schmidt adjoint of a superoperator $\mathcal{E}$ is defined in terms of the Hilbert-Schmidt inner product of two arbitrary operators A and B via $\mathrm{Tr}\left(A\mathcal{E}^\dagger(B)\right) = \mathrm{Tr}\left(\mathcal{E}(A)B\right)$.

[6]The method also applies to finite groups, where the integrals are replaced by discrete sums and the uniform weight $\mathrm{d}\mu_g$ by the inverse of the group size. For finite groups, perfect reference frame systems with finite-dimensional Hilbert spaces can be prepared. See [8] and [37] for examples of such systems.

bounded size and finite-dimensional Hilbert spaces, then the decoding process is always accompanied by decoherence. When the state of the reference system is itself G-invariant, however, $p(g)$ is a uniform distribution, and the decoding process is of no help. The result of Eq. (1.8) is the same as twirling the state of the system by itself,

$$\mathcal{G}(\rho) := \int \mathrm{d}\mu_g \, U_S(g)\rho_S U_S^\dagger(g). \tag{1.11}$$

Of course, if Bob does not receive the reference token at all, then he has to take a partial trace of the density operator of $\mathcal{G}(\rho_S \otimes |e\rangle\langle e|)$, resulting once again in the same invariant state:

$$\mathrm{Tr}_R \left(\mathcal{G}(\rho_S \otimes |e\rangle\langle e|)\right) = \mathcal{G}(\rho_S). \tag{1.12}$$

We can view this encoding and decoding procedure as a model for the physical process through which Bob gains information about Alice's reference-frame alignment. As long as he has not received the token, the states prepared by Alice are twirled, and thus G-invariant, relative to his frame. Once he receives the token, he can retrieve the state as it was originally prepared by Alice with some probability. Finite-dimensional and bounded-sized tokens provide Bob with only partial information about Alice's reference frame and thus lead to an 'effective' decoherence.

We can choose some resource state, say the state $|+\rangle := (1/\sqrt{2})\,(|0\rangle + |1\rangle)$ for example, to represent the refbit, or 'unit' asymmetry [89]. The degree of asymmetry of other states in units of the rebit would then the rate with which they can be asymptotically converted to the refbit by covariant transformations [37, 89]. A refbit is analogous to an ebit, the maximally entangled qubit state $|\Phi^+\rangle = (1/\sqrt{2})\,(|00\rangle + |11\rangle)$ acting as the unit of entanglement. However, what state one chooses to be the refbit is quite arbitrary, because a maximally asymmetric state does not always exist [37].

Conserved quantities are not the only thing that can be deduced from symmetry arguments. For example, there also exist quantities that are not conserved but change

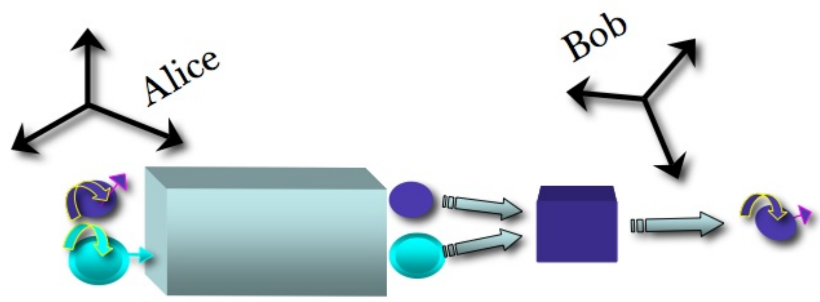

Figure 1.4: Alice can include a non-invariant state with the target state through the channel. The relational degrees of freedom are not affected by the effective decoherence in the channel. Bob performs a joint operation on the two states that he receives and recovers the original target state aligned with his reference frame.

monotonically. In other words, they are guaranteed not to increase (or decrease) during a symmetric time evolution[7].

Asymmetry monotones can be viewed as generalizations of conserved quantities. An important application of Noether's theorem is to help determine when a transition from one state to another is not allowed due to violation of some conservation law. The rules that specify which transitions are possible are the selection rules [38]. Conservation laws alone do not provide all the selection rules induced by the symmetry. The question what combination of rules and conditions is sufficient to fully determine all the consequences of a given symmetry is still an open question. Comparing the values of an asymmetry monotone for two states of a system may determine whether or not transition from one state to the other is possible under symmetric time evolutions.

The above discussion shows that there is much more to symmetry than conservation laws. To extract all the dynamical consequences of a symmetry, we need to treat the symmetry as a full-fledged resource theory. This insight points to quantum information

[7]We need consider only monotones that are non-increasing, as any non-decreasing monotone can always be multiplied by negative one to become a non-increasing one.

theory as the most conducive approach to the study of symmetry in quantum systems [8].

One particular symmetry-breaking task that can be performed using an asymmetry resource is preparing additional asymmetric states from symmetric ones. The auxiliary resource state, relative to which the target state is prepared in the above scheme, is the finite-sized quantum reference frame. As mentioned, both the finite size and the quantum nature of the asymmetry resource distinguish it from an ideal reference frame [6].

In fact, a quantum reference frame is exactly the same thing as an asymmetry resource [61]. If the reference frame were invariant under the group of transformations, its states corresponding to different values of the respective degree of freedom would not be distinct anymore and thus could not act as a reference frame for that degree of freedom at all. The more asymmetric or non-invariant the state of the system is, the larger is the orbit of any of its relevant states under symmetry transformations, and thus more of its states are distinct. In other words, the system is a better quantum reference frame.

From a resource-theoretic point of view, the ensuing restriction on states and operations is a superselection rule, and, consequently, we can apply the resource theory of asymmetry to situations where an external idealized reference frame is lacking. In a communication setting like the one we discussed for entanglement theory, the restriction arises due to a lack of shared reference frames between the parties, or equivalently, when their local references are not aligned. Asymmetry, viewed as a resource for reference frames, is also known as "frameness" in this context and has applications in many areas such as data hiding, cryptography and quantum error correction [8, 35, 37, 49, 94]. That is why the unit asymmetry of a standard state is termed a refbit, short for "reference frame bit", in analogy to ebits in entanglement theory and similar units in other resource theories [89].

1.5 A review of previous work

In this section, we review the main results of the resource theory of asymmetry, or equivalently, the resource theory of frameness. As we saw earlier in Section 1.2.2, Wick et al. introduced the notion of superselection rules (SSRs) for the first time as additional axiomatic restrictions to quantum theory [105]. The possibility of linking a SSR with the absence of a reference frame was first recognized by Aharonov and Susskind for the charge superselection rule [1]. Aharonov and Susskind showed how a superposition of different charge eigenstates can be prepared and observed *relative* to the state of a second system. They also showed how lack of alignment between two Cartesian frames can lead to an effective SSR for angular momentum.

Years later, a similar debate arose in the field of optics about whether coherent optical states could be prepared at all, or whether coherence was merely a useful fiction, and a superselection on photon numbers existed in the lab [66, 76]. In his 1997 paper, Klaus Mølmer argued that if the state of the gain medium is quantized and assumed to be in an incoherent mixture of energy eigenstates, and if the interactions between the atoms in the gain medium and the field are assumed to conserve the total energy, then the joint state of the gain medium and the electromagnetic field evolves into an incoherent sum of entangled states comprised of excited and de-excited atoms, each correlated with a different corresponding number of photons in the field [66]. It then follows that the reduced density operator of the field itself must be in an incoherent mixture of different photon number states. Mølmer further presented numerical simulations to demonstrate that this conclusion does not contradict the usual experimental results. Sanders et al. analytically verified those results [76].

In the debate that followed, what became known as 'the optical coherence controversy', it was eventually realized that both descriptions are valid and equivalent [7]. The two pictures correspond to whether a suitable phase reference, or a clock, is treated as an external reference frame or whether it is incorporated in the dynamics of the systems involved [7]. These considerations were one of the factors that lead to the modern study of quantum reference frames and their associated resource theories.

The need to study the impacts of SSR restrictions on quantum information processes also arose in the field of quantum cryptography. The principal goal of classical cryptography is to achieve computational security for cryptographic tasks. Computational security requires the adversary, or the dishonest party, to complete an exceptionally difficult computational task. On the other hand, in quantum cryptography, the aim is instead to achieve information-theoretic security, *i.e.* security that remains unbroken even if the adversary or the dishonest party has access to *unlimited* computational power [54].

For some tasks, such as quantum key distribution, protocols with information-theoretic security, also called unconditional security, have been devised and verified [62]. There are tasks, however, like bit commitment [57, 63] or strong quantum coin flipping with arbitrarily small bias, that have been demonstrated to lack information-theoretic security [2, 23].

Popescu suggested that SSRs can pose restrictions on the cheating strategies and thus enhance the security of cryptographic protocols, perhaps even allowing them to achieve unconditional security [54]. Kitaev *et al.* showed that SSR cannot thwart a dishonest party as long as his or her computational powers are assumed to be unlimited [54]. In particular, in the case of compact symmetry groups with irreducible unitary representations, they demonstrated how a cheater can, in principle, prepare a reference state that breaks the respective symmetry, use it to overcome the restrictions imposed by the SSR and implement the cheating strategy. For the same reason, if a protocol is information-theoretically secure in the absence of the SSR, it will remain so as long as the SSR arises from compact symmetry groups [54]. In the same paper, Kitaev *et al.* also generalize the result to SSRs associated with general groups in case of two-party protocols.

Bartlett *et al.* showed how privately shared RFs can function as private keys allowing for both classical and quantum communication over public quantum channels [5]. Ioannou and Mosca [49] introduced an identification scheme based on bounded quantum RFs in a quantum-public-key cryptographic framework that can be regarded as the public-key analogue of the framework developed in [5].

Following the same general line of research, Verstraete and Cirac introduced a data-hiding protocol in the presence of a SSR associated with the group $U(1)$ to determine whether the additional restriction allows the protocol to achieve unconditional security [93]. In a data-hiding protocol, either classical or quantum information is distributed among two or more parties in such a way that the information is retrieved only when the parties come together to perform joint measurements. However, they also concluded that although the security of the protocol is enhanced as a result of the SSR, it is not enhanced enough to reach unconditional security. By taking advantage of suitable reference states, phase references in this case, it is still possible to circumvent the restriction and thus successfully attack the protocol and break the security.

As entanglement is a key resource in quantum information theory, the study of the effects of SSRs on the capacity of entangled states to perform various tasks became another focus of research. The main question here is: How much of a state's entanglement remains accessible for use as a resource in quantum information processing tasks once a SSR is imposed [10, 51, 88, 104, 109]. Wiseman *et al.* observed that performing teleportation, superdense coding or violating a Bell inequality requires operations that are forbidden by a particle-number SSR for indistinguishable particles. They showed that when the SSR is in effect, different already-existing operational entanglement measures, *i.e.* measures that quantify how well a certain task can be performed by utilizing the entangled state, assign different values to the strength of a state's entanglement [109].

For example, whereas in the absence of the SSR, all operational measures assign maximum entanglement to a Bell state, under a total-particle-number SSR, some operational measures would not even designate a Bell state as entangled.

Wiseman and Vaccaro proposed a new measure of entanglement defined by the average entanglement of the projections of the state into different subspaces, each of fixed local particle number [109]. In effect, the new measure quantifies the amount of bipartite entanglement that two parties can generate between two local and distinguishable register states that each owns by local operations that satisfy the particle-number SSR.

Schuch *et al.* also considered the effects of a $U(1)$-SSR on the entanglement of bipartite states [79]. They showed that entanglement is not the only resource in the presence of the SSR. States can also be categorized in accordance to a second bipartite resource arising due to the effects of the SSR. They introduced a second measure, beside entropy of entanglement, to quantify the new resource they called *superselection-induced variance* (SiV). The two measures together fully specify the necessary and sufficient conditions for asymptotic bipartite pure-state transformations. Next, Gour *et al.* showed that the equivalent of SiV for unipartite states, the *number variance*, is a monotone under $U(1)$-covariant transformations and quantifies the asymptotic rate of reversible interconversion between two bounded-sized quantum phase references [37]. One can also view the number variance as a measure quantifying the rate at which one can distill copies of the state $|+\rangle := (1/\sqrt{2})\,(|0\rangle + |1\rangle)$, chosen as the refbit for phase references.

The notion of a unit of *shared* quantum reference frame was introduced by van Enk [89] and he initially coined the term *refbit* for such a unit. The choice of van Enk himself for a refbit of phase references was the bipartite state $(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)\,/\sqrt{2}$. Gour et al. generalized the notion of the refbit, or more accurately the notion of a *local refbit*, to include unipartite states acting as quantum reference frames associated with a general group G [37].

The first function identified to be a monotone under G-covariant transformations was introduced by Vaccaro *et al.* [88]. The monotone they called the G-*asymmetry* is defined as the difference between the von Neumann entropy of a state and the von Neumann entropy of that state after it has been averaged over the group. The G-asymmetry was shown in [35] to be equivalent to the *relative entropy of frameness*, a measure introduced in analogy with the well-known relative entropy of entanglement [91].

The notion of a measure for frameness, meaning a measure of the quality of a reference-frame token, was first made explicit by Bartlett *et al.* [6], where the authors study monotone functions under deterministic G-covariant transformations. The authors introduce a measure of frameness in terms of the average probability of success of estimating quantum states with the help of a bounded-sized quantum reference-frame token. The problem of estimating physical parameters that identify a particular transformation from a given symmetry group, and the problem of determining the optimal signal states and the optimal estimation strategies were studied in [19]. Yet another line of research involves determining the efficiency, consumption, degradation and transmission rates of various bounded-sized reference frames [4, 9, 20, 103]. For an extensive review see [8].

Frameness monotones were studied in detail in [37], where they were classified into three categories: deterministic monotones, ensemble monotones and stochastic monotones. The authors introduce particular frameness monotones for the specific groups Z_2, $U(1)$ and $SU(2)$, and under the more restrictive conditions of pure-state-to-pure-state interconversion. Further work on frameness monotones include the paper by Gour et al. [36], where the authors study frameness resources under time-reversal SSR that now involves an anti-unitary representation of the group Z_2. In [81], the authors provide an operational interpretation for G-asymmetry in terms of the accessible information in an alignment protocol associated with the cyclic groups Z_M, as well as the group $U(1)$, and relate the G-asymmetry to the Holevo quantity [42].

We discuss the contributions of the present thesis in the next section.

1.6 The original contributions of the thesis

We first present our method of linking the resource theories of asymmetry and entanglement for the special case of the symmetry group U(1) in Chapter 3. We introduce the map between pure states of the original system to a set of bipartite pure states, and show how U(1)-covariant time evolutions correspond to LOCC transformations. The group U(1) is the simplest Lie group, and by focusing on this group first, we demonstrate the main ideas of the thesis in their simplest form before going to the general case. Already, we find many new results even though the group U(1) is Abelian and despite the focus primarily on pure states.

In Chapter 4, we build on the earlier work and generalize the method and the results of the previous chapter to general Lie groups. The key idea here is to embed the system's Hilbert space $\mathscr{H}$ within a larger tensor product space $\mathscr{H}_A \otimes \mathscr{H}_B$. We show that covariant maps can be 'simulated' by a restricted subset of LOCC transformations. Figure 4.1 demonstrates what we mean by simulate in this context. Two states related by a G-covariant transformation $\mathcal{E}_{\text{cov}}$ are mapped by the LOCC-simulating isometry to two bipartite states that are related by LOCC transformation represented by $\tilde{\mathcal{E}}_{\text{local}}$.

We show that such isometries can be found for symmetries associated with semi-simple compact Lie groups. Moreover, for any asymmetric state, we show that there exists an isometry that maps it to an entangled state. Hence, the entanglement in the image space captures many of the asymmetry properties of the state. Our results follow from an application of the Wigner-Eckart theorem, generalized to all semi-simple Lie groups [16], that allows us to determine the general form of all covariant transformations [37]. Our

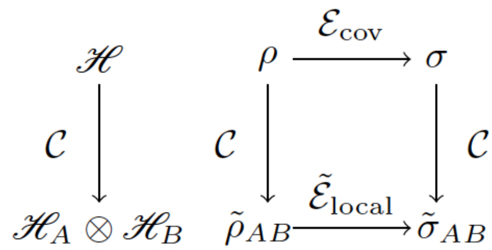

Figure 1.5: Simulating a covariant transformation $\mathcal{E}_{\rm cov}$ by a LOCC transformation $\tilde{\mathcal{E}}_{\rm local}$.

results demonstrate that the resource theory of asymmetry is equivalent to a subclass of entanglement theory restricted to a specific set of local operations.

From this key insight flows many important consequences. Every entanglement measure or monotone, can be utilized to quantify the asymmetry properties of quantum states. For reversible time evolutions, the entanglement monotones become conserved quantities associated with novel conservation laws. However, unlike Hamiltonian-based conservation laws that are in terms of expectation values of the generators of the symmetry, the new conserved quantities give rise to new selection rules that work not only for reversible transformations but also for the more general case involving irreversible transformations and open-system dynamics.

Finally, we introduce a second form of embedding within a bipartite setting that does not lead directly to LOCC operations to simulate the symmetric time evolution. Nevertheless, we show that new and additional selection rules for the general case of both closed and open systems can be constructed from entanglement considerations by taking advantage of this second embedding.

In Chapter 7, we summarize the main results of the thesis and elaborate their significance in more detail. We also highlight novel aspects of our approach that qualifies it as an original contribution to the field. We also discuss some remaining open questions as well as some new questions that have arisen from these results, and suggest possible new applications in other related research programs.

Chapter 2

Preliminaries

In this chapter, we review some of the physical and mathematical background information that is required in later chapters. We also introduce the symbols and notations that we use in the rest of the thesis. This chapter is organized as followed. In Section 2.1, we review some basic facts in group representation theory. Section 2.2 reviews the formal treatment of symmetric evolutions and G-covariant transformations. In Section 2.3, we discuss those elements of entanglement theory that are needed in later chapters. Finally, Section 2.4 discusses monotones and the conditions that they satisfy.

2.1 Group representation theory

In this thesis we will only consider semi-simple compact Lie groups and Lie algebras. We start with the definition of a Lie group and review some important topics in group theory and representation theory that we use later in the thesis [18, 30, 65, 114].

Definition 1. *A Lie group is both a group and a differential manifold such that the group's binary operation and the group's inverse operation are both differentiable functions if the manifold is real, or analytic functions if the manifold is complex.*

The dimension of a Lie group is equal to the dimension of the group's manifold. Examples of Lie groups include the general linear groups $GL(n, \mathbb{C})$ of $n \times n$ dimensional linear operators, the special linear group $SL(n, \mathbb{C})$ of unit determinant, the orthogonal, and special orthogonal groups $O(n)$ and $SO(n)$, respectively, and the unitary and special unitary groups $U(n)$ and $SU(n)$, respectively. The unitary group $U(1)$ is Abelian and is the simplest of all the unitary groups. In Chapter 3 we focus on this group to introduce some of the main ideas that are expounded and generalized to all Lie groups in Chapter 4. If the manifold is compact, the group is also called compact. The groups $O(n)$, $SO(n)$, $U(n)$ and $SU(n)$ are examples of compact Lie groups. The group of real numbers $\mathbb{R}$ with the addition operator, and the group $SU(1,1)$[1] are examples of non-compact groups. Compact Lie groups have a lot of characteristics in common with finite groups.

Let G be a Lie group whose manifold, $\mathscr{M}$, is defined over the field $\mathbb{F}$, where $\mathbb{F}$ is either the field of real numbers $\mathbb{R}$, or the field of complex numbers, $\mathbb{C}$. Also let the group's manifold $\mathscr{M}$ be of dimension n. Consider an invertible and differentiable (or analytic) curve $\gamma : \mathbb{R}\ \mathbb{F} \to \mathscr{M} \,:\, t \mapsto \gamma(t)$, passing through the group's identity element $e = \gamma(0)$. The tangent vector to $\gamma(t)$ at the identity is the vector

$$\boldsymbol{\chi} := \left.\frac{d\gamma(t)}{dt}\right|_{t=0}. \tag{2.1}$$

Let the tangent vectors for two invertible differentiable curves γ and δ passing through the group identity be $\boldsymbol{\chi}$ and $\boldsymbol{\xi}$ respectively.

Definition 2. *The commutator $[\boldsymbol{\chi}, \boldsymbol{\xi}]$ of tangent vectors $\boldsymbol{\chi}$ and $\boldsymbol{\xi}$ is the vector at the identity of the curve $\kappa : \mathbb{F} \to \mathscr{M}$ given by*

$$\kappa(\tau) := \gamma(\tau^2)\delta(\tau^2)\gamma^{-1}(\tau^2)\delta^{-1}(\tau^2), \quad \forall \tau \in \mathbb{F}. \tag{2.2}$$

In other words, the commutator $[\boldsymbol{\chi}, \boldsymbol{\xi}]$ is the coefficient of τ^2 in the Taylor expansion of the curve κ at the identity [65]. The tangent vectors at e form a vector space that we call the tangent space $\mathrm{T}_e G$. The commutator operation defined above, also known as a Lie bracket, satisfies all the conditions of a bilinear operation of an algebra (see for example [74]).

Definition 3. *The Lie algebra $\mathfrak{g}$ of the Lie group G is the tangent space T_eG equipped with scalar multiplication, vector addition and the commutator operation of Definition 2 [65].*

[1]Let $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. The group $SU(1,1)$ is the group of 2×2 matrices with determinant equal to one that obey $A^\dagger J A = J$.

A homomorphism between two Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ is a linear map $f : \mathfrak{g}_1 \to \mathfrak{g}_2$ that preserves the commutation relations:

$$f\left([\boldsymbol{\chi}, \boldsymbol{\xi}]_1\right) = [f(\boldsymbol{\chi}), f(\boldsymbol{\xi})]_2 \,, \quad \forall\, \boldsymbol{\chi}, \boldsymbol{\xi} \in \mathfrak{g}_1. \tag{2.3}$$

A subspace $\mathfrak{h} \subseteq \mathfrak{g}$ that is closed under the commutator operation is called a Lie subalgebra.

Definition 4. *A subset $\mathfrak{I} \subseteq \mathfrak{g}$ is called an* ideal *if $[\boldsymbol{\chi}, \boldsymbol{\eta}] \in \mathfrak{I}$ for all $\boldsymbol{\chi} \in \mathfrak{g}$ and $\boldsymbol{\eta} \in \mathfrak{I}$. In short, $[\mathfrak{g}, \mathfrak{I}] \subseteq \mathfrak{I}$. The ideal is called proper if $\mathfrak{I}$ is a proper subset of $\mathfrak{g}$, i.e. $\mathfrak{I} \subset \mathfrak{g}$. The ideal $\mathfrak{I}$ is Abelian if for every $\boldsymbol{\eta}_1, \boldsymbol{\eta}_2 \in \mathfrak{I}$, the commutator $[\boldsymbol{\eta}_1, \boldsymbol{\eta}_2] = 0$.*

The notion of Lie algebras and their representations plays an important role in the study of asymmetry resources.

Definition 5. *A Lie algebra is called simple if it contains no proper ideals, and it is called semi-simple if it contains no proper Abelian ideals.*

A group is said to be semi-simple if its associated algebra is semi-simple [111]. A simple algebra is necessarily semi-simple. However, a semi-simple algebra is not always simple. Instead, a semi-simple algebra satisfies the following condition:

Theorem 1. *A Lie algebra $\mathfrak{g}$ is semi-simple if and only if $\mathfrak{g}$ can be expressed as a direct sum,*

$$\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_k, \tag{2.4}$$

where $\mathfrak{g}_i$ are ideals of $\mathfrak{g}$, with each ideal forming a simple Lie algebra [65].

2.1.1 Group-invariant measures and group averages

Consider a measure space Ω. The σ-algebra, $\sigma(\Omega)$, is a non-empty subset of the power set of Ω that is closed under complementation and countable unions. An invertible function $f:(\sigma(\Omega_1))\to(\sigma(\Omega_2))$ is called a measurable function if for every $B\in\sigma(\Omega_2)$, its inverse image is in $\sigma(\Omega_1)$, *i.e.* $f^{-1}(B)\in\sigma(\Omega_1)$. In particular, we will be using measurable functions that map Lie groups (or Lie algebras) to the group of linear automorphisms of the system's state space later in thesis, when we work extensively with the representations of Lie groups and Lie algebras (see Section 2.1.2).

Definition 6. *A Borel measure on Ω is a non-negative countably additive function from the σ-algebra of Ω to the extended real number line, $\mu:\sigma(\Omega)\to\bar{\mathbb{R}}$ that assigns zero to the empty set and finite and non-negative values on compact subsets of Ω.*

The function μ is countably additive if

$$\mu\left(\bigcup B_i\right)=\sum\mu(B_i), \tag{2.5}$$

for $\{B_i\}$ a countable set of pairwise disjoint subsets of Ω. The extended real number line $\bar{\mathbb{R}}$ is obtained by augmenting the real number system $\mathbb{R}$ by adding two elements called the positive infinity $+\infty$ and the negative infinity $-\infty$.

Consider a Lie group G. For any fixed element $h\in G$, and a subset $B\subseteq G$, we denote as $hB=\{hg|\ g\in G\}$ the subset onto which the diffeomorphism $g\mapsto hg$ maps B. We define $Bh=\{gh|\ g\in G\}$ in a similar manner.

Definition 7. *A Borel measure μ_L on a Lie group G is called* left-invariant *if*

$$\mu(hB)=\mu(B), \tag{2.6}$$

for every group element $h\in G$ and every set $B\in\sigma(\Omega)$. Similarly, a measure μ_R is called right-invariant *if*

$$\mu(Bh)=\mu(B), \tag{2.7}$$

for all $h\in G$ [19, 114].

Theorem 2. *Every Lie group G admits both a left-invariant and a right-invariant measure. Moreover, each left-invariant measure on G is unique up to a scalar factor, i.e. a multiplicative constant in $\mathbb{F}$. The same is true for each right-invariant measure of G [19, 114].*

In general, the left-invariant and the right-invariant measures of a Lie group need not be equal. If the left and right-invariant measures are equal (up to a scalar factor) the group is called unimodular.

Theorem 3. *All compact Lie groups are unimodular [19, 114].*

As we deal only with compact Lie groups in the present thesis, we always utilize a measure of the group that is both left and right-invariant.

Definition 8. *A measure μ of the group G that is both left and right-invariant is called a* Haar *measure of the group.*

The Haar measures of a compact Lie group differ only by a multiplicative constant. Furthermore, we use the Haar measures in the integrals of measurable functions, otherwise known as Haar integrals. In the rest of the thesis, we assume that the Haar measure of the Lie group is normalized: $\int_{g\in G} \mathrm{d}\mu(g) = 1$, where $\int_{g\in B} \mathrm{d}\mu(g) = \mu(B)$ for every subset B of the group. The left invariance of the Haar measure implies

$$\int_G \mathrm{d}\mu(g)\, f(hg) = \int_G \mathrm{d}\mu(g)\, f(g), \quad \forall\, h \in G. \tag{2.8}$$

A similar relation exists naturally for the right invariance as well. The Haar integral formalism is developed in the general theory of Lebesgue integrals (see for example [101]).

2.1.2 Representations of groups and algebras

Given that we primarily work with quantum states and Hilbert spaces, we need to specify how the appropriate Lie group acts on those mathematical objects. Representation theory allows us to systematically study the action of groups on vector spaces and Hilbert spaces.

Let $\mathscr{H}$ be the system's Hilbert space over $\mathbb{C}$, the field of complex numbers. We assume that the input and output Hilbert spaces are the same. In cases where this is not true we differentiate them by $\mathscr{H}_{\text{in}}$ and $\mathscr{H}_{\text{out}}$ respectively.

Definition 9. *A representation $T : G \to GL(\mathscr{H})$ of a group G acting on the space $\mathscr{H}$ is a homomorphism from the group G to the group of linear automorphisms of $\mathscr{H}$.*

For groups with real manifolds, we consider homomorphisms that are differentiable. For groups with complex manifolds we consider homomorphisms that are analytic. By a differentiable or an analytic homomorphism, we mean a homomorphism whose matrix elements $T_{i,j}(g)$ with respect to any basis in $\mathscr{H}$ are, respectively, differentiable or analytic functions of the local coordinates of g in G.

Definition 10. *A unitary representation $U : G \to GL(\mathscr{H})$ is a representation of the group G such that $U(g)^{-1} = U(g)^{\dagger}$ for all $g \in G$.*

Equivalently, a representation $U : G \to GL(\mathscr{H})$ is a unitary representation of G if and only if for all $g \in G$

$$\langle U(g)\boldsymbol{v}, U(g)\boldsymbol{w}\rangle = \langle \boldsymbol{v}, \boldsymbol{w}\rangle, \quad \boldsymbol{v}, \boldsymbol{w} \in \mathscr{H}, \tag{2.9}$$

where $\langle , \rangle$ denotes the inner product on $\mathscr{H}$.

Definition 11. *Two representations T_1 and T_2 of a group G carried by Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$, respectively, are said to be* equivalent *if there exists an invertible linear transformation $A : \mathscr{H}_1 \to \mathscr{H}_2$ such that*

$$T_2(g) = A\, T_1(g)\, A^{-1}, \quad \forall g \in G. \tag{2.10}$$

The invertible linear transformation A is an isomorphism also known as an *intertwiner*. If $\mathscr{H}_1$ and $\mathscr{H}_2$ are the same Hilbert space then (2.10) is a change of basis.

Theorem 4. *Every representation of a compact Lie group is equivalent to a unitary representation [65].*

Proof. If T is not already a unitary representation, we define a new inner product $(,)$ on $\mathscr{H}$ with respect to which T becomes a unitary representation. Let

$$(\boldsymbol{v_1}, \boldsymbol{v_2}) := \int_G \mathrm{d}_\mu(g) \, \langle T(g)\boldsymbol{v_1}, T(g)\boldsymbol{v_2} \rangle. \tag{2.11}$$

The integral is taken over the group with a Haar measure, consequently

$$\begin{aligned}(T(h)\boldsymbol{v_1}, T(h)\boldsymbol{v_2}) &= \int_G \mathrm{d}_\mu(g) \, \langle T(gh)\boldsymbol{v_1}, T(gh)\boldsymbol{v_2} \rangle \\ &= \int_G \mathrm{d}_\mu(g') \, \langle T(g')\boldsymbol{v_1}, T(g')\boldsymbol{v_2} \rangle = (\boldsymbol{v_1}, \boldsymbol{v_2}) \, . \end{aligned} \tag{2.12}$$

Let $\{|\boldsymbol{v}_i\rangle\}$ be an orthonormal basis of $\mathscr{H}$ with respect to the original inner product and $\{|\boldsymbol{w}_i\rangle_2\}$ be an orthonormal basis of $\mathscr{H}_2$, which is the Hilbert space with respect to the new inner product $(,)$. Define the invertible linear transformation $S : \mathscr{H} \to \mathscr{H}_2$ as the transformation that relates the two basis states, $S|\boldsymbol{v}_i\rangle = |\boldsymbol{w}_i\rangle_2$. It follows that

$$U(g) := S \, T(g) \, S^{-1} \tag{2.13}$$

is a unitary operator for every $g \in G$ as it satisfies (2.9). □

From now on, we only consider unitary representations. The representation that maps every group element to the identity operator is called the trivial representation, otherwise the representation is called non-trivial.

Definition 12. *A non-trivial representation $T : G \to GL(\mathscr{H})$ is reducible if there exists a proper subspace $\mathscr{V} \subset \mathscr{H}$ that remains invariant under the action of the group representation. In other words, a representation is reducible if for every vector $|v\rangle \in \mathscr{V}$, the state $T(g)|v\rangle \in \mathscr{V}$, for all $g \in G$. Alternatively, the representation $T : G \to GL(\mathscr{H})$ is called irreducible, or an irrep for short, if no such subspace $\mathscr{V}$ exists.*

Any subspace $\mathscr{V}$ satisfying Definition 12 is known as an invariant subspace of $\mathscr{H}$.

Theorem 5. *If G is a compact Lie group and if $U : G \to GL(\mathscr{H})$ is a (unitary) representation of G on a Hilbert space $\mathscr{H}$, then the unitaries $U(g)$ can be decomposed into a direct sum of a discrete number of irreps [19].*

A representation that, by a suitable choice of basis, can be written as a direct sum of irreps is called *fully reducible*. Thus, every representation of a compact Lie group is fully reducible to a sum of irreps where each irrep has finite dimension [18]. Every finite unitary representation of a semi-simple group is also fully reducible. We use many of the features of fully reducible representations later in the thesis. In particular, the results of Chapters 3, 4 and 6 rely heavily on the direct sum decomposition of unitary representations into irreps. We will come back to the direct-sum decomposition shortly, but first we review how irreps are labeled and how their labels are related to the Lie algebra of the group.

Two important results concerning irreducible representations are contained in two lemmas known as Schur's lemmas [18, 65].

Lemma 6. *If $U : G \to GL(\mathscr{H})$ is an irrep and $A : \mathscr{H} \to \mathscr{H}$ is a linear map that commutes with $U(g)$ for all $g \in G$ then $A = \lambda I$, where I is the identity operator and $\lambda \in \mathbb{C}$.*

Lemma 7. *If $U : G \to GL(\mathscr{H})$ and $V : G \to GL(\mathscr{H})$ are two irreps and $A : \mathscr{H} \to \mathscr{H}$ is a linear map such that $A\,U(g) = V(g)\,A$, for all $g \in G$, then either $A = 0$ or $U \cong V$, i.e. $A\,U(g)A^{-1} = V(g)$ for all $g \in G$, and A is invertible and an intertwiner between the two representations.*

It follows immediately from Schur's lemmas that every irrep of an Abelian group must be 1-dimensional.

Now consider a representation $U : G \to GL(\mathscr{H})$. Suppose $g(\boldsymbol{x}) = g(x_1, \cdots, x_r)$, with $\boldsymbol{x} \in \mathbb{F}^r$, is a point of the manifold in the neighbourhood of the point $(0, \cdots, 0)$ corresponding to the group identity. We can use the properties of the manifold and Taylor expand the unitary operator around this point:

$$U\left(g(\boldsymbol{x})\right) = I + \sum_k x_k \left(\frac{\partial U(g)}{\partial x_k}\right)\Bigg|_{\boldsymbol{x}=0} + \text{higher order terms in the coordinates } x_k. \tag{2.14}$$

The matrix

$$X_k := \left(\frac{\partial U(g)}{\partial x_k}\right)\Bigg|_{\boldsymbol{x}_0=0}, \tag{2.15}$$

is called an infinitesimal generator of the group representation.

Theorem 8. *The matrices $\{X_k\}$ in Eq. (2.15) satisfy the relation*

$$[X_i, X_j] = \sum_k C^k_{i,j} X_k, \tag{2.16}$$

where $[\ ,\ ]$ denotes the commutator of two operators in $GL(\mathscr{H})$. The numbers $C^k_{ij} \in \mathbb{F}$ are called the structure constants *of the Lie group.*

Proof. Note that the X_k is determined by the derivative of $U(g)$ at the identity and is thus independent of the choice of $\boldsymbol{x}$ in Eq. (2.15). Hence, for simplicity, we consider the representation of two group elements $U(g(\boldsymbol{x}_i))$ and $U(g(\boldsymbol{x}_j))$, where the coordinates $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$ both have all but one of their entries equal to zero. Furthermore, assume that the sole non-zero element in both cases is equal to a given ϵ, in the i^{th} and j^{th} positions respectively. In other words, both coordinates are of the form $\boldsymbol{x} = (0, \cdots, \epsilon, \cdots, 0)$. As U is a representation of G, it follows that

$$U(g(\boldsymbol{x}_i))U(g(\boldsymbol{x}_j))U^{-1}(g(\boldsymbol{x}_i))U^{-1}(g(\boldsymbol{x}_j)) = U(h(i, j, \epsilon)), \tag{2.17}$$

for some $h \in G$, where h is a suitable function of i, j and ϵ: $h = h(i, j, \epsilon)$. Expanding the right hand side of Eq. (2.17) as in Eq. (2.14) gives

$$U(g(\boldsymbol{x}_i))U(g(\boldsymbol{x}_j))U^{-1}(g(\boldsymbol{x}_i))U^{-1}(g(\boldsymbol{x}_j)) = I + \epsilon^2 [X_i, X_j] + O(\epsilon^3). \tag{2.18}$$

Similarly, assuming h is parametrized as $h = g(s_1, \cdots, s_r)$, where each $s_k = s_k(i, j, \epsilon)$ is again a function of i, j and ϵ, and expanding the right hand side of Eq. (2.17), we get

$$U(h) = I + \sum_k s_k X_k + \text{higher order terms} \tag{2.19}$$

As there is no term of order ϵ in (2.18), it follows that $s_k(i, j, \epsilon)$ must be of order ϵ^2. Equating the terms of order ϵ^2 in Eqs. (2.18) and (2.19) leads to

$$[X_i, X_j] = \sum_k C_{i,j}^k X_k, \tag{2.20}$$

where each $C_{i,j}^k := s_k(i, j, \epsilon)/\epsilon^2$ is a constant. □

The infinitesimal generators X_k defined in Eq. (2.15) together with the commutator on $GL(\mathscr{H})$ belong to a representation of the Lie algebra $\mathfrak{g}$ [18]. In the present thesis we deal primarily with representations of Lie groups and Lie algebras on the Hilbert space of quantum systems and not with the abstract Lie group or Lie algebra itself. So, unless otherwise stated,we refer to the representation of a Lie algebra simply as the Lie algebra for brevity when the context is clear and unambiguous, and we denote it by LieG.

Definition 13. *The* adjoint operator *of an infinitesimal generator X_i is the map $\breve{X}_i$ defined as*

$$\breve{X}_i : \text{LieG} \to \text{LieG} : X_k \mapsto [X_k, X_i], \tag{2.21}$$

Let $A = \sum_k a_k X_k$ be an element of a semi-simple Lie algebra LieG. Consider the eigenvector equation for the adjoint operator $\breve{A}$:

$$\breve{A}X = aX, \tag{2.22}$$

or equivalently,

$$[A, X] = aX. \tag{2.23}$$

Theorem 9. *If A has the maximum number of distinct eigenvalues, then the only eigenvalue that is degenerate (*ie. *has multiplicity greater than one) is the eigenvalue zero [18].*

Definition 14. *The* rank *of the Lie algebra LieG is the degeneracy of the eigenvalue zero of the adjoint operator with the maximum number of distinct eigenvalues.*

A Lie group of rank ℓ is a Lie group whose Lie algebra is of rank ℓ. Let us denote the ℓ independent eigenvectors associated with the eigenvalue zero by H_i $(i = 1, \cdots, \ell)$. In other words $[A, H_i] = 0$, where $\breve{A}$ is the adjoint operator with the maximum number of distinct eigenvalues. Note that $[A, A] = 0$ too, so that A must be of the form $A = \sum_i \lambda_i H_i$. In fact, the operators H_i, $i = 1, \cdots, \ell$, form a subalgebra of LieG called the *Cartan subalgebra* of LieG [18]. In general, the Cartan subalgebra of a Lie algebra $\mathfrak{g}$ is the maximal Abelian subalgebra of $\mathfrak{g}$. Thus, the dimension of the Cartan subalgebra is the same as the rank of the Lie algebra.

If G is of dimension r, then the remaining $r - \ell$ non-degenerate eigenvectors satisfy the following relations [18, 111]:

$$\begin{aligned}
[H_i, H_j] &= 0, \;\; i, j = 1, \cdots \ell \\
[H_i, D_{\boldsymbol{\alpha}}] &= \alpha_i D_{\boldsymbol{\alpha}}, \;\; \alpha_i \in \mathbb{F} \\
[D_{\boldsymbol{\alpha}}, D_{\boldsymbol{\beta}}] &= N_{\boldsymbol{\alpha}\boldsymbol{\beta}} D_{\boldsymbol{\alpha}+\boldsymbol{\beta}}, \;\; \alpha_i \in \mathbb{F} \;\; (\text{if } \boldsymbol{\alpha} + \boldsymbol{\beta} \neq 0) \\
[D_{\boldsymbol{\alpha}}, D_{-\boldsymbol{\alpha}}] &= \sum_i \alpha_i \, H_i.
\end{aligned} \tag{2.24}$$

Thus, each operators $D_{\boldsymbol{\alpha}}$ is simultaneously the eigenvector of all the adjoint operators $\breve{H}_1, \cdots, \breve{H}_\ell$ with eigenvalues $\alpha_1, \cdots, \alpha_\ell$ respectively, where $\alpha_i \in \mathbb{F}$, for $i = 1, \cdots, \ell$. The eigenvalues can be regarded as elements of a vector $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_\ell)$ called a *root* *vector* (or a *root* for short). The roots span an ℓ-dimensional vector space that we call the *root space* of the Lie algebra.

The r operators $\{H_i\} \cup \{D_\alpha\}$ belong to a representation of the *Cartan-Weyl* basis of the Lie algebra. As the ℓ operators H_i all commute, we can build a set of simultaneous eigenvectors $|\boldsymbol{m}\rangle$ such that,

$$H_i|\boldsymbol{m}\rangle = m_i|\boldsymbol{m}\rangle, \quad i = 1, \cdots, \ell. \tag{2.25}$$

The ℓ eigenvalues comprise a vector $\boldsymbol{m} = (m_1, \cdots, m_\ell)$, called a *weight vector*, or simply a *weight*, of the representation of the Lie algebra. The weight vectors span a vector space that we call the weight space Δ_U. Also, let us define the operator vector $\boldsymbol{H} := (H_1, \cdots, H_\ell)$. The set of relations in Eq. (2.24) imply (see [111]),

$$\boldsymbol{H}\, D_{\boldsymbol{\alpha}}|\boldsymbol{m}\rangle = (\boldsymbol{m} + \boldsymbol{\alpha})\, D_{\boldsymbol{\alpha}}|\boldsymbol{m}\rangle. \tag{2.26}$$

A weight $\boldsymbol{m}$ is called positive if its smallest non-vanishing component is positive. The weight $\boldsymbol{m}_1$ is said to be higher than $\boldsymbol{m}_2$, denoted as $\boldsymbol{m}_1 > \boldsymbol{m}_{\boldsymbol{2}}$, if $\boldsymbol{m}_1 - \boldsymbol{m}_2$ is a positive weight. If a weight $\boldsymbol{j}$ satisfies $\boldsymbol{j} > \boldsymbol{m}$ for all the other weights $\boldsymbol{m}$, then $\boldsymbol{j}$ is called the highest weight in the representation. The following important theorem, that we present without proof here, implies that that the highest weight of an algebra can be used to label the irrep.

Theorem 10. *Two representations with the same highest weight are equivalent [65].*

Recall that a unitary representation $U : G \to GL(\mathscr{H})$ of a compact Lie group is fully reducible, and we can thus write every matrix $U(g)$ for every $g \in G$ as the direct sum of irreps $U_{\boldsymbol{j}}$, *i.e.* in a suitable choice of basis,

$$U(g) = \bigoplus_{\boldsymbol{j} \in \Lambda_U} \lambda_{\boldsymbol{j}}\, U_{\boldsymbol{j}}(g), \tag{2.27}$$

where $\boldsymbol{j}$ is the label for the inequivalent irreps, $\lambda_{\boldsymbol{j}} \in \mathbb{N}$ is the multiplicity of the irrep labeled by $\boldsymbol{j}$ in the representation and Λ_U is the set of all irrep labels in the representation U. The Hilbert space that carries U can also be decomposed as the direct sum

$$\mathscr{H} = \bigoplus_{\boldsymbol{j} \in \Lambda_U} \mathscr{H}_{\boldsymbol{j}}, \tag{2.28}$$

where each subspace $\mathscr{H}_{\boldsymbol{j}}$ can, in general, carry multiple copies of the irrep $U_{\boldsymbol{j}}$:

$$\mathscr{H}_{\boldsymbol{j}} = \bigoplus_{\lambda=1}^{\lambda_{\boldsymbol{j}}} \mathscr{H}_{\boldsymbol{j},\lambda}. \tag{2.29}$$

As all the $\mathscr{H}_{\boldsymbol{j},\lambda}$ are equivalent, the subspace $\mathscr{H}_{\boldsymbol{j}}$ is isomorphic to

$$\mathscr{H}_{\boldsymbol{j}} \cong \mathscr{M}_{\boldsymbol{j}} \otimes \mathscr{N}_{\boldsymbol{j}}, \tag{2.30}$$

where $\mathscr{M}_{\boldsymbol{j}}$ is known as the carrier space acted on by the irrep $U_{\boldsymbol{j}}$, and $\mathscr{N}_{\boldsymbol{j}}$ is known as the multiplicity space acted on by the identity (or trivial) representation of the group.

The suitable basis states that span the space $\mathscr{H}_{\boldsymbol{j}}$ can be labeled as $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle$, where $\boldsymbol{m}$ denotes the ℓ-dimensional weight vectors, $\boldsymbol{j}$ is the highest weight and consequently the label of the irrep itself, and λ labels the multiplicity.

2.2 Symmetric transformations

Let $\mathcal{B}(\mathscr{H})$ denote the set of bounded operators of $\mathscr{H}$. The most general quantum transformations that we consider in the present thesis are completely positive (CP) maps [67]. Consider a CP map $\mathcal{E} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ that takes density operators to density operators. Every CP-map can be expressed as the sum

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger, \tag{2.31}$$

where $K_i : \mathscr{H} \to \mathscr{H}$ satisfy $\sum_i K_i^\dagger K_i \leq I$, or equivalently, $I - \sum_i K_i^\dagger K_i$ is a positive semi-definite operator. The operators $\{K_i\}$ are known as *Kraus operators* or *operation elements* of the map $\mathcal{E}$ [67].

Let G be a group of transformations, and define the map $\mathcal{U}(g) : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ as

$$\mathcal{U}(g)[\bullet] := U(g)(\bullet)U^{\dagger}(g), \tag{2.32}$$

where $U : G \to \mathcal{B}(\mathscr{H}) : g \mapsto U(g)$ is a representation of the group G, and the bullet sign $\bullet$ represents any member in the domain of the map. As we only consider compact semi-simple Lie groups with fully reducible unitary representations in this thesis, we will always assume that the representation of the group comes with a Haar measure.

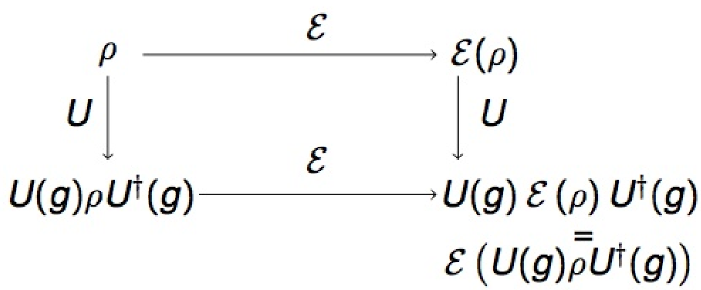

Figure 2.1: G-covariant transformations are those transformations $\mathcal{E}$ such that $U(g)\mathcal{E}(\rho)U^{\dagger}(g) = \mathcal{E}\left(U(g)\rho U^{\dagger}(g)\right)$.

We say that the mapping $\mathcal{E}$ is symmetric with respect to G, or equivalently, that $\mathcal{E}$ is G-covariant, if for all ρ and for all $g \in G$ (Figure 2.1),

$$\mathcal{E} \circ \mathcal{U}(g)[\rho] = \mathcal{U}(g) \circ \mathcal{E}[\rho]. \tag{2.33}$$

In particular, if the CP-map consists of a single unitary V, $\mathcal{E}[\bullet] = V(\bullet)V^{\dagger}$, then the condition of G-covariance in Eq. (2.33) becomes

$$[U(g), V] = 0, \ \forall g \in G. \tag{2.34}$$

The unitary V is called G-invariant in this case. Similarly, a symmetric state ρ is any state that remains invariant under the application of the group representation, also known as a G-invariant state,

$$[U(g), \rho] = 0, \ \forall g \in G. \tag{2.35}$$

Consider the uniform average of the group action:

$$\mathcal{G}[\rho] := \int \mathrm{d}\mu(g)\, \mathcal{U}(g)[\rho], \tag{2.36}$$

where $\mathrm{d}\mu(g)$ denotes the group's Haar measure. The averaging superoperator $\mathcal{G}$ in Eq. (2.36) is known as the G-twirling operation. It follows from the uniformity of the measure that twirled states are invariant under the action of any element of the group, *i.e.* they are G-invariant. In fact, it can be shown that every G-invariant state can be expressed as the outcome of a twirling operation [8].

If we decompose the Hilbert space as in Eq. (2.37),

$$\mathscr{H} = \bigoplus_{\boldsymbol{j},\lambda} \mathscr{H}_{\boldsymbol{j},\lambda}, \tag{2.37}$$

the form of the G-twirling of a state ρ can be expressed as

$$\mathcal{G}[\rho] = \sum_{\boldsymbol{j},\lambda} p_{\boldsymbol{j},\lambda} \Pi_{\boldsymbol{j},\lambda}, \tag{2.38}$$

where $\Pi_{\boldsymbol{j},\lambda}$ denotes the projection of ρ onto subspace $\mathscr{H}_{\boldsymbol{j},\lambda}$ that carries the $\boldsymbol{j}^{\text{th}}$ irrep.

The definition of G-covariance in Eq. (2.33) is equivalent to

$$\mathcal{E} = \mathcal{U}(g) \circ \mathcal{E} \circ \mathcal{U}(g^{-1}), \ \ \forall g \in G. \tag{2.39}$$

Clearly, if $\{K_i\}$ is a set of Kraus operators of a G-covariant CP-map $\mathcal{E}$ then Eq. (2.39) implies that $\left\{U(g)K_iU^\dagger(g)\right\}$ is also a set of Kraus operators for $\mathcal{E}$. Now, two operator-sum representations of the same channel $\mathcal{E}$ are related by a unitary matrix. Therefore, it follows that

$$U(g)K_iU^\dagger(g) = \sum_{i'} u_{ii'}(g)\ K_{i'} \tag{2.40}$$

where $u_{ii'}(g)$ are the elements of a unitary matrix $u(g)$. It was shown in [37] that if the $\{K_i\}$ are linearly independent, then $u(g)$ is also a representation of the group G.

Furthermore, bringing the matrix $u(g)$ to the block diagonal form,

$$u(g) = \bigoplus_{\boldsymbol{j},\lambda} u_{\boldsymbol{j},\lambda}(g) \tag{2.41}$$

of the group's irreps simply amounts to a different unitary remixing of the Kraus operators, and is thus allowed. This, in turn, means that the Kraus operators of a G-covariant CP-map can be grouped into subsets that mix only among themselves, each labeled by the irrep labels of the group. Thus, every G-covariant CP-map admits a Kraus decomposition, labeled $K_{\boldsymbol{j},\boldsymbol{m},\alpha}$, with α being a multiplicity index, such that

$$K_{\boldsymbol{j},\boldsymbol{m},\alpha} = \sum_{\boldsymbol{m}'} u^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g)\ K_{\boldsymbol{j},\boldsymbol{m}',\alpha}, \quad \forall g \in G. \tag{2.42}$$

For each irrep label $\boldsymbol{j}$, Kraus operators of the set $\{K_{\boldsymbol{j},\boldsymbol{m},\alpha}\}$ are called irreducible tensor operators of rank $\boldsymbol{j}$.

A CP-map with a Kraus decomposition comprised of a set of irreducible tensor operators,

$$\mathcal{E}_{\boldsymbol{j},\alpha}(\bullet) = \sum_{\boldsymbol{m}} K_{\boldsymbol{j},\boldsymbol{m},\alpha}\,(\bullet)\ K^{\dagger}_{\boldsymbol{j},\boldsymbol{m},\alpha}, \tag{2.43}$$

is an irreducible G-covariant operation. Every G-covariant CP-map can be expressed as a sum of irreducible G-covariant operations.

2.2.1 The collective representation

The representation of symmetry groups for composite systems that we consider in the present thesis is the so-called collective representation. Consider a composite system comprised of, say, two systems with corresponding Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$. Assuming that the unitary representations of a group element $g \in G$ on the Hilbert spaces are $U_1(g)$ and $U_2(g)$, respectively, the collective representation of that same group element on the composite system is the tensor product $U_1(g) \otimes U_2(g)$. Most symmetries studied in physics are represented on the state space of composite systems as collective representations.

The generalized Clebsch-Gordan (CG)-coefficients $\left(\begin{array}{cc|c} \boldsymbol{j}_1 & \boldsymbol{j}_2 & \boldsymbol{j}_3 \\ \boldsymbol{m}_1 & \boldsymbol{m}_2 & \boldsymbol{m}_3 \end{array}\right)$ relate the basis $|\boldsymbol{j}_1, \boldsymbol{m}_1\rangle \otimes |\boldsymbol{j}_2, \boldsymbol{m}_2\rangle$ to the basis $|\boldsymbol{j}_3, \boldsymbol{m}_3; (\boldsymbol{j}_1, \boldsymbol{j}_2)\rangle$ that reduces the tensor product, also known as the Kronecker product, of the two irreps $U_{12} := U_1 \otimes U_2$,

$$|\boldsymbol{j}_3, \boldsymbol{m}_3;\ (\boldsymbol{j}_1, \boldsymbol{j}_2)\rangle = \sum_{\boldsymbol{m}_1, \boldsymbol{m}_2} \left(\begin{array}{cc|c} \boldsymbol{j}_1 & \boldsymbol{j}_2 & \boldsymbol{j}_3 \\ \boldsymbol{m}_1 & \boldsymbol{m}_2 & \boldsymbol{m}_3 \end{array}\right) |\boldsymbol{j}_1, \boldsymbol{m}_1\rangle \otimes |\boldsymbol{j}_2, \boldsymbol{m}_2\rangle. \tag{2.44}$$

Here, we have dropped the multiplicity index λ, as the CG-coefficients do not depend on the multiplicity. We use $|\boldsymbol{j}; \boldsymbol{m}\rangle$, or $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle$ instead of $|\boldsymbol{j}, \boldsymbol{m}; (\boldsymbol{j}_1, \boldsymbol{j}_2)\rangle$ or $|\boldsymbol{j}, \lambda, \boldsymbol{m}; (\boldsymbol{j}_1, \boldsymbol{j}_2)\rangle$ for brevity whenever the context is clear.

The tensor product, or Kronecker product, of two irreps is, in general, not irreducible. In fact, if the group is semi-simple, then the representation of the Kronecker product is fully reducible. If the irreps in the Kronecker product have no additional multiplicities due to the "coupling", the algebra, and the group, are called simply reducible.

If the algebra is not simply reducible, then the change of basis will instead take the following form

$$|\boldsymbol{j}_3, \mu_3; \boldsymbol{m}_3;\ (\boldsymbol{j}_1, \boldsymbol{j}_2)\rangle = \sum_{\mu_3} \sum_{\boldsymbol{m}_1, \boldsymbol{m}_2} \left(\begin{array}{cc|c} \boldsymbol{j}_1 & \boldsymbol{j}_2 & \boldsymbol{j}_3, \mu_3 \\ \boldsymbol{m}_1 & \boldsymbol{m}_2 & \boldsymbol{m}_3 \end{array}\right) |\boldsymbol{j}_1, \boldsymbol{m}_1\rangle \otimes |\boldsymbol{j}_2, \boldsymbol{m}_2\rangle, \tag{2.45}$$

where μ_3 is the label for the additional multiplicity arising from the tensor product of the initial two irreps due to the the coupling, and is known as the outer multiplicity. The CG coefficients are zero unless $\boldsymbol{m}_1 + \boldsymbol{m}_2 = \boldsymbol{m}_3$ [111].

The Wigner-Eckart theorem specifies the form of the matrix elements of $K_{\boldsymbol{J}, \boldsymbol{M}, \alpha}$ in the basis $\{|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\}$ as we now discuss. For a simply reducible algebra, the Wigner-Eckart theorem states that the matrix elements of $K_{\boldsymbol{j},\boldsymbol{m},\alpha}$ are given by

$$\langle \boldsymbol{j}', \lambda'; \boldsymbol{m}' | K_{\boldsymbol{J},\boldsymbol{M},\alpha} | \boldsymbol{j}, \lambda; \boldsymbol{m} \rangle = \left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}' \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array} \right) \langle \boldsymbol{j}', \lambda' \parallel K_{\boldsymbol{J},\alpha} \parallel \boldsymbol{j}, \lambda \rangle, \tag{2.46}$$

where $\langle \boldsymbol{j}', \lambda' \parallel K_{\boldsymbol{J},\alpha} \parallel \boldsymbol{j}, \lambda \rangle$ is known as the reduced matrix element independent of $\boldsymbol{m}$ and $\boldsymbol{m}'$, and $\left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}' \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array} \right)$ are the generalized CG-coefficients. If the algebra is not simply reducible, the general form of the Wigner-Eckart theorem takes the form

$$\langle \boldsymbol{j}', \lambda'; \boldsymbol{m}' | K_{\boldsymbol{j},\boldsymbol{M},\alpha} | \boldsymbol{j}, \lambda; \boldsymbol{m} \rangle = \sum_{\mu'} \left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}', \mu' \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array} \right) \langle \boldsymbol{j}', \lambda' \parallel K_{\boldsymbol{J},\alpha} \parallel \boldsymbol{j}, \lambda \rangle_{\mu'}, \tag{2.47}$$

where μ' is the outer multiplicity of the Kronecker product.

A set of linearly independent operators $\{K_{\boldsymbol{j},\boldsymbol{m}}\}_{\boldsymbol{m}}$, for a with fixed $\boldsymbol{j}$, is said to form an irreducible tensor operator belonging to the representation labeled by $\boldsymbol{j}$ under the group G if under the operation of the group they transform as

$$U(g) K_{\boldsymbol{j},\boldsymbol{m}} U^{-1}(g) = \sum_{\boldsymbol{m}'} \langle \boldsymbol{j}; \boldsymbol{m} | U(g) | \boldsymbol{j}, \boldsymbol{m}' \rangle \; K_{\boldsymbol{j},\boldsymbol{m}'}. \tag{2.48}$$

The irreducible tensor operators with respect to the $SU(2)$ algebra are also known as spherical tensor operators (for example see pp. 193-195 in [3]). We utilize the Wigner-Eckart theorem extensively in Chapter 4.

2.3 Entanglement as a quantum resource

2.3.1 Composite systems

The Hilbert space of a composite quantum system comprised of two subsystems, each associated with Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_B$ respectively, is the Kronecker product of the individual Hilbert spaces,

$$\mathscr{H}_A \otimes \mathscr{H}_B. \tag{2.49}$$

The generalization for more than two systems is straightforward. The Hilbert space of a composite system of n subsystems is the tensor product of the n Hilbert spaces. Here, we only consider the case of bipartite systems.

If the joint state of a composite system $\rho \in \mathcal{B}(\mathscr{H})$ can be expressed as the tensor product of states acting on each subsystem,

$$\rho_{AB} = \rho_A \otimes \rho_B, \tag{2.50}$$

where $\rho_A \in \mathcal{B}(\mathscr{H}_A)$, and $\rho_B \in \mathcal{B}(\mathscr{H}_B)$, the system is said to be in a product state.

Definition 15. *A system whose state can be expressed as a convex sum of product states*

$$\rho_{AB} = \sum_i p_i \, \rho_A \otimes \rho_B, \tag{2.51}$$

is said to be in a separable state, where the $p_i \in \mathbb{R}^+$ are probabilities that sum to one. We denote the set of separable states by SEP. If a system is not in a separable state, it is said to be entangled.

Given the state of a composite system, the state of a subsystem is reached by taking the partial trace of the overall state

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}). \tag{2.52}$$

The resulting density operator is known as the reduced density operator. The partial trace over the system B is defined as

$$\mathrm{Tr}_B\left(|a_1\rangle_A\langle a_2| \otimes |b_1\rangle_B\langle b_2|\right) := \mathrm{Tr}\left(|b_1\rangle_B\langle b_2|\right)\, |a_1\rangle_A\langle a_2|. \tag{2.53}$$

The reduced density operator for the system B is calculated in an analogous way.

2.3.2 Quantum operations

The general form of a quantum transformation on the state of a composite system that we consider is described by the completely positive (CP)-map, $\mathcal{E} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$, with the operator sum decomposition

$$\mathcal{E}(\rho_{AB}) = \sum_i K_i \, \rho_{AB} \, K_i^\dagger.$$

The operators K_i are the Kraus operators discussed in Section 2.2. A quantum operation is separable if its operator elements can be written as a tensor product of operators, $K_i = K_{i,A} \otimes K_{i,B}$. If K_i cannot be expressed as a tensor product, the transformation $\mathcal{E}$ is said to be non-separable.

2.3.3 Generalized measurements and POVMs

Measurements in quantum mechanics are described by a set of operators $\{M_i\}$, known as measurement operators, that act on the Hilbert space of the system under measurement. Each index i corresponds to one of the possible outcomes of the measurement. If the state of the system is described by ρ, then the probability of outcome i is given by

$$p_i = \mathrm{Tr}(M_i^\dagger M_i \, \rho), \tag{2.54}$$

and the (normalized) state of the system after the measurement is

$$\rho_i = \frac{M_i \, \rho \, M_i^\dagger}{p_i}. \tag{2.55}$$

The sum of the probabilities p_i must add to one. Thus, the measurement operators must satisfy

$$\sum_i M_i^\dagger M_i = I, \tag{2.56}$$

known as the completeness equation.

If the measurement operators are a set of mutually orthogonal projectors P_i, so that $P_i P_i' = \delta_{i,i'} P_i$, then the measurement is called a projective measurement.The different possible states after the measurement are orthogonal to each other and are thus fully distinguishable.

An observable is a Hermitian operator acting on the system's Hilbert space. Consider the spectral decomposition of an observable A,

$$A = \sum_i a_i P_i. \tag{2.57}$$

Each P_i is a projector to the eigenspace of A with eigenvalue a_i. Whenever the i^{th} outcome is actualized after the measurement, it is understood that the observable A is measured to have the magnitude a_i. If the resulting state after a projective measurement undergoes the same projective measurement immediately after the first one, the outcome will remain the same and the resulting state will not change [67].

However, not all measurements need be projective measurements. Other measurement schemes also exist that correspond to more general measurement operations, where, for example, a projective measurement is performed on a larger system and then the ancillary parts traced out. In such cases the states after the measurement need not all remain orthogonal to each other, and a second round of the same measurement could change the outcome. Measurements comprised of a general set of measurement operators are known as *generalized* measurements as long as the operators satisfy the completeness equation (2.56) [67].

In some cases, the actual eigenvalues of the observable being measured are not of primary importance. Rather, we are interested only in the probabilities of each outcome. In order to study the statistics of generalized measurements, we define

$$T_i := M_i^\dagger M_i. \tag{2.58}$$

The set of operators T_i are sufficient to determine the probabilities of different measurement outcomes:

$$p_i = \mathrm{Tr}(T_i \rho). \tag{2.59}$$

The set $\{T_i\}$ is called a *positive operator-valued measure*, or a *POVM*. The two conditions for a set of operators to be a POVM are that they be positive and satisfy

$$\sum_i T_i = I. \tag{2.60}$$

Projective measurements, for example, are special cases of POVM where T_i are equal to the projectors P_i. Of course, under additional restrictions like a SSR, not every POVM can be implemented. Nevertheless, for such restrictions a subset of both projective and generalized measurements could still feasible, *i.e.* those measurements whose POVM still satisfy the SSR restrictions.

2.3.4 Local operations with classical communication (LOCC)

An important class of separable operations is called local operations with classical communication (LOCC). The LOCC transformations correspond to the following scenario: Alice and Bob can only perform local operations on their share of the bipartite state, but they are allowed to communicate classically and correlate their local operations with each other. An LOCC transformation can always be decomposed in to Kraus elements of the form $K_i = M_{i,A} \otimes U_{i,B}$, where $M_{i,A}$ is a generalized measurement by Alice, and $U_{i,B}$ is a unitary by Bob [67].

2.3.5 Pure state entanglement

A bipartite state $|\psi\rangle_{AB}$ can alway be expressed in a standard form as

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\, |v_i\rangle_A \otimes |w_i\rangle_B, \tag{2.61}$$

where $\{|v_i\rangle_A\}$ and $\{|w_i\rangle_B\}$ are orthonormal states. The basis in which the state is expanded in (2.61) is particularly suitable for the study of entanglement as it simplifies many features of the bipartite state. The real numbers $\{p_i\}$ are known as Schmidt coefficients. A direct corollary is that the reduced states ρ_A and ρ_B (see Eq. (2.52)) have the same eigenvalues. If we sort the Schmidt coefficients $p = (p_1, \cdots, p_d)$ and $q = (q_1, \cdots, q_d)$ of two pure states, $|\psi\rangle_{AB}$ and $|\phi\rangle_{AB}$ respectively, in decreasing order $p_1 \geq \cdots \geq p_d$, and $q_1 \geq \cdots \geq q_d$, where d is the dimension of the system's Hilbert space, then p is said to be majorized by q, denoted by $p \preceq q$, if the following inequalities hold,

$$\begin{aligned} p_1 &\leq q_1, \\ p_1 + p_2 &\leq q_1 + q_2 \\ &\vdots \\ p_1 + \cdots + p_d &\leq q_1 + \cdots + q_d. \end{aligned} \tag{2.62}$$

The states being normalized, the last term is actually always an equality, where both sides are of course equal to one.

Theorem 11. *(Nielsen's theorem) [67]. The state $|\psi\rangle_{AB}$ can be transformed to a state $|\phi\rangle_{AB}$ by LOCC if and only if $p \preceq q$, or equivalently, if and only if,*

$$E_k\left(|\psi\rangle_{AB}\right) \geq E_k\left(|\phi\rangle_{AB}\right), \quad k = 1, \cdots, d, \tag{2.63}$$

where $E_k\left(|\psi\rangle_{AB}\right) = \sum_{i=k}^{d} p_i$.

Definition 16. *The functions*

$$E_k\left(|\psi\rangle_{AB}\right) := \sum_{i=k}^{d} p_i \tag{2.64}$$

are known as Vidal's monotones [95].

A similar condition exists for non-deterministic transformations in terms of the average monotones [50].

Theorem 12. *The state $|\psi\rangle_{AB}$ can be transformed by LOCC to one of the states in the ensemble $\{|\phi_i\rangle_{AB}, p_i\}$, each $|\phi_i\rangle_{AB}$ with probability p_i respectively, if and only if,*

$$E_k\left(|\psi\rangle_{AB}\right) \geq \sum_i p_i\, E_k\left(|\phi_i\rangle_{AB}\right), \quad k = 1, \cdots, d. \tag{2.65}$$

Finally, the following corollary deals with the case of single copy stochastic transformation of two pure states.

Corollary 13. *The maximum probability to convert $|\psi\rangle$ to $|\phi\rangle$ using LOCC is equal to*

$$P_{\max}\left(|\psi\rangle \to |\phi\rangle\right) = \min_{k=1,\cdots,d}\left\{\frac{E_k\left(|\psi\rangle\right)}{E_k\left(|\phi\rangle\right)}\right\}. \tag{2.66}$$

Recall the maximally entangled bipartite states, or the Bell states, of Eq. (1.4):

$$\begin{aligned} |\psi^{\pm}\rangle &:= \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B\right) \\ |\phi^{\pm}\rangle &:= \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B\right). \end{aligned} \tag{2.67}$$

The Bell states can be transformed to each other by local unitaries. The entanglement of Bell states is greater than all other two-qubit states with unequal amplitudes. The entanglement is greater in two different ways. For one, a Bell state can be deterministically transformed to states with unequal amplitudes, but the reverse is not possible. On the other hand, using Bell states to perform tasks, such as teleportation, has a higher success rate than when one uses any other bipartite state, where the success rate is measured by some suitable figure of merit. For pure states, the two notions of strength of entanglement coincide. For mixed states the two notions are not in general equivalent. For the case of higher dimensional states, generalizations of Bell states in the form of full-rank states comprised of tensor products of Bell states, are more entangled than all other states.

For a general pure state, the entropy of entanglement is given by,

$$E(|\psi\rangle_{AB}) := S\left(\mathrm{Tr}_B\left(|\psi\rangle_{AB}\langle\psi|\right)\right), \tag{2.68}$$

where $S(\rho) = -\mathrm{Tr}(\rho\log\rho)$ is the von Neumann entropy. The entropy of entanglement quantifies the asymptotic rate of conversion of multiple copies of a pure state to (any one of) the Bell states. The entanglement of a Bell state thus acts as a unit of entanglement strength and is known as an ebit. For mixed states, the convex roof extension of the entropy of entanglement can be regarded as a measure of entanglement. The measure is known as the entanglement of formation, and is formally defined as

$$E_A(\rho) := \min_{\{|\psi_i\rangle, p_i\}} \sum_i p_i \; E(|\psi\rangle_{AB}). \tag{2.69}$$

The quantification of entanglement in terms of the LOCC transformations in the asymptotic limit is one possible route to take to quantify the entanglement as a resource.

Another approach to identifying entanglement measures is to assign entanglement to a state in terms of some measure of 'distance' of that state to the set of separable states. Examples of such *distance-based* measures of entanglement that we use later in the thesis (see section 5.6) include the *geometric* measure of entanglement, the *relative entropy* of entanglement (REE) and the *robustness* of entanglement. At this point, we only give a formal definition for each of them:

Definition 17. *The geometric measure $G(\rho)$ [100] is defined as*

$$G(\rho) := -\log_2 \left\{ \max_{w \in SEP} Tr(\rho w) \right\}. \tag{2.70}$$

Definition 18. *The relative entropy of entanglement (REE) is defined to be*

$$E_R(\rho) := \max_{w \in SEP} S(\rho \parallel w), \tag{2.71}$$

where

$$S(\rho \parallel w) := Tr(\rho \log w) - S(\rho), \tag{2.72}$$

is known as the relative entropy of the states ρ and w. For a review of the role of relative entropy in quantum information theory, including entanglement theory, see [90].

Definition 19. *The global robustness of entanglement [96] is the function*

$$r_E(\rho) := \min \left\{ t \,\middle|\, \frac{1}{1+t} (\rho + t\Delta) \in SEP, \; \Delta \in \mathcal{B}(\mathscr{H}) \right\}. \tag{2.73}$$

where $\mathscr{H}$ is the Hilbert space of the state ρ.

Finally, another alternative route is to take an axiomatic approach and consider any real function that changes monotonically under LOCC transformations as a function that quantifies some aspect of the state's entanglement. The ensuing entanglement monotones are examples of a more general notion of monotone in resource theories. We consider them in a general setting in the next section.

2.4 Monotones in resource theories

In this section, we establish a set of reasonable conditions that a valid asymmetry measure should satisfy, and we provide insight and background for this choice of conditions.

Every restriction on quantum operations defines a resource theory that determines how quantum states that cannot be prepared under the restriction may be manipulated and used to circumvent the restriction. Here we discuss briefly how the strength of these quantum states as resources is quantified. We will focus on entanglement theory and the theory of asymmetry that is associated with a group G of transformations. In entanglement theory, the quantum operations or CP-maps are confined to LOCC, and only separable states can be prepared by LOCC (assuming no access to previously existing entanglement). In the resource theory of quantum asymmetry, the only allowed operations are G-covariant CP maps, and the only states that can be prepared without any resources are G-invariant states.

A quantum state cannot turn into a stronger resource by the set of restricted (or allowed) operations. Therefore, the strength of the resource must be quantified by functions that do not increase under the set of allowed operations, *ie.* by monotones.

The most general quantum transformations that we consider in the present thesis are those that convert an initial state ρ into one of a set of possible final states, say σ_x, occurring with probability p_x, where the index x is a positive integer, $x \in \mathbb{Z}^+$. Such a general quantum transformation is described by a CP map $\mathcal{E} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ that is itself composed of a number of CP (in general trace decreasing) maps $\{\mathcal{E}_x\}$, so that $\mathcal{E} = \sum_x \mathcal{E}_x$, and

$$\sigma_x := \mathcal{E}_x[\rho]/p_x, \tag{2.74}$$

where the probability $p_x = \mathrm{Tr}\,(\mathcal{E}_x[\rho])$. We say that $\mathcal{E}$ is G-symmetric if all $\{\mathcal{E}_x\}$ are G-covariant.

The ensemble of outcomes is written as $\{\sigma_x, p_x\}$. This ensemble can be equivalently expressed as a density operator

$$\tilde{\sigma} := \sum_x p_x \, \sigma_x \otimes |x\rangle_I\langle x|. \tag{2.75}$$

The set of states $\{|x\rangle_I\}$ consist of mutually orthogonal unit states belonging to the Hilbert space $\mathscr{H}_I$ of an ancillary system I, such that when the system is in the state σ_x the ancillary system is prepared in the state $|x\rangle$ labeled by the same index x.

States of the ensemble $\{\sigma_x, p_x\}$ can always be prepared by first preparing the density operator $\tilde{\sigma}$ and then performing the measurement $\mathcal{M} = \{|x\rangle_I\langle x|\}$ on the ancillary system I and keeping a record of the outcome. We assume there is a second ancillary system R that records the label x of the measurement outcome. For example, the system R could be the measuring device that by the end of the measuring process ends up in the state $\tau_x^{(R)}$ whenever $|x\rangle_I$ was the outcome of the measurement. We also assume the states $\tau_x^{(R)}$ with different values of x are mutually orthogonal and belong to a set of orthogonal (or classical) states, each labeled by a different value of the index x.

The density operator $\tilde{\sigma}$ can be reproduced again from the ensemble by losing the information about the measurement outcome, *ie.* by *tracing out* the record-keeping ancillary system from the joint state of the system and both ancillas I and R after the measurement:

$$\tilde{\sigma} = \mathrm{Tr}_R \left(\sum_x \sigma_x \otimes |x\rangle_I \langle x| \otimes \tau_x^{(R)} \right). \tag{2.76}$$

We conclude that the density operator $\tilde{\sigma}$ contains the same information as the ensemble $\{\sigma_x, p_x\}$.

A single state $\rho \in \mathscr{H}$ is, in effect, an ensemble with one member. The non-deterministic transformations that convert the state ρ to an ensemble $\{\sigma_x, p_x\}$ have a deterministic counterpart that converts the state $\rho \otimes |1\rangle\langle 1|$ to the state $\tilde{\sigma}$ with probability one. We can now define an asymmetry, or similarly an entanglement monotone, in a general setting:

Definition 20. *A function* $\mathfrak{A} : \mathcal{B}\left(\mathscr{H} \otimes \mathscr{H}_I\right) \to \mathbb{R}^+$ *is called an asymmetry (or, similarly, an entanglement) monotone, if, for any state* $\rho \in \mathcal{B}\left(\mathscr{H}\right)$*, it satisfies*

$$\mathfrak{A}\left(\rho \otimes |1\rangle_I \langle 1|\right) \geq \mathfrak{A}\left(\sum_x p_x \, \sigma_x \otimes |x\rangle_I \langle x| \right), \tag{2.77}$$

where the states σ_x *are the states that* ρ *is converted to by* G*-covariant (or by LOCC) transformations (see Eq. (2.74)).*

Of course, if the outcome of the transformation is a single state σ, *i.e.* if the transformation $\rho \to \sigma$ is already deterministic to begin with, then Definition 20 implies

$$\mathfrak{A}\left(\rho \otimes |1\rangle_I \langle 1|\right) \geq \mathfrak{A}\left(\sigma \otimes |1\rangle_I \langle 1|\right). \tag{2.78}$$

Thus, for every state $\rho \in \mathcal{B}(\mathscr{H})$, one can also define the function $A(\rho) := \mathfrak{A}\left(\rho \otimes |1\rangle_I \langle 1|\right)$ of ρ alone, that changes monotonically under *deterministic* G-covariant (or LOCC) transformations:

Definition 21. *The function* $A : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+ : \rho \mapsto \mathfrak{A}\left(\rho \otimes |1\rangle_I \langle 1|\right)$ *is called a deterministic monotone.*

A natural question to ask at this stage is how the deterministic monotone functions $A(\rho)$ and $A(\sigma_x)$ relate to each other when ρ is converted to one of the states of the ensemble $\{\sigma_x, p_x\}$ with probability less than one. The answer is that a deterministic monotone A need not always change monotonically in case of a *non-deterministic* transformation, even though the corresponding monotone $\mathfrak{A}$, in terms of which A is defined, always does.

One possible situation in which a deterministic monotone A does change monotonically is, for example, when $A(\rho) \geq A\left(\sum_x p_x \sigma_x\right)$ and A is a linear or a convex function so that $A\left(\sum_x p_x \sigma_x\right) \geq \sum_x p_x A(\sigma_x)$. More generally, if a deterministic monotone A has the (additional) property that it remains non-increasing on average under non-deterministic transformations, it belongs to a category of monotones known as *ensemble* monotones:

Definition 22. *The asymmetry (or entanglement) monotone* $A : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+$ *is called an ensemble monotone if it satisfies*

$$A(\rho) \geq \sum_x p_x \, A(\sigma_x), \tag{2.79}$$

whenever a G*-covariant (or LOCC) transformation converts a given state* ρ *to one of the states of an ensemble* $\{\sigma_x, p_x\}$.

A well-known example of an ensemble monotone is the entropy of entanglement (2.68). A counterexample is the Z_2-monotone $A_{Z_2}(|\psi\rangle\langle\psi|) = -\log(|p_0 - p_1|)$ for qubit pure states of the form $|\psi\rangle = p_0|0\rangle + p_1|1\rangle$ [37]. The function A_{Z_2} is not an ensemble monotone as it becomes infinite if even one of the final states of a non-deterministic transformation is the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Thus, the set of ensemble monotones is a strict subset of the set of deterministic monotones of Definition 21.

Finally, if the function A remains a monotone for each outcome σ_x, separately:

$$A(\rho) \geq A(\sigma_x), \;\; \forall \sigma_x \in \{\sigma_x, p_x\}\,. \tag{2.80}$$

then A is known as a *stochastic* monotone [37]. The Schmidt-rank of a pure state is an example of a stochastic entanglement monotone.

Clearly, for two sets of numbers, if the i^{th} number of the first set is no larger than the i^{th} number of the second set, then the average over the first set is no larger than the average over the second set. Thus, every stochastic monotone is automatically an ensemble monotone as well (and of course a deterministic monotone too). The reverse, however, is not always true in entanglement theory [48]. The entropy of entanglement, for example, is not a stochastic monotone. Nor is it true in the resource theory of asymmetry that every ensemble monotone is automatically a stochastic monotone, as shown in the case of A_{Z_2}, among other examples [37].

Finally, let us define the notion of faithfulness of a monotone:

Definition 23. *An asymmetry (or an entanglement) monotone $A : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+$ is faithful if it satisfies the following condition: $A(\rho) = 0$ if and only if ρ is a G-invariant (or, respectively, a separable) state.*

In other words, if a faithful monotone assigns the value zero to a state, we can be sure that the state is not a resource (and consequently no other monotone will assign a non-zero value to that state either).

Of course, specific monotones can satisfy additional conditions. One such characteristic is convexity. The monotone A is convex, if for any ensemble $\{\sigma_i, p_i\}$,

$$\sum_i p_i\, A(\sigma_i) \geq A\left(\sum_i p_i \sigma_i\right). \tag{2.81}$$

However, in general a condition such as convexity may not be necessary for a valid entanglement, or asymmetry, monotone. For example, the logarithmic negativity (which provides an upper bound for distillable entanglement) is a useful measure of entanglement but it is not convex [70]. In Chapter 3, we focus on convex measures. However, for the general result expounded in Chapter 4 the extra conditions like convexity are not required.

Chapter 3

Constructing monotones for quantum phase references in totally dephasing channels

Before presenting the main result of the thesis, it is instructive to introduce the key ideas of our approach in a simpler setting. In this chapter, we consider the special case of the Abelian Lie group U(1) as the symmetry group. We also confine our attention primarily to pure states. In the next chapter, we consider the general case that applies to all semi-simple compact Lie groups, and to mixed states as well as pure states.

This chapter is organized as follows: In Section 3.1, we briefly review the structure of the resource theory associated with the group U(1). In Section 3.2 we introduce pure-state asymmetry monotones and prove two useful lemmas that we use in later sections. In Section 3.3, we introduce the first sketch of the mapping to bipartite states. In 5 we present some of the applications that follow from the mapping. Already, despite the simple and the limited scope that we have chosen in this chapter, we see that whole classes of new asymmetry monotones can be constructed for the symmetry group U(1). Even though U(1) has a simple group structure, the resource theory associated with it is important in its own right. Throughout this chapter, we use the terms asymmetry and frameness interchangeably. Also, we refer to the restriction as U(1)-covariance, U(1)-superselection rule, or U(1)-SSR for short.

3.1 Covariant transformations for the symmetry group U(1) and the lack of shared phase references

Now we consider the case of U(1)-covariance following the approach of Gour and Spekkens [37]. The Abelian group U(1) has a unitary representation $\theta \mapsto U(\theta) = \exp(-\imath\theta\hat{n})$ with spectrum $\{n \in \mathbb{Z}^+\}$. We refer to $\hat{n}$ as the number operator.

The Hilbert space of the particular physical system under study can be expressed as the direct sum $\mathscr{H} = \bigoplus_n \mathscr{H}_n$ with n an irrep index for U(1) and $\mathscr{H}_n$ the multiplicity subspaces. The eigenstates $|n, \beta\rangle$ of the number operator form a basis for $\mathscr{H}_n$ where β is a multiplicity index. Operations on multiplicity spaces are unaffected by the U(1)-SSR, and, as a result, any pure state can be transformed via the U(1)-covariant unitary transformation to a standard form. We already discussed the standard form of pure states for a general group in Section 5.1. Here we once again develop the specific form of the transformation for the group Abelian U(1) where the irrep label and the weight label are identical. Consider the pure state

$$|\psi\rangle = \sum_n c_n |\psi_n\rangle, \tag{3.1}$$

where $|\psi_n\rangle \in \mathscr{H}_n$ are normalized states, and let $\lambda_n := |c_n|^2$. We apply the Gram-Schmidt process to extend $|\psi_n\rangle$ to a full orthonormal basis $\{|\psi_n\rangle\} \cup \{|\phi_{n,\beta}\rangle\}_\beta$ of the subspace $\mathscr{H}_n$. The extra states $|\phi_n\rangle$ do not affect the state $|\psi\rangle$, but they are needed to fully specify the unitary transformation that takes $|\psi\rangle$ to its standard form. The unitary transformation

$$U := \sum_n \left(\frac{c_n^*}{|c_n|} |n, 0\rangle\langle\psi_n| + \sum_{\beta \neq 0} |n, \beta\rangle\langle\phi_{n,\beta}| \right), \tag{3.2}$$

is U(1)-covariant, in fact it is U(1)-invariant, and takes the state $|\psi\rangle$ to the standard form,

$$|\psi\rangle = \sum_n \sqrt{\lambda_n} |n\rangle, \tag{3.3}$$

where $|n\rangle$ is shorthand notation for a fixed choice of the multiplicity index, for example, the state $|n,0\rangle$. The spectrum of the state $|\psi\rangle$ is defined to be the set,

$$\operatorname{spec}(|\psi\rangle) := \{n; \lambda_n > 0\}. \tag{3.4}$$

The U(1)-covariant operator $\mathcal{E}$ can be expressed in a Kraus operator decomposition as

$$\mathcal{E}[\rho] = \sum_{\ell} \hat{K}_{\ell}^{(\alpha)} \rho \hat{K}_{\ell}^{(\alpha)\dagger}, \tag{3.5}$$

where the Kraus operators are of the form,

$$\hat{K}_{\ell}^{(\alpha)} = \sum_{n} k_{\ell,n}^{(\alpha)} |n+\ell\rangle\langle n|, \tag{3.6}$$

for ℓ an integer, and for $k_{\ell,n}^{(\alpha)} \in \mathbb{C}$ such that $\sum_i |k_{\ell,n}^{(\alpha)}|^2 \leq 1$ with equality holding if the transformation is trace-preserving [37]. In this notation, ℓ represents the number-shift imposed by the Kraus operator and α an index for a particular ℓ-shifting Kraus decomposition.

States that are not U(1)-invariant are resources that Alice or Bob can use to circumvent SSR restrictions, and asymmetry, or frameness, denotes this quantum resource. Here we focus on the U(1)-SSR that corresponds to lacking a common phase, for example the phase of a laser in homodyne measurements or orientation in a plane.

3.1.1 U(1)-asymmetry and phase references

Let us go over the link between symmetry resources and reference frames for the particular case of the symmetry group U(1). We cast the theory in a quantum communication context in which two parties, Alice and Bob, collaborate so that Alice can effect a completely-positive map $\mathcal{E}$ to her state $\rho \in \mathcal{B}(\mathscr{H})$, for $\mathscr{H}$ the Hilbert space and $\mathcal{B}(\mathscr{H})$ the space of bounded operators that act on $\mathscr{H}$. Also let $\mathcal{P}(\mathscr{H})$ be the projective space of the Hilbert space $\mathscr{H}$. For a finite Hilbert space $\mathscr{H} = \mathbb{C}^d$, the projective Hilbert space is the complex projective space $\mathbb{PC}^{d-1}$.

Alice and Bob have identical systems, so their Hilbert spaces are isomorphic, but we assume that Alice lacks the tools to perform mapping $\mathcal{E}$ and relies on Bob, who has this capability. Alice sends the state ρ to Bob via a (completely-positive trace-preserving) communication channel $\mathcal{C} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$, but unfortunately Alice and Bob lack shared reference frame information. Lacking shared reference frames implies a superselection rule (SSR) on the transformation $\mathcal{E}$ that Alice, with Bob's collaboration, wishes to implement [8].

The specific channel we consider is a random unitary channel (RUC) for the group U(1). We denote the channel as $\mathcal{U}(\theta)$ such that $\mathcal{U}(\theta)[\rho] = U(\theta)\,\rho\,U^\dagger(\theta)$ for $\theta \in \mathrm{U}(1)$. The group U(1) is the group parametrizing unitary channels connecting Alice to Bob that perform phase shifts. Thus, when Alice and Bob lack shared phase frame information, U(1) is the group of transformations between the frames. The lack of reference frame information is manifested as a complete ignorance of θ by Alice and Bob; mathematically, this complete ignorance corresponds to a uniform prior distribution for θ over the Haar measure for the group U(1), where $\mathrm{d}\mu(\theta) = \frac{1}{2\pi}\mathrm{d}\theta$. If they had some prior knowledge about the actual phase θ_0 that connects the two frames, then the measure $\mathrm{d}\mu(\theta)$ for values of θ close to θ_0 would have to be greater than other values of the phase, and the thus the appropriate measure would no longer be the uniform Haar measure. See the discussion in Section 1.4 for a more detailed analysis.

Alice sends the state ρ to Bob via the channel $\mathcal{U}(\theta_0)$, and Bob then effects the mapping $\mathcal{E}$ and sends the resultant state $\mathcal{E} \circ \mathcal{U}(\theta_0)[\rho]$ back to Alice. For $\mathcal{U}^\dagger(\theta_0)[\rho] := U^\dagger(\theta_0)\,\rho\,U(\theta_0)$, and given Alice's uniform lack of knowledge of θ, she receives the state

$$\tilde{\mathcal{E}}_{\mathrm{U}(1)}[\rho] := \int_{\mathrm{U}(1)} \mathrm{d}\mu(\theta)\,\mathcal{U}^\dagger(\theta) \circ \mathcal{E} \circ \mathcal{U}(\theta)[\rho]. \tag{3.7}$$

As this relation holds for any ρ, we can write

$$\tilde{\mathcal{E}}_{\mathrm{U}(1)} := \int_{\mathrm{U}(1)} \mathrm{d}\mu(\theta)\,\mathcal{U}^\dagger(\theta) \circ \mathcal{E} \circ \mathcal{U}(\theta) =: \mathcal{G}\left(\mathcal{E}\right), \tag{3.8}$$

which is the twirling operation discussed in Chapter 2. Twirling is idempotent: Twirling a twirled operator leaves the twirled operator intact. This imposes a direct-sum structure on Alice's Hilbert space, which is a SSR [8].

Of course, Alice and Bob can continue this procedure and send the state back and forth, with Bob each time effecting a different map $\mathcal{E}_1$, $\mathcal{E}_2, \ldots$. However every time the same (unknown) angle θ_0 connects the two local reference frames. Thus, the final state that Bob sends to Alice after k consecutive repetitions of the procedure is the state $\mathcal{E}_k \circ \cdots \circ \mathcal{E}_1 \circ \mathcal{U}(\theta_0)[\rho]$, and Alice receives the state

$$\tilde{\mathcal{E}}_{\mathrm{U}(1)}[\rho] := \int_{\mathrm{U}(1)} \mathrm{d}\mu(\theta)\, \mathcal{U}^\dagger(\theta) \circ \mathcal{E}_k \circ \cdots \circ \mathcal{E}_1 \circ \mathcal{U}(\theta)[\rho]. \tag{3.9}$$

In other words, only a single collective twirling is performed at the final state. Hence, we can consider the consecutive repeated uses of the channel as a single collective procedure that we denote by $\mathcal{E} = \mathcal{E}_k \circ \cdots \circ \mathcal{E}_1$, and it is this collective map $\mathcal{E}$ that we use henceforth.

A U(1)-covariant map $\mathcal{E}$ satisfies $\mathcal{E} \circ \mathcal{U}(\theta) = \mathcal{U}(\theta) \circ \mathcal{E}$ for all θ, or equivalently, $\tilde{\mathcal{E}}_{U(1)} = \mathcal{E}$. Therefore the lack of reference information is not an impediment for Alice and Bob to collaborate to effect $\mathcal{E}$ as long as $\mathcal{E}$ is U(1)-covariant. Note that we express everything with respect to Alice's RF and make a distinction between the preparation procedure by Alice and the consequent transformations of the prepared state performed by Bob, who has access to the prepared state only through the twirling channel. Alice can prepare any state, including coherent superpositions that are restricted by the SSR.

However, as all operations afterwards are performed by Bob who does not have access to Alice's RF, the transformations of the state have to be U(1)-covariant. Thus, a coherent superposition, like the state $|\psi\rangle$ in Eq. (3.3), is distinct from the mixture

$$\rho := \sum_n \lambda_n |n\rangle\langle n|, \tag{3.10}$$

that results from twirling the state. Let us compare the case where Alice prepares the coherent state $|\psi\rangle$ versus the case where she prepares the invariant state ρ. Of course, Bob receives the twirled state ρ in either case and he is free to perform any operation on the state he receives relative to his own RF before sending the state back to Alice.

With respect to Alice's RF, however, the net result is a U(1)-covariant transformation on a coherent superposition in the first case and on the twirled mixture in the second case (see Eqs. (3.7) and (3.8)). The two cases are distinct. For example, $|\psi\rangle$ can be transformed to ρ while ρ cannot be transformed to $|\psi\rangle$ by U(1)-covariant operations, *i.e.* by Bob when viewed in Alice's RF. A state like $|\psi\rangle$ that is not U(1)-invariant is a resource, while U(1)-invariant states like ρ are not. Alice can accompany a resource state (known to herself and to Bob) with the target state that Bob is supposed to act on and send them together to Bob. This way, the resource state acts as a token of Alice's phase reference and can be used to partially overcome the SSR-restriction on transformations [8, 9]. The situation is a particular instance of the general detailed discussion in Section 1.4, now applied to the group U(1). If Alice accompanies a U(1)-invariant state instead of a resource with the target state, this is no longer possible. Symmetric states, *i.e.* states that are U(1)-invariant, are non-resource states.

3.2 Pure-state monotones

In this section we briefly consider some of the features of monotones primarily defined for pure states only. Pure-state monotones are functions that behave monotonically under the more restricted set of allowed operations that map pure states to pure states only. General monotones defined over all states, of course, must remain a monotone when applied to pure states, but the reverse need not be true. Pure state monotones, thus comprise a larger category that contains the set of all monotones. In what follows, we use the terminology of the resource theory of asymmetry and the restriction of operations to U(1)-covariant transformations, but, again, the discussion equally applies to all resource theories. First, we formally define *pure-state* asymmetry monotones that are a special case of asymmetry monotones discussed in Section 2.4, namely ensemble monotones, but now defined over the projective space associated with the system's Hilbert space.

Definition 24. *A function,*

$$A_{pure} : \mathcal{P}(\mathscr{H}) \ \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \mapsto A_{pure}\left(|\psi\rangle\langle\psi|\right), \tag{3.11}$$

where $\mathcal{P}(\mathscr{H})$ denotes the projective space of the Hilbert space $\mathscr{H}$, is an ensemble pure-state *asymmetry monotone if it satisfies*

A1. $A_{pure}(|\psi\rangle\langle\psi|) = 0$ *for any U(1)-invariant state* $|\psi\rangle\langle\psi| = \mathcal{G}(|\psi\rangle\langle\psi|)$*;*

A2. $A_{\ pure}(|\psi\rangle\langle\psi|) \ \geq \ \sum_x p_x A_{pure}(|\phi_x\rangle\langle\phi_x|)$, *for U(1)-covariant transformations* $\mathcal{E}_x$, *such that* $|\phi_x\rangle\langle\phi_x| := \mathcal{E}_x[|\psi\rangle\langle\psi|]/p_x, \ p_x := Tr\left(\mathcal{E}_x[|\psi\rangle\langle\psi|]\right).$

Note that whereas entanglement monotones are zero whenever the state is separable, the asymmetry monotones are zero when the state is invariant. Naturally, in the case of pure-state asymmetry monotones, the monotone is zero when the pure state is invariant.

If an ensemble asymmetry monotone already exists for pure states, one way to extend the pure-state monotone to a measure defined for all states ρ is according to the following definition:

Definition 25. *Given a pure-state asymmetry monotone*

$$A_{pure} : \mathcal{P}(\mathscr{H}) \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \mapsto A_{pure}\left(|\psi\rangle\langle\psi|\right),$$

the convex-roof extension A is defined by

$$A : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+ : \rho \mapsto A(\rho) = \min_{\{|\psi_i\rangle, p_i\}} \sum_i p_i \ A_{pure}\left(|\psi_i\rangle\langle\psi_i|\right), \tag{3.12}$$

with the minimum taken over all possible pure-state decompositions of $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

For pure states (*i.e.* rank-one density operators) the two monotones are of course always equal:

$$A(|\psi\rangle\langle\psi|) = A_{\text{pure}}(|\psi\rangle\langle\psi|), \quad \forall|\psi\rangle \in \mathscr{H}. \tag{3.13}$$

As we presently show, the convex-roof extension of a pure-state ensemble monotone is an ensemble monotone for all states based on Definition 22. To see this, consider the following two lemmas that follow directly from the definition of the convex-roof extension.

Lemma 14. *The convex-roof extension of a pure-state asymmetry monotone is a convex function.*

Proof. Let $\rho = \sum_i p_i \rho_i$, and let $\rho_i = \sum_j p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$ be the optimal decomposition of ρ_i in the sense of Eq. (3.12). The minimum average asymmetry of ρ is reached either by the sum

$$A(\rho) = \sum_{i,j} p_i p_{ij} A_{\text{pure}}\left(|\psi_{ij}\rangle\langle\psi_{ij}|\right) = \sum_i p_i A(\rho_i), \tag{3.14}$$

or by some other ensemble $\left\{|\phi_\ell^{(\alpha)}\rangle, q_\ell\right\}$ forming ρ, in which case

$$A(\rho) = \sum_\ell q_\ell A_{\text{pure}}\left(|\phi_\ell\rangle\langle\phi_\ell|\right) < \sum_i p_i A(\rho_i), \tag{3.15}$$

so that in general $A(\rho) \leq \sum_i p_i A(\rho_i)$. □

Lemma 15. *If*

$$A_{pure} : \mathcal{P}(\mathscr{H}) \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \mapsto A_{pure}\left(|\psi\rangle\langle\psi|\right), \tag{3.16}$$

does not increase on average under U(1)-covariant transformations between pure states (i.e. A_{pure} is a pure-state ensemble monotone) then the convex-roof extension defined by Eq. (3.12) is an ensemble asymmetry monotone (see Definition 22 in Section 2.4).

Proof. We need to show that, for any ρ and U(1)-covariant operation $\mathcal{E} = \sum_x \mathcal{E}_x$, we have $A(\rho) \geq \sum_x p_x A(\sigma_x)$, where

$$\sigma_x := \mathcal{E}_x[\rho]/p_x, \; p_x := \operatorname{Tr}\left(\mathcal{E}_x[\rho]\right), \tag{3.17}$$

with p_x the probability of the x^{th} outcome. The ensemble of outcomes is written as $\{\sigma_x, p_x\}$. Assume $\{|\psi_i\rangle, q_i\}$ is the optimal decomposition of ρ in the sense that

$$A(\rho) = \sum_i q_i A_{\text{pure}}(|\psi_i\rangle\langle\psi_i|). \tag{3.18}$$

Let $\hat{K}^{(\alpha)}_{x,\ell}$ be a choice of Kraus operators for $\mathcal{E}_x$. Each $\hat{K}^{(\alpha)}_{x,\ell}$ effects the mapping

$$|\psi_i\rangle \mapsto |\phi^{(\alpha)}_{x,i,\ell}\rangle := \frac{\hat{K}^{(\alpha)}_{x,\ell}}{\sqrt{q^{(\alpha)}_{x,i,\ell}}} |\psi_i\rangle\,, \tag{3.19}$$

with probability $q^{(\alpha)}_{x,i,\ell} = \|\hat{K}^{(\alpha)}_{x,\ell}|\psi_i\rangle\|^2$. Thus,

$$\sigma_x = \frac{1}{p_x} \sum_{i.\ell,\alpha} q_i q^{(\alpha)}_{x,i,\ell} |\phi^{(\alpha)}_{x,i,\ell}\rangle\langle\phi^{(\alpha)}_{x,i,\ell}|. \tag{3.20}$$

The convex-roof extension is a convex function (Lemma 14) so

$$\begin{aligned} A(\sigma_x) &\leq \frac{1}{p_x} \sum_{i.\ell,\alpha} q_i q^{(\alpha)}_{x,i,\ell} A(|\phi^{(\alpha)}_{x,i,\ell}\rangle\langle\phi^{(\alpha)}_{x,i,\ell}|) \\ &= \frac{1}{p_x} \sum_{i.\ell,\alpha} q_i q^{(\alpha)}_{x,i,\ell} A_{\text{pure}}(|\phi^{(\alpha)}_{x,i,\ell}\rangle\langle\phi^{(\alpha)}_{x,i,\ell}|). \end{aligned} \tag{3.21}$$

The operators $\hat{K}^{(\alpha)}_{x,\ell}$ are themselves U(1)-covariant, and as we have assumed that A_{pure} is an ensemble monotone on pure states,

$$A_{\text{pure}}\left(|\psi_i\rangle\langle\psi_i|\right) \geq \sum_{x,\ell,\alpha} q^{(\alpha)}_{x,i,\ell} A_{\text{pure}}\left(|\phi^{(\alpha)}_{x,i,\ell}\rangle\langle\phi^{(\alpha)}_{x,i,\ell}|\right), \tag{3.22}$$

readily follows. Putting everything together, we obtain

$$\begin{aligned} A(\rho) &= \sum_i q_i\ A_{\text{pure}}\left(|\psi_i\rangle\langle\psi_i|\right) \\ &\geq \sum_{i,x,\ell,\alpha} q_i q^{(\alpha)}_{x,i,\ell} A_{\text{pure}}\left(|\phi^{(\alpha)}_{x,i,\ell}\rangle\langle\phi^{(\alpha)}_{x,i,\ell}|\right) \\ &\geq \sum_x p_x A(\sigma_x). \end{aligned} \tag{3.23}$$

Thus, the convex-roof extension is indeed an ensemble monotone. □

In other words, if a pure-state asymmetry measure is an ensemble monotone on pure states, then the convex-roof extension is an ensemble monotone under all allowed CP-maps. Therefore, we need only consider how a function behaves on pure-state to pure-state transformations in order to determine if it is an ensemble monotone. Also note that we do not interpret the convex-roof extension in terms of the cost of forming the state at this stage. Rather, we treat the convex-roof extension only as an ensemble asymmetry monotone under U(1)-covariant transformations.

3.3 Mapping to bipartite states

We are now in a position to explore the link between U(1)-covariant maps and LOCC transformations. Although we discuss quantum RFs for phase, our results apply to Abelian symmetry groups in general. Suppose there is a U(1)-SSR in place. This means that it is impossible to prepare the state in a coherent superposition like, $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, or $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Instead, only states like $|0\rangle$ or $|1\rangle$ can be prepared, or mixed states like $\frac{1}{2}I = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ that happen to be the twirling of either of the two earlier pure states. However, if by adding a second system, one can prepare the pair of systems in a way that a well-defined relative phase exists between them. The states $|\psi_+\rangle_{SR} = \frac{1}{\sqrt{2}}(|0\rangle_S \otimes |n\rangle_R + |1\rangle_S \otimes |n-1\rangle_R)$ and $|\psi_-\rangle_{SR} = \frac{1}{\sqrt{2}}(|0\rangle_S \otimes |n\rangle_R - |1\rangle_S \otimes |n-1\rangle_R)$ are both preparable despite the SSR on total number, where, by the total number in a state $|n_1\rangle \otimes |n_2\rangle$ we mean the sum $n_1 + n_2$. They are derived from the original states $|\psi_+\rangle$ and $|\psi_-\rangle$ by identifying $|m\rangle$ with $|m\rangle_S \otimes |n-m\rangle_R$ for $m = 0, 1$. Note that both bipartite states are entangled. Under the same mapping, the states $|0\rangle$ or $|1\rangle$ that could be prepared initially and were thus non-asymmetry-resources, are mapped to product states $|0\rangle_S \otimes |n\rangle_R$, and $|1\rangle_S \otimes |n-1\rangle_R$.

The reason such entangled states can be alternatively regarded as a joint state of a system and a phase reference is the following: The states $|\psi_+\rangle$ and $|\psi_-\rangle$ can be expressed alternatively as

$$|\psi_\pm\rangle_{SR} \cong |n\rangle_{\text{Total}} \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_{\text{Rel}} \pm |1\rangle_{\text{Rel}}\right), \tag{3.24}$$

in terms of a different decomposition of the Hilbert space into the 'total number' states and 'relative' states. The relative states are, in fact, in a superposition of different *relative* number states, relative, that is, to the total number n that labels the total number state $|n\rangle_{\text{Total}}$. The total number state $|n\rangle_{\text{Total}}$ thus acts as a bounded-sized substitute for the reference state relative to which coherent superposition of states with different number labels can be prepared, despite the global SSR on the joint system that of course still remains in effect.

The same idea can be immediately generalized to higher dimensions. We bring all states into the standard form without multiplicities: $|\psi\rangle = \sum_n \sqrt{\lambda_n}|n\rangle$. Let $n_{\min}(|\psi\rangle)$ and $n_{\max}(|\psi\rangle)$ denote the minimum and maximum values of n in the number spectrum defined in Eq. (3.4), with the restriction $n_{\max}(|\psi\rangle) - n_{\min}(|\psi\rangle) \leq d$. Let us define,

$$|\tilde{\psi}\rangle = \sum_n \sqrt{\lambda_n}|n\rangle_{\text{S}} \otimes |n_{\max}(|\psi\rangle) - n\rangle_{\text{R}} \in \mathscr{H}_{\text{S}} \otimes \mathscr{H}_{\text{R}}, \tag{3.25}$$

by adding an auxiliary reference system R to the system S that signifies the original system. Note that $|\tilde{\psi}\rangle$ is also a possible purification of the state ρ_ψ, defined as

$$\rho_\psi := \mathcal{G}\left(|\psi\rangle\langle\psi|\right). \tag{3.26}$$

Thus, if the original state was U(1)-invariant, *i.e.* equal to its twirling, then the bipartite state to which it is mapped would be separable. But there is more to the mapping than merely mapping non-resources to separable states and resource states to entangle ones. More importantly, it preserves this structure when acted on by U(1)-covariant transformations.

Consider a U(1)-covariant transformation $\hat{K}_\ell^{(\alpha)}$ of Eq. (3.6) that maps

$$|\psi\rangle \mapsto |\phi_\ell^{(\alpha)}\rangle = \frac{\hat{K}_\ell^{(\alpha)}}{\sqrt{p_\ell^{(\alpha)}}}|\psi\rangle\,, \tag{3.27}$$

with probability $p_\ell^{(\alpha)} = \|\hat{K}_\ell^{(\alpha)}|\psi\rangle\|^2$, where $\hat{K}_\ell^{(\alpha)}$ effects the mapping

$$|\psi\rangle \mapsto \sum_n \sqrt{\lambda_n} k_{\ell,n}^{(\alpha)}|n+\ell\rangle. \tag{3.28}$$

If we follow the same procedure for the mapping of the state $|\phi_\ell^{(\alpha)}\rangle$, noting that $n_{\max}(|\phi_\ell^{(\alpha)}\rangle) = n_{\max}(|\psi\rangle) + \ell$, we arrive at

$$\begin{aligned}|\tilde{\phi}_\ell^{(\alpha)}\rangle :=& \frac{1}{\sqrt{p_\ell^{(\alpha)}}}\sum_n \sqrt{\lambda_n} k_{\ell,n}^{(\alpha)}|n+\ell\rangle_{\mathrm{S}} \\ &\otimes |n_{\max}(|\phi_\ell^{(\alpha)}\rangle) - (n+\ell)\rangle_{\mathrm{R}} \\ =& \frac{1}{\sqrt{p_\ell^{(\alpha)}}}\sum_n \sqrt{\lambda_n} k_{\ell,n}^{(\alpha)}|n+\ell\rangle_{\mathrm{S}} \otimes |n_{\max}(|\psi\rangle) - n\rangle_{\mathrm{R}}.\end{aligned} \tag{3.29}$$

Evidently, $|\tilde{\psi}\rangle$ can be transformed to $|\tilde{\phi}_\ell^{(\alpha)}\rangle$ via the local transformation $\hat{K}_\ell^{(\alpha)} \otimes I_{\mathrm{R}}$, where I_{R} is the identity operator on R.

The states $|\tilde{\psi}\rangle$ and $|\tilde{\phi}_\ell^{(\alpha)}\rangle$ are dependent in the sense that one state can be mapped to the other via operations acting *only* on the system S, *i.e.* via local operations. The fact that the two bipartite states, in Eqs. (3.25) and (3.29), the purifications of the twirled state, can be linked together by a local operation is due to the SSR restriction on the operations $\hat{K}_\ell^{(\alpha)}$. To see this, suppose the restriction was lifted to allow a number state $|n\rangle$ to transform to a superposition of two number states $|n_1\rangle + |n_2\rangle$ with $n_2 > n_1$. The purification process in (3.25) maps the outcome superposition to an entangled state

$$|\tilde{\phi}_\ell^{(\alpha)}\rangle \propto \sqrt{\eta_1}|n_1\rangle_{\mathrm{S}} \otimes |n_2 - n_1\rangle_{\mathrm{R}} + \sqrt{\eta_2}|n_2\rangle_{\mathrm{S}} \otimes |0\rangle_{\mathrm{R}}, \tag{3.30}$$

whereas the purified version of the initial state, $|\tilde{\psi}\rangle = |n\rangle_{\mathrm{S}} \otimes |0\rangle_{\mathrm{R}}$, is separable, and no local operation can make it entangled.

Our particular choice of auxiliary states in the purification process was motivated by ensuring that the bipartite states always remain within a superselected block of some fixed total number as in Eq. (3.25). Thus, we can see that the operators $\hat{K}_\ell^{(\alpha)}$ in (3.6) are precisely those Kraus operators that act on system S alone and, at the same time, either keep the joint state of the two systems S and R within the multiplicity space of total number $n_{\max}(|\psi\rangle)$ or transfer them both to the multiplicity space of another total number $n_{\max}(|\psi\rangle)+\ell$, for some $\ell \geq -n_{\max}(|\psi\rangle)$. System R acts as a sort of quantum phase reference, in the sense that it enables system S to break the SSR locally while preserving the overall SSR. The partial trace that results from lack of access to the reference system R is equivalent to the twirling map on the initial unipartite state.

Once realized, however, we can simplify the mapping without losing any of its relevant consequences. Consider the mapping that takes the state $|m\rangle$ to the state $|m\rangle \otimes |m\rangle$ instead of $|m\rangle \otimes |n-m\rangle$ as was the case before, consider the mapping,

$$|m\rangle \mapsto |m\rangle \otimes |m\rangle. \tag{3.31}$$

Again, non-resources, *i.e.* U(1)-invariant states, are mapped to separable states and resource states are mapped to entangled states. Furthermore, the corresponding operator acting on the bipartite states that maps the image of the states to each other is related to the original U(1)-invariant transformation as $\hat{K}_\ell^{(\alpha)} \to \hat{K}_\ell^{(\alpha)} \otimes T_\ell$, where $T_\ell := \sum_n |n+\ell\rangle\langle n|$ is the operator of translation by amount ℓ. Of course, in the new mapping (3.31), the total number is no longer preserved. However, it does not need to preserve the total number, because in the new picture that is presented in Chapter 4 we use the isometry as a *tool* to quantify the resource state itself, and not the joint state of the system and the reference frame together, that is bound by the global SSR. For example, the state could have been prepared before the SSR was set in place, when Alice and Bob still shared aligned reference frames with each other. So a resource state need not preserve the SSR.

In our treatment in later chapters, only the operations that are performed on states must be G-covariant and satisfy the SSR, not the states themselves.

The simple isometry in (3.31) is what allows us to map a problem of asymmetry to one of entanglement, and symmetric transformations to local operations. In Chapter 4, we show that an analogous map exists for all compact semi-simple Lie groups. Appendix B brings the map that we defined here within the formalism of the LOCC-simulating maps developed for general groups. In the rest of this chapter, we explore some of the applications of the mapping to bipartite states that we introduced in (3.25).

3.4 Applications

Since the image states transform under local operations, whatever entanglement they possess does not increase. Thus, any entanglement monotone of the bipartite states also quantifies the asymmetry of the original state and gives rise to a corresponding asymmetry monotone. All bipartite pure-state entanglement monotones can be expressed as concave functions of the Schmidt coefficients of the states, or equivalently, the eigenvalues of the reduced density matrix [95]. The reduced density matrix of the state $|\tilde{\psi}\rangle$ is the same as ρ_ψ defined in Eq. (3.26). Thus, from any entanglement monotone function defined for states acting on $\mathscr{H}_{\mathrm{S}} \otimes \mathscr{H}_{\mathrm{R}}$, we can build a monotone under U(1)-SSR for states acting on $\mathscr{H}$ by replacing the partial trace with the twirling map. We formalize this result in the following proposition:

Proposition 16. *Suppose a function $f : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+$ satisfies the following two conditions.*

E1. Unitary invariance: $f(\rho) = f(U\rho\, U^\dagger)$, $\forall U \in \mathcal{B}(\mathscr{H})$.

E2. Concavity: $f(t\rho_1 + [1-t]\rho_2) \geq t f(\rho_1) + [1-t] f(\rho_2)$, $\forall\, t \in [0,1]$.

Then

$$A_{pure} : \mathcal{P}(\mathscr{H}) \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \mapsto f(\mathcal{G}(|\psi\rangle\langle\psi|)),$$

is a pure-state ensemble monotone under U(1)-covariant operations, and its convex-roof extension $A : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+$ *is an ensemble monotone for all states.*

Proof. We first prove that A_{pure} is a pure-state ensemble monotone. Let $\mathcal{E} = \sum_x \mathcal{E}_x$ for $\mathcal{E}_x$ being U(1)-covariant completely positive operators that map pure states to pure states. Given a pure state $|\psi\rangle$, we follow the notation of Definition 24:

$$|\phi_x\rangle\langle\phi_x| := \frac{1}{p_x}\mathcal{E}_x\left[|\psi\rangle\langle\psi|\right],\ p_x := \text{Tr}\left(\mathcal{E}_x\left[|\psi\rangle\langle\psi|\right]\right). \tag{3.32}$$

Let the corresponding U(1)-covariant Kraus operators be indexed as

$$\hat{K}_{x,j}|\psi\rangle = \sqrt{p_{x,j}}|\phi_x\rangle, \tag{3.33}$$

where $\sum_j p_{x,j} = p_x$. The purifications of ρ_ψ and ρ_{ϕ_x} according to Eqs. (3.25) and (3.29) are then related to each other by

$$\hat{K}_{x,j} \otimes I_R|\tilde{\psi}\rangle = \sqrt{p_{x,j}}|\tilde{\phi}_x\rangle. \tag{3.34}$$

The reduced density operator of the auxiliary system R does not change under the transformation. For

$$\tau := \text{Tr}_\text{S}\left(|\tilde{\psi}\rangle\langle\tilde{\psi}|\right),\ \tau_x = \text{Tr}_\text{S}\left(|\tilde{\phi}_x\rangle\langle\tilde{\phi}_x|\right), \tag{3.35}$$

we obtain

$$\tau = \sum_{x,j} p_{x,j}\tau_x = \sum_x p_x\tau_x. \tag{3.36}$$

Condition E1 (unitary invariance) ensures that f is a function only of the state's eigenvalues, and concavity ensures that

$$f(\tau) = f\left(\sum_x p_x\tau_x\right) \geq \sum_x p_x f\left(\tau_x\right). \tag{3.37}$$

On the other hand

$$f\left(\mathrm{Tr}_{\mathrm{S}}\left[|\tilde{\psi}\rangle\langle\tilde{\psi}|\right]\right) = f\left(\mathrm{Tr}_{\mathrm{R}}\left[|\tilde{\psi}\rangle\langle\tilde{\psi}|\right]\right) = f\left(\mathcal{G}\left(|\psi\rangle\langle\psi|\right)\right) = A_{\mathrm{pure}}\left(|\psi\rangle\langle\psi|\right), \tag{3.38}$$

and similarly for $\{|\phi_x\rangle\}$. Finally, Eqs. (3.37) and (3.38) together imply

$$A_{\mathrm{pure}}\left(|\psi\rangle\langle\psi|\right) \geq \sum_x p_x A_{\mathrm{pure}}\left(|\phi_x\rangle\langle\phi_x|\right), \tag{3.39}$$

which is the desired result. Lemma 15 ensures that the convex-roof extension F defined by Eq. (3.12) is also an ensemble monotone for all states. □

We can now build the counterparts of Vidal's entanglement monotones for pure states [95]. Let

$$\boldsymbol{\lambda}^{\downarrow}(\rho_\psi) = \left(\lambda_1^{\downarrow}, \ldots, \lambda_d^{\downarrow}\right), \tag{3.40}$$

be the vector obtained by rearranging the coordinates of $\boldsymbol{\lambda}(\rho_\psi)$ in decreasing order.

Corollary 17. *The family of pure-state functions*

$$A_k : \mathcal{P}(\mathscr{H}) \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \mapsto \sum_{i=k}^{d} \lambda_i^{\downarrow},\ k = 2, \ldots, d, \tag{3.41}$$

together with their convex-roof extensions are a family of U(1)-asymmetry ensemble monotones.

This family of functions clearly satisfies both conditions of Prop. 16. Consequently, we see that the outcomes of any U(1)-covariant transformation majorize the initial state on average. This generalizes what was already established for the case of deterministic transformations [37].

As another example, consider the entropy of the twirled state that is both concave and unitarily invariant.

Corollary 18. *The entropy,*

$$S_F(|\psi\rangle\langle\psi|) := -\,Tr\left(\rho_\psi \log \rho_\psi\right), \tag{3.42}$$

is an ensemble monotone under a U(1)-SSR as defined in Section 2.4 (see Definition 22). Here the density operator ρ_ψ is the state obtained by twirling the state $|\psi\rangle$ as defined in Eq. (3.26).

The entropy is equal to the relative entropy of frameness (G-asymmetry) for pure states [35].

Conditions E1 and E2 in Prop. 16 are only sufficient conditions for U(1)-monotones and not necessary ones, not even for monotones defined over pure states. If $|\tilde{\psi}\rangle$ can be transformed to $|\tilde{\phi}_\ell^{(\alpha)}\rangle$ under general local operations, it does not follow that $|\psi\rangle$ is necessarily transformable into $|\phi\rangle$ under a U(1)-SSR. This reasoning follows simply because the local transformation that takes $|\tilde{\psi}\rangle$ to $|\tilde{\phi}_\ell^{(\alpha)}\rangle$ need not have Kraus operators of the form $\hat{K}_\ell^{(\alpha)} \otimes I_R$ for $\hat{K}_\ell^{(\alpha)}$ specified in Eq. (3.6). Thus, the asymmetry monotones, unlike entanglement monotones, do not have to remain non-increasing on average for *all* local operations and therefore need not be of the form derived in Prop. 16. The mappings between the bipartite images constitute only a strict subset of all LOCC operations, *ie.* local operations that either preserve the total number or shift it by a fix amount (as discussed in Section 3.3).

As a counterexample, consider the normalized number variance

$$V_{\text{pure}}(|\psi\rangle\langle\psi|) = 4\left(\langle\psi|\hat{n}^2|\psi\rangle - \langle\psi|\,\hat{n}\,|\psi\rangle^2\right). \tag{3.43}$$

The variance is neither concave nor convex, and yet it was shown to be an ensemble monotone over pure states [37, 79, 80]. In fact, the total-number variance of bipartite states, unlike the von Neumann entropy, is not an entanglement monotone.

Note that if the state $|\psi\rangle$ is prepared without access to a resource after the SSR is imposed, then it would be an invariant state and its variance is identically zero. However, if the state is prepared in the absence of the SSR, for example during a time when Alice and Bob did share a reference frame, then its variance will not be zero. Similarly, Alice could prepare the state relative to a bounded-sized token of her RF, so that the numbers n are relative numbers and thus local quantities, while the SSR is global and acting on the joint states. In fact, asymmetry resources are precisely those states that violate the SSR and, consequently, cannot be prepared under the SSR restriction.

For similar reasons, majorization is a necessary but not a sufficient condition for pure-state to pure-state deterministic transformations. Thus, the U(1)-asymmetry monotones of Eq. (3.41), unlike Vidal's monotones in entanglement theory, do not fully characterize deterministic U(1)-covariant transformations [95].

Motivated by Wootters's formula for the concurrence of bipartite two-qubit states [110], later extended to bipartite qudit states [31,32,75], we can also construct a family of concurrence measures for qudits with $d \geq 2$. Let

$$S_k(\boldsymbol{\lambda}(\rho_\psi)) = \sum_{m_1 < m_2 < \cdots < m_k} \lambda_{m_1}\lambda_{m_2}\ldots\lambda_{m_k}, \tag{3.44}$$

for $k = 2, \ldots, d$, denote the k^{th} elementary symmetric function of the eigenvalues $\boldsymbol{\lambda}(\rho_\psi) = (\lambda_1, \ldots, \lambda_d)$ of ρ_ψ. We assume that $\lambda_n = 0$ for $n_{\max}(|\psi\rangle) < n \leq d$. The summation is over all terms $\lambda_{m_1}\lambda_{m_2}\ldots\lambda_{m_k}$ whose subscripts satisfy the inequality $m_1 < \cdots < m_k$, so that each given set of the labels $m_1, \cdots, m_k$ contributes only once to the final sum.

Definition 26. *The family of concurrence-of-frameness functions are defined for pure states as*

$$C_k : \mathcal{P}(\mathscr{H}) \to \mathbb{R}^+ : |\psi\rangle\langle\psi| \to f_k(\rho_\psi) := \left[\frac{S_k\left(\boldsymbol{\lambda}(\rho_\psi)\right)}{S_k\left(\frac{1}{d}, \ldots, \frac{1}{d}\right)}\right]^{\frac{1}{k}}, \tag{3.45}$$

and extended to mixed states via their convex-roof extensions.

The f_k are concave functions of $\boldsymbol{\lambda}(\rho)$ [33]. Hence Prop. 16 guarantees that $\{C_k\}$ are ensemble monotones as summarized in the following corollary.

Corollary 19. *The concurrence $C_k(\rho)$ for $k = 2, \ldots, d$ of a state ρ does not increase on average under $U(1)$-invariant operations.*

Note that non-resource states are number eigenstates hence not of full rank. Thus, their concurrence is identically zero as is expected from Condition A1 in Def. 24.

Now, we demonstrate the similarity between the entanglement and asymmetry resource measures by calculating the concurrence of mixed qubit states. For a pure single-qubit state ($d = 2$), $C_2(|\psi\rangle) = |\langle\psi|X|\psi^*\rangle|$, where $*$ denotes complex conjugation in the basis $\{|0\rangle, |1\rangle\}$, and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ denotes the flip operator in this basis. Let

$$R := \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}},\ \tilde{\rho} := X\rho^* X, \tag{3.46}$$

and let the set of eigenvalues of R be $\mu(R) = \{\mu_1, \mu_2\}$. In Section 3.4.2, we derive the explicit dependence of μ_1 and μ_2 on the parameters of the spectral decomposition of ρ.

Proposition 20. *The concurrence of frameness for a qubit state ρ is*

$$C_2\left(\rho\right) = |\mu_1 - \mu_2|. \tag{3.47}$$

Proof. The proof is similar to Wootters's proof for concurrence of entanglement [110]. Without loss of generality we assume that $\mu_1 \geq \mu_2$. Let

$$\rho = |\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2| \tag{3.48}$$

be the spectral decomposition of ρ, where each state $|\phi_i\rangle$ is unnormalized. Also define the matrix $\tau_{ij} := \langle\phi_i|\tilde{\phi}_j\rangle$, where $|\tilde{\phi}_j\rangle = \hat{X}|\phi_j\rangle^*$, which yields the symmetric relation $\tau_{ij} = \tau_{ji}$ [110]. As a symmetric matrix, τ can be diagonalized by a unitary U such that $\tau' = U\tau U^{\top}$, where

$$\tau'_{11} = \mu_1,\ \tau'_{22} = -\mu_2\ , \tau'_{12} = \tau'_{21} = 0, \tag{3.49}$$

and where $\{\mu_1, \mu_2\}$ are the eigenvalues of R (in fact, the eigenvalues of R are the square roots of the eigenvalues of $\tau\tau^*$ [110].). The unitary U relates the spectral decomposition of ρ to a different decomposition $\rho = |\xi_1\rangle\langle\xi_1| + |\xi_2\rangle\langle\xi_2|$. The average concurrence of the ensemble $\{|\xi_1\rangle, |\xi_2\rangle\}$ that realizes ρ is

$$\langle C\rangle = \sum_{i=1}^{2} |\tau'_{ii}| = \mu_1 + \mu_2, \tag{3.50}$$

and we define the average preconcurrence of this ensemble as

$$\langle\tilde{C}\rangle := \sum_{i=1}^{2} \tau'_{ii} = \mu_1 - \mu_2. \tag{3.51}$$

If the concurrences of the states $|\xi_i\rangle$ are not equal, we can always interchange them by an orthogonal transformation. Due to continuity, there must also be an intermediary orthogonal transformation V that takes $|\xi_i\rangle$ to states $|\zeta_i\rangle$,

$$|\zeta_i\rangle = \sum_j V_{i,j}|\xi_j\rangle, \tag{3.52}$$

with the following property: $C_2\left(|\zeta_1\rangle\langle\zeta_1|\right) = C_2\left(|\zeta_2\rangle\langle\zeta_2|\right) = \langle\tilde{C}\rangle$. Hence, the average concurrence of the new decomposition also equals the preconcurrence,

$$\langle C\rangle = \langle\tilde{C}\rangle = \mu_1 - \mu_2. \tag{3.53}$$

For any other decomposition of ρ attained by the unitary operator V', let $v_{ij} := V'^2_{ij}$ so that $\sum_i |v_{ij}| = 1$. The average concurrence is equal to

$$\begin{aligned}\langle C\rangle = \sum_i \left|\sum_j v_{ij}\tau'_{jj}\right| &\geq \left|\mu_1 - \sum_i v_{i2}\mu_2\right| \\ &\geq \mu_1 - \left|\sum_i v_{i2}\mu_2\right| \geq \ \mu_1 - \mu_2,\end{aligned} \tag{3.54}$$

where we assume v_{i1} are real, by a suitable change of the overall phase if necessary, so that $\sum_i v_{i1} = 1$. Thus, the average concurrence of the ensemble $\{|\zeta_1\rangle, |\zeta_2\rangle\}$ is the minimum average concurrence. □

As for entanglement, we can use the closed form of the average concurrence to calculate the convex-roof extension of a set of other asymmetry monotones. The following corollary specifies what type of monotones belong to this set.

Corollary 21. *If, for every pure state* $|\psi\rangle\langle\psi| \in \mathcal{P}(\mathscr{H})$*, a pure-state asymmetry measure* $A_{pure}(|\psi\rangle\langle\psi|)$ *is equal to* $\mathcal{F}\left(C_2(|\psi\rangle\langle\psi|)\right)$*, where* $\mathcal{F}: \mathbb{R}^+ \to \mathbb{R}^+$ *is a non-decreasing convex function, then the convex roof extension of* A_{pure} *is also equal to the value of* $\mathcal{F}(C_2(\rho))$ *for all mixed states* ρ*. In other words,*

$$A(\rho) = \mathcal{F}(C_2(\rho)), \;\; \forall \rho \in \mathcal{B}(\mathscr{H}), \tag{3.55}$$

with A *the convex-roof extension of* A_{pure}*.*

Proof. Recall that there exists a decomposition with the minimum average concurrence where $C_2(\rho) = C_2(|\zeta_1\rangle\langle\zeta_1|) = C_2(|\zeta_2\rangle\langle\zeta_2|)$ as defined in Eq. (3.52). Thus, for any other decomposition of $\rho = \sum_j q_j' |\psi_j\rangle\langle\psi_j|$, we must have $C_2(|\zeta_1\rangle\langle\zeta_1|) \leq \sum_j q_j' C_2(|\psi_j\rangle\langle\psi_j|)$. As $\mathcal{F}(C_2)$ is non-decreasing and convex, we have

$$\begin{aligned} \mathcal{F}\left(C_2(\rho)\right) = \mathcal{F}\left(C_2(|\zeta_1\rangle\langle\zeta_1|)\right) & \\ \leq \mathcal{F}\left(\sum_j q_j' \, C_2(|\psi_j\rangle\langle\psi_j|)\right) & \leq \sum_j q_j' \, \mathcal{F}\left(C_2\left(|\psi_j\rangle\langle\psi_j|\right)\right) \\ & = \sum_j q_j' \, A_{\text{pure}}(|\psi_j\rangle\langle\psi_j|). \end{aligned} \tag{3.56}$$

Thus, $\mathcal{F}\left(C_2(\rho)\right)$ is the minimum average pure-asymmetry A_{pure} taken over all the pure-state decompositions of ρ. □

In the next section, we use this corollary to calculate the convex-roof extension of the variance (3.43), which is the asymptotic measure of U(1)-asymmetry, as is shown in [37]. Finally, we note that this corollary can also be used for the convex-roof extension of the asymptotic $\mathbb{Z}_2$-asymmetry measure [37].

3.4.1 Frameness of formation

Proposition 16 enables us to systematically construct asymmetry monotones under U(1)-SSR, but as we noted earlier, not all U(1)-asymmetry monotones can be obtained this way. Yet, there is still a chance that the convex-roof extension of monotones that cannot be obtained by the method of Proposition 16 may be expressed directly as a function of monotones that can. In particular, Corollary 21 specifies which monotones can be related in this way to the concurrence of frameness in the case of single-qubit states.

The number variance (3.43) is an important asymmetry monotone that does not meet the conditions of Proposition 16, *i.e.* it is not a concave function of the twirled state. Besides being an ensemble monotone, variance is the unique measure of asymmetry of pure states in the sense that it quantifies the rate at which they can be asymptotically formed from or distilled into the state $|+\rangle := (1/\sqrt{2})\left(|0\rangle + |1\rangle\right)$ [37]. The $|+\rangle$ state is chosen as a standard unit resource state and is an instance of a unipartite, or local, refbit [37, 89]. Thus, the convex-roof extension of the variance is the equivalent of the entanglement of formation [14] and is therefore called the frameness of formation (FoF) of the group U(1) [37].

Definition 27. *The frameness of formation for the group G=U(1) of a state ρ in terms of refbits $|+\rangle$ is*

$$V(\rho) = \min_{\{|\psi_i\rangle, q_i\}} \sum_i q_i \, V_{pure}(|\psi_i\rangle\langle\psi_i|), \tag{3.57}$$

where $V_{pure}(|\psi_i\rangle\langle\psi_i|) = 4\left(\langle\psi_i|\hat{n}^2|\psi_i\rangle - \langle\psi_i|\,\hat{n}\,|\psi_i\rangle^2\right)$.

As we presently show, the variance of a qubit is a convex function of the concurrence, and we can determine the FoF of a qubit analytically by relating the variance to the qubit's concurrence of frameness using Corollary 21. The outcome is analogous to Wootters's formula for the entanglement of formation of bipartite two-qubit states [110].

Proposition 22. *The FoF of a single qubit is*

$$V(\rho) = |\mu_1 - \mu_2|^2 \tag{3.58}$$

for $\mu_R = \{\mu_1, \mu_2\}$ *the set of eigenvalues for state* $R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$.

Proof. Recall that $|\psi\rangle = \sqrt{\lambda_0}|0\rangle + \sqrt{\lambda_1}|1\rangle$. We have $C_2(|\psi\rangle\langle\psi|) = 2\sqrt{\lambda_0\lambda_1}$ and $V_{\text{pure}}(|\psi\rangle\langle\psi|) = 4\lambda_0\lambda_1$. The frameness (3.43) is a convex, non-decreasing function of the concurrence, $\mathcal{V}(C_2) = C_2^2$. The result follows from Corollary 21. □

Schuch et. al. already identified the equivalent of the number variance in a bipartite setting as a separate measure of non-locality under the joint restrictions of LOCC and total-number SSR, where they call the bipartite measure the "superselection-induced variance" and also show, among other things, that its convex-roof extension can be obtained from the bipartite entanglement concurrence [79, 80].

The SSR-induced variance and U(1)-frameness of formation are related, and the arguments in Section 3.3 that relate asymmetry resources to entanglement through purification of the twirled state makes the link between the two measures even more explicit. However, although we employ bipartite states for purification, our aim is not to study nonlocal asymmetry. Rather, the resources we consider are unipartite and are not restricted by this SSR. Only the operations have to obey the SSR. The monotones and measures of asymmetry we consider, including the concurrence of frameness and the variance, are viewed as local RF resources and are treated on their own, independent of entanglement theory.

Strictly speaking, the variance quantifies the rate of formation for states $|\psi\rangle = \sum_n \lambda_n|n\rangle$ whose number spectrum, spec($|\psi\rangle$) (3.4), is gapless, *i.e.* states for which $\lambda_{n_1} > 0$ and $\lambda_{n_2} > 0$ implies that $\lambda_n > 0$ for all n between n_1 and n_2. For example, we call the state whose spectrum is equal to the set $\{3, 4, 5, 6\}$ as a gapless state, while the state with spectrum $\{3, 4, 6\}$ has a gap, since the number 5 is missing while both 4 and 6 belong to the set. The reason is that states with gaps cannot be transformed to gapless states with any non-zero probability under the U(1)-SSR. However, the problem can be solved by employing negligible amount of catalyst resources that makes it possible to asymptotically transform gapless and gapped states to each other in a reversible manner [37,79,80]. Here, we have assumed all pure states are mutually interconvertible, by which we mean that any of the pure states can be transformed to any other with some probability (not necessarily probability one) under some, deterministic or non-deterministic, $U(1)$-invariant transformation. Under this assumption, we can consistently interpret the convex-roof extension of the variance as the minimum average cost, in terms of refbits, of preparing the ensemble of states that realize the mixed state.

3.4.2 Explicit concurrence of frameness and U(1)-asymmetry of formation of a qubit

Let $\rho = p|\phi_1\rangle\langle\phi_1| + (1-p)|\phi_2\rangle\langle\phi_2|$ be the spectral decomposition of the state ρ. The two states $|\phi_1\rangle$ and $|\phi_2\rangle$ have the same relative phase and can be simultaneously transformed by U(1)-covariant transformations to states with real amplitudes on the Bloch sphere:

$$\begin{aligned} |\phi_1\rangle &= \cos\frac{\alpha}{2}|0\rangle + \sin\frac{\alpha}{2}|1\rangle, \\ |\phi_2\rangle &= -\sin\frac{\alpha}{2}|0\rangle + \cos\frac{\alpha}{2}|1\rangle. \end{aligned} \tag{3.59}$$

The two singular values of the state $R(\rho)$ in Eq. (3.46) are

$$\mu_{1,2} = \sqrt{p(1-p) + \frac{1}{2}(1-2p)^2 \sin^2\alpha \pm K} \tag{3.60}$$

for

$$K := \frac{1}{2}\left|(1-2p)\sin\alpha\right|\sqrt{(1-2p)^2\sin^2\alpha + 4p(1-p)}. \tag{3.61}$$

The state's concurrence is equal to

$$C_2(\rho) = \left|(1-2p)\sin\alpha\right|, \tag{3.62}$$

and

$$V_2(\rho) = (1-2p)^2\sin^2\alpha \tag{3.63}$$

is the qubit U(1)-frameness of formation.

The measure is zero for $\alpha = 0$ and $\alpha = \pi$ corresponding to the number eigenstates $|0\rangle$ and $|1\rangle$. The measure V_2 is also zero for the case of $p = 1/2$, irrespective of the value of α, as it corresponds to the totally-mixed state that can be decomposed into $|0\rangle$ and $|1\rangle$ eigenstates with equal probability,

$$\rho_I := \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|. \tag{3.64}$$

For all other value of the parameters, the variance of formation ensures that the state is a $U(1)$-resource.

Here we have, for the first time, found a closed formula for the asymmetry of a (in general) mixed state. The definition of the convex roof extension involves a minimization over all states which is a computationally difficult task for a general state. We have provided a closed formula that calculates the minimum value for a single-qubit state. Moreover, it is the analogue of the formula of Wootters in entanglement theory, that was, in its own turn, one of the first discovered closed formulas for computing an entanglement measure of two-qubit mixed states.

Chapter 4

Simulating symmetric transformations with local operations

In this chapter, we show that covariant CP-maps can be ‘simulated’ by a restricted subset of local operations and classical communications (LOCC). The key idea is to embed the system’s Hilbert space $\mathscr{H}$ within a larger tensor product space $\mathscr{H}_A \otimes \mathscr{H}_B$. The embedding is done with an isometry

$$\mathscr{H} \xrightarrow{\text{iso}} \mathscr{W} \subseteq \mathscr{H}_A \otimes \mathscr{H}_B, \tag{4.1}$$

that has the following properties. First, the isometry maps symmetric states to separable states. Furthermore, consider two density operators ρ and σ acting on $\mathscr{H}$, and their corresponding bipartite images $\tilde{\rho}_{AB}$ and $\tilde{\sigma}_{AB}$ that act on the image subspace $\mathscr{W}$. If there exists a covariant transformation $\mathcal{E}_{\text{cov}}$ that maps ρ to σ, *i.e.* $\sigma = \mathcal{E}_{\text{cov}}(\rho)$, then there must also exist a *local* transformation $\tilde{\mathcal{E}}_{\text{local}}$ that maps $\tilde{\rho}_{AB}$ to $\tilde{\sigma}_{AB}$, *i.e.* $\tilde{\sigma}_{AB} = \tilde{\mathcal{E}}_{\text{local}}(\tilde{\rho}_{AB})$ (Figure 4.1). In this sense, the local operator $\tilde{\mathcal{E}}_{\text{local}}$ simulates the covariant map $\mathcal{E}_{\text{cov}}$.

We show here that such isometries can be found for all covariant CP-maps that are associated with finite-dimensional representations of compact semi-simple Lie groups. Moreover, for any asymmetric state, we show that there exists an isometry that maps it

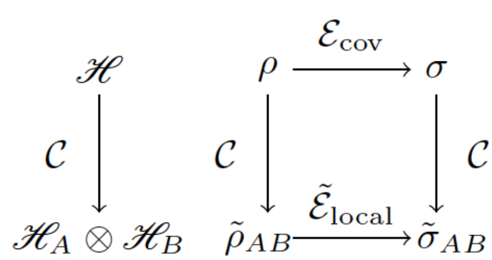

Figure 4.1: Simulating a covariant transformation $\mathcal{E}_{\text{cov}}$ by a LOCC transformation $\tilde{\mathcal{E}}_{\text{local}}$.

to an entangled state.

Hence, the entanglement in the image space captures important aspects of the asymmetry properties of the original state. Our results follow from an application of the Wigner-Eckart theorem, generalized to all semi-simple compact groups [16], that determines the general form of the Kraus operators of covariant transformations [37].

The study of the evolution of entanglement governed by the LOCC map $\mathcal{E}_{\text{local}}$ opens a new window to explore symmetric dynamics. In particular, it shows that important features of the resource theory associated with the asymmetry of quantum states [37,60] is captured by a particular sub-class of the resource theory of entanglement under a restricted subset of LOCC transformations.

A comprehensive collection of theorems and theoretical tools has been developed to study quantum entanglement for more than a decade [48, 71, 92]. The equivalence between asymmetry and entanglement resources allows us to take advantage of the repertoire of tools of entanglement theory in order to study the asymmetry properties of quantum states. In particular, the established equivalence allows us to use any entanglement monotone and construct a corresponding 'asymmetry monotone' [1]. An asymmetry monotone, as the name suggests, is a real function defined on the set of quantum states such that its magnitude changes monotonically (*i.e.* non-increasingly) during a symmetric evolution. In the case of reversible symmetric transformations, asymmetry monotones of course remain conserved. They can thus be regarded as generalizations of conserved quantities. Taking asymmetry monotones into account allows us to rule out classes of transformations that cannot be ruled out based on conservation laws alone. Asymmetry monotones can also quantify the strength of quantum resources, just as entanglement

[1] In [60, 61] it was called an 'asymmetry measure' and in [37] it was called a 'frameness monotone'. Here we use the terminology of asymmetry monotones rather than asymmetry measures since these functions do not necessarily *measure* asymmetry, but can sometimes only *detect* it. To see it, consider for example the asymmetry monotone that is equal to 7.2 for asymmetric states, and zero for symmetric states. Clearly, this monotone does *not* measure asymmetry, only detects asymmetry.

monotones measure the entanglement strength of states [95].

A state that lacks a particular symmetry encodes information about the physical quantity that is associated with that symmetry. For example, a direction in space changes to another direction via rotation. An angular-momentum eigenstate picks out a specific direction in space and thus breaks the rotational symmetry. Therefore, the state of an electron with non-zero angular momentum along a particular direction in space is not symmetric under rotations and consequently encodes some information about that direction. In contrast, a symmetric state does not carry any such information. So, electrons in a rotationally invariant state of zero total-angular momentum contain no information about any preferred direction.

So far, the study of asymmetry properties of quantum systems has mostly been focused on pure states. For example, interconversion of pure states under specific symmetry groups has been studied [8, 37, 86] and a general classification of pure-state asymmetry properties for arbitrary finite or compact Lie groups has been developed [61]. Prior to the present result, little was known about the general properties of mixed-state asymmetry, and, with few but important exceptions like the G-asymmetry [88] (also known as the relative entropy of frameness [35]), asymmetry monotone functions of mixed-states were not identified for symmetries associated with general groups.

Our work introduces a wide class of asymmetry monotones, defined for all states, pure or mixed. Some of the asymmetry monotones we construct can only be defined in terms of the entanglement of a bipartite system. A case in point is the negativity measure of entanglement [97]. Negativity is specially interesting as it provides us with an easily calculable asymmetry monotone for all states and for all types of symmetry.

Although monotones are extremely useful tools in resource theories [71,95], the conditions for the symmetric evolution of states need not always come in the form of asymmetry monotones. We derive a separate necessary condition for the existence of a covariant transformation from one state to another. However, the condition is such that it cannot be expressed in terms of asymmetry monotones, though for reversible symmetric transformations our necessary condition leads to new conserved quantities. We arrive at this condition by a new isometry-embedding of the system's Hilbert space into a different tensor-product structure. This additional result shows that the isometry in Eq. (4.1) can be useful even if it does not simulate covariant transformations with LOCC.

The chapter is organized as follows: We present our main result in Section 4.1. In Section 4.2 we demonstrate how entanglement monotones can be applied to the resource theory of asymmetry. Sections 5.2.1 and 5.3 focus on specific examples of asymmetry monotones and how they compare with their entanglement counterparts. In Section 6, we introduce a new isometry that in general does not simulate covariant maps with LOCC, but nonetheless leads to new results on time-symmetric evolutions. In Appendix A, we generalize the main result to general finite or compact Lie groups. Appendix B contains a special form of the general results for the case of Abelian groups.

4.1 Simulating G-covariant transformations

The central idea of this thesis is to embed the system's Hilbert space within a larger Hilbert space in such a way that the covariant transformations between original states map to LOCC transformations in the larger Hilbert space. We now proceed to make precise the concepts and procedures involved. We use the notations introduced in Chapter 2. As before, we assume that G is a compact semi-simple Lie group and the Hilbert space $\mathscr{H}$ carries a fully-reducible unitary representation of G.

Definition 28. *A LOCC-simulating isometry is an isometry $\mathcal{C} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{W})$, with a bipartite image space $\mathscr{W} \subseteq \mathscr{H}_A \otimes \mathscr{H}_B$ (see Eq. 4.1), that satisfies the following three conditions:*

(1) *For any G-covariant map, $\mathcal{E}_{cov}$, the map*

$$\mathcal{C} \circ \mathcal{E}_{cov} \circ \mathcal{C}^{-1} = \mathcal{E}_{local} : \ \mathcal{B}(\mathscr{W}) \to \mathcal{B}(\mathscr{W})$$

is local; that is, $\mathcal{E}_{local}$ can be implemented by LOCC.

(2) *If ρ is G-invariant then $\mathcal{C}(\rho)$ is separable.*

(3) *There exists an asymmetric state (i.e. non-G-invariant state) σ for which $\mathcal{C}(\sigma)$ is entangled.*

The third point excludes trivial isometries that map every state, whether G-invariant or not, to a separable state. One example of such a trivial isometry is simply adding an ancilla state to every state ρ, *i.e.*,

$$\rho \mapsto \mathcal{C}(\rho) := \rho \otimes |0\rangle\langle 0|. \tag{4.2}$$

Trivial isometries of this sort are of course always possible, but they differentiate neither between G-invariant and non-invariant states, nor between G-covariant or non-covariant transformations. Thus, they tell us nothing about the states' asymmetry properties or about the conditions under which covariant transformations are possible. The other extreme, that of mapping every asymmetric state to an entangled state, although ideal, is not likely to always be possible. The isometries that we consider here do not fall under either extreme. Nevertheless, we are able to find a *set* of isometries that is complete in the sense that for any asymmetric state there exists at least one isometry in the set that takes it to an entangled state. In this sense, entanglement capture all aspects of asymmetry.

4.1.1 The main isometry

The Wigner-Eckart theorem determines the matrix elements of an irreducible tensor operator, like the Kraus operators of G-covariant transformations, in the basis $|\boldsymbol{j}, \lambda; m\rangle$

introduced in Chapter 2. An important consequence of the Wigner-Eckart theorem is the existence of the so-called selection rules. The generalized CG coupling coefficients $\left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}' \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array}\right)$ are zero unless the weights $\boldsymbol{m}$, $\boldsymbol{M}$ and $\boldsymbol{m}'$ satisfy the relation,

$$\boldsymbol{m} + \boldsymbol{M} = \boldsymbol{m}'. \tag{4.3}$$

The matrix elements that do not satisfy Eq. (4.3) must vanish. It thus follows from the Wigner-Eckart theorem that the only thing a G-covariant Kraus operator $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ does on the weight $\boldsymbol{m}$ of a basis state is to translate it by $\boldsymbol{M}$, independently of the other relevant parameters, $\boldsymbol{j}$, $\boldsymbol{J}$, λ and α. We exploit this fact in the following definition and theorem when we introduce an isometry that satisfies the three conditions of definition 28.

Definition 29. *Let $\mathscr{H}_B$ denote the Hilbert space spanned by the states labeled as $|\boldsymbol{m}\rangle$ where $\boldsymbol{m}$ ranges over the representation weights of the Lie algebra of the group, and let*

$$\mathscr{W} := span\{|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \otimes |\boldsymbol{m}\rangle\} \subset \mathscr{H} \otimes \mathscr{H}_B. \tag{4.4}$$

The isometry $\mathcal{C}$ is defined by its action on the basis kets as:

$$|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \mapsto^{\mathcal{C}} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \otimes |\boldsymbol{m}\rangle. \tag{4.5}$$

We now show that $\mathcal{C}$ satisfies all the conditions of definition 28.

Theorem 23. *$\mathcal{C}$ is a LOCC-simulating isometry.*

Proof. First, note that as the states $|m\rangle$ are orthonormal, if $|\psi\rangle \mapsto^{\mathcal{C}} |\tilde{\psi}\rangle$ and $|\phi\rangle \mapsto^{\mathcal{C}} |\tilde{\phi}\rangle$, then we have $\langle\tilde{\psi}|\tilde{\phi}\rangle = \langle\psi|\phi\rangle$. Similarly $\mathrm{Tr}(\mathcal{C}(\rho)\mathcal{C}(\sigma)) = \mathrm{Tr}(\rho\sigma)$, as can be similarly verified by considering the spectral decompositions of density operators. Thus, the map $\mathcal{C}$ is indeed an isometry. To see that the first condition in definition (28) is satisfied, consider a G-covariant CP-map $\mathcal{E}_{\mathrm{cov}}$ whose operator sum representation is given in terms of Kraus operators $\{K_{\boldsymbol{J},\boldsymbol{M},\alpha}\}$. We define

$$\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha} := K_{\boldsymbol{J},\boldsymbol{M},\alpha} \otimes T_{\boldsymbol{M}}, \tag{4.6}$$

where,

$$T_{\boldsymbol{M}} := \sum_{\boldsymbol{m}} |\boldsymbol{m} + \boldsymbol{M}\rangle\langle\boldsymbol{m}| \tag{4.7}$$

is a translation operator. Let $\mathcal{E}_{\text{local}}$ denote the CP-map whose operator sum representation corresponds to the Kraus operators $\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha}$ given in Eq.(4.6). Note that from Eq. (4.3) it follows that $\mathcal{E}_{\text{local}} = \mathcal{C} \circ \mathcal{E}_{\text{cov}} \circ \mathcal{C}^{-1}$. We need to show that $\mathcal{E}_{\text{local}}$ can be implemented by LOCC. Indeed, the operator $T_{\boldsymbol{M}}$, being merely a translation operator, is unitary (assuming the range of the weights in the decomposition (2.37) is unbounded). Therefore, the map $\mathcal{E}_{\text{local}}$ can be implemented as follows: Alice perform a 'local' measurement described by the Kraus operators $\{K_{\boldsymbol{J},\boldsymbol{M},\alpha}\}$ and send the part $\boldsymbol{M}$ of her measurement outcome to Bob, who then performs the unitary transformation $T_{\boldsymbol{M}}$. Hence, the first criterion of Definition 28 is satisfied.

Secondly, recall that any G-invariant state ρ is equal to its own G-twirling (see Eq. 3.8),

$$\rho = \sum_{\boldsymbol{j},\lambda} p_{\boldsymbol{j},\lambda} \Pi_{\boldsymbol{j},\lambda}, \tag{4.8}$$

where the projection $\Pi_{\boldsymbol{j},\lambda}$ is equal to

$$\Pi_{\boldsymbol{j},\lambda} = \sum_{\boldsymbol{m}} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\langle\boldsymbol{j}, \lambda; \boldsymbol{m}|. \tag{4.9}$$

The state $\mathcal{C}(\rho)$ is thus equal to

$$\mathcal{C}(\rho) = \sum_{\boldsymbol{j},\lambda} p_{\boldsymbol{j},\lambda} \sum_{\boldsymbol{m}} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\langle\boldsymbol{j}, \lambda; \boldsymbol{m}| \otimes |\boldsymbol{m}\rangle\langle\boldsymbol{m}|, \tag{4.10}$$

which is clearly a separable state.

Finally, a state of the form

$$|\psi\rangle = c_1\,|\boldsymbol{j}_1, \lambda_1; \boldsymbol{m}_1\rangle + c_2\,|\boldsymbol{j}_2, \lambda_2; \boldsymbol{m}_2\rangle, \tag{4.11}$$

is mapped to the entangled state,

$$|\tilde{\psi}\rangle = c_1\,|\boldsymbol{j}_1, \lambda_1; \boldsymbol{m}_1\rangle \otimes |\boldsymbol{m}_1\rangle + c_2\,|\boldsymbol{j}_2, \lambda_2; \boldsymbol{m}_2\rangle \otimes |\boldsymbol{m}_2\rangle. \tag{4.12}$$

This completes the proof. □

The example in Eq. (4.11) suggests that if a state has coherence in $\boldsymbol{m}$ it is mapped to an entangled state. In the next proposition, we make this claim rigorous and give necessary and sufficient conditions for a general mixed state ρ to be mapped to an entangled state by the isometry $\mathcal{C}$.

Proposition 24. *Let $\Pi_{\boldsymbol{m}}$ be the projection*

$$\Pi_m := \sum_{\boldsymbol{j},\lambda} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\langle \boldsymbol{j}, \lambda; \boldsymbol{m}|\ .$$

Then, the isometry $\mathcal{C}$ maps a state ρ to an entangled state if and only if there exists $\boldsymbol{m}$ such that $[\rho, \Pi_{\boldsymbol{m}}] \neq 0$; i.e. ρ has coherence in $\boldsymbol{m}$.

Proof. Every state $\tilde{\rho}$ acting on $\mathscr{W}$ is the image of some state acting on $\mathscr{H}$, *i.e.* $\tilde{\rho} = \mathcal{C}(\rho)$. If $\tilde{\rho}$ is a separable state, it must have a pure-state decomposition comprised of product states

$$\tilde{\rho} = \sum_i q_i |\tilde{\phi}_i\rangle\langle\tilde{\phi}_i|,$$

where each $|\tilde{\phi}_i\rangle$ is both a product state and the image of some state $|\phi_i\rangle$ under the isometry $\mathcal{C}$. This is because $\mathcal{C}$ is a linear invertible map, and any pure-state decomposition of ρ corresponds to a pure-state decomposition of $\tilde{\rho}$ and vice versa. Thus, since $|\tilde{\phi}_i\rangle = \mathcal{C}(|\phi_i\rangle)$ is a product state, $|\phi_i\rangle$ must have the form

$$|\phi_i\rangle = \sum_{\boldsymbol{j},\lambda} c_{i;\boldsymbol{j},\lambda} |\boldsymbol{j}, \lambda; \boldsymbol{m}_i\rangle. \tag{4.13}$$

where $c_{i;\boldsymbol{j},\lambda}$ are some complex coefficients and the superposition above consists of a *single* value for $\boldsymbol{m} = \boldsymbol{m}_i$. Otherwise, containing two different values for $\boldsymbol{m}$ in the above expansion necessarily renders the state $|\tilde{\phi}_i\rangle$ entangled. Consequently, the form of the initial state ρ corresponding to $\tilde{\rho} = \mathcal{C}(\rho)$ must be,

$$\rho = \sum_i q_i |\phi_i\rangle\langle\phi_i| \ ,$$

with $|\phi_i\rangle$ as in Eq (4.13). According to Eq.(4.13) each $|\phi_i\rangle\langle\phi_i|$ commutes with $\Pi_{\boldsymbol{m}}$ for all $\boldsymbol{m}$ and therefore $[\rho, \Pi_{\boldsymbol{m}}] = 0$. The argument works in the other direction as well. In other words, if every pure-state decomposition of ρ contains at least one pure state that is in a coherent superposition of two or more eigenstates with different values of $\boldsymbol{m}$, then $\mathcal{C}(\rho)$ will be an entangled state. This completes the proof. □

The isometry $\mathcal{C}$ does not map *all* asymmetric states to entangled states. For example, the state $|\phi\rangle = |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle$ is not G-invariant (assuming $\boldsymbol{j}$ does not label the identity irrep), and yet it is mapped to the product state

$$|\tilde{\phi}\rangle = |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \otimes |\boldsymbol{m}\rangle.$$

However, as we now show, we can define another LOCC-simulating isometry, similar to $\mathcal{C}$, that maps $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle$ to an entangled state.

4.1.2 A complete set of LOCC-simulating isometries

In Definition 29 we have used the basis $\{|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\}$ to define the isometry $\mathcal{C}$. However, there is nothing special about the choice of the irrep weights $\boldsymbol{m}$. In fact, the set of states,

$$|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_g := U(g)|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \tag{4.14}$$

forms an equally valid basis for the irreps, labelled by the new weights $\boldsymbol{m}_g$ (the multiplicity index λ can always be relabelled if it is needed). On the other hand, by definition, the irrep basis states mix among themselves under the action of the group,

$$U(g)|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g)\,|\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle, \tag{4.15}$$

where $D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g)$ is the matrix representation of the $\boldsymbol{j}^{\text{th}}$ irrep. Reversing Eq. (4.14), we get,

$$|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g^{-1})\,|\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle_g. \tag{4.16}$$

Hence, if we had defined the isometry relative to the new weights, the state $|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle$ would be mapped to an entangled state. In fact, the isometry $\mathcal{C}$ is only one of a class of isometries that can be defined for different choices of $g \in G$ relative to the weights $\{\boldsymbol{m}_g\}$. The map $\mathcal{C}$ is merely the isometry corresponding to the identity element of the group.

Definition 30. *For every $g \in G$, we define the isometry $\mathcal{C}_g$ as,*

$$\mathcal{C}_g := (\mathcal{U}(g) \otimes \mathcal{I}_B) \circ \mathcal{C} \circ \mathcal{U}^{\dagger}(g), \tag{4.17}$$

where $\mathcal{U}(g) := U(g)(\bullet)U^{\dagger}(g)$, and $\mathcal{I}_B$ is the identity superoperator acting on $\mathscr{H}_B$.

The isometry $\mathcal{C}_g$ acts on basis states, $|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle_g$, and maps them to

$$|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle_g \mapsto |\boldsymbol{j},\lambda;\boldsymbol{m}\rangle_g \otimes |\boldsymbol{m}\rangle.$$

Note that the image space of all the isometries $\{\mathcal{C}_g\}$ is the space $\mathscr{W}$ in (4.4). Clearly, the proof of Proposition 23 can easily be modified to apply to all the set of isometries $\{\mathcal{C}_g\}$. Moreover, note that the state $|\phi\rangle = |\boldsymbol{j},\lambda;\boldsymbol{m}\rangle$ is mapped to

$$|\phi\rangle \mapsto^{\mathcal{C}_g} |\tilde{\phi}\rangle = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j},\lambda)}_{\boldsymbol{m},\boldsymbol{m}'}(g^{-1})\,|\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle_g \otimes |\boldsymbol{m}'\rangle, \tag{4.18}$$

which is, in general, an entangled state.

It is instructive at this stage to look at the specific group SU(2) to gain some intuition. The same results also holds for the group of rotations SO(3), as it has the same Lie algebra, so we do not need to consider that case separately. The weights $\boldsymbol{m}$ of the associated algebra $\mathfrak{su}(2)$ are one dimensional and correspond to the eigenvalues of the angular momentum operator, J_z, along the z-direction. Each irrep is labeled by the single number j corresponding to the maximum z-eigenvalue of angular momentum, and the total angular momentum, J^2, equals $j(j+1)$. There is obviously nothing special about the choice of the z-axis. The z-axis can be rotated to a new axis $\hat{\mathrm{n}}$, which corresponds to applying the respective group representation on the quantum states. One way to specify an element of the group is to determine the axis $\hat{\mathrm{n}}$ to which it takes the z-axis. In other words, each isometry in the class of definition 30 is identified by the choice of a new z-direction and can be denoted as $\mathcal{C}_{\hat{\mathrm{n}}}$.

Thus, to take full advantage of the entanglement features of the embedding, one has to take more than one isometry into consideration. As we shall now see, if $\rho \in \mathcal{B}(\mathscr{H})$ is an asymmetric state then there exists $g \in G$ such that $\mathcal{C}_g(\rho)$ is an entangled state. In fact, for the $SU(2)$ group we will see that only two directions are needed to characterize all the asymmetry properties of a state. That is, if $\mathcal{C}_{\hat{\mathrm{n}}}(\rho)$ is separable for two independent choices of $\hat{\mathrm{n}}$, then ρ is necessarily G-invariant.

Also for more general simply connected groups, there exists a *finite* number of isometries $\{\mathcal{C}_{g_i}\}$ (associated with a finite number of group elements $\{g_i\}$) that capture all the asymmetry properties of a state. That is, if a state is mapped to a separable state by all the isometries in the finite set $\{\mathcal{C}_{g_i}\}$, then the state must be symmetric. This allows in principle to check whether a state is G-invariant or not, by considering its bipartite image states only for a finite number of isometry elements. Otherwise, all the infinite isometries, each associated with a member of the group, must have been considered before such an assessment could be made.

Before proving the above claim rigorously, let us illustrate the idea of the proof with the simple and more familiar example of the group SU(2). Suppose that $\mathcal{C}(\rho)$ is separable for some state ρ. Then, according to Proposition 24 the state ρ has no coherence in $\boldsymbol{m}$, the eigenvalue of the J_z operator. It means, in turn, that the state ρ commutes with J_z. By the same argument if $\mathcal{C}_{\hat{x}}(\rho)$ is separable then the state ρ commutes with J_x. Therefore, if both $\mathcal{C}(\rho)$ and $\mathcal{C}_{\hat{x}}(\rho)$ are separable then ρ commutes with both J_z and J_x. But since $[J_z, J_x] = \imath J_y$, ρ also commutes with J_y and so it must commute with all the elements of the group, which means that ρ is an $SU(2)$-invariant state. This line of argument can be generalized to other groups, as we now demonstrate.

Suppose G is a simply connected group parametrized by r parameters. Let $\mathfrak{g}$ be the Lie algebra of G of rank ℓ, and let $\mathfrak{h}$ be its ℓ-dimensional Cartan subalgebra. Denote the operator representation of the infinitesimal generators of the group as $X_a : \mathscr{H} \to \mathscr{H}$, for $a = 1, \cdots, r$. Similarly, denote the representation of the Cartan operators spanning $\mathfrak{h}$ as $H_i : \mathscr{H} \to \mathscr{H}$, where $i = 1, \cdots, \ell$.

Now, let $S \subset G$ be the subgroup of G whose members permute the infinitesimal generators of the group among themselves. By this we mean, for every $s \in S$,

$$U(s)\, X_a\, U(s)^\dagger = X_{a'(s)}, \;\; a, a' \in \{1, \ldots, r\}\,. \tag{4.19}$$

As both $\mathfrak{g}$ and $\mathfrak{h}$ are finite, the subgroup S contains only a *finite* number of elements. We are now ready to prove the general case.

Proposition 25. *Let $\rho \in \mathcal{B}(\mathscr{H})$. The state ρ is G-invariant if and only if for all s belonging to the finite subgroup $S \subset G$, the state $\mathcal{C}_s(\rho)$ is separable.*

Proof. If ρ is G-invariant, then $\mathcal{C}_g(\rho)$ is separable for all $g \in G$, and thus for all $s \in S$, since $\{\mathcal{C}_g\}$ is a set of LOCC-simulating maps.

We therefore assume that $\mathcal{C}_s(\rho)$ is separable for all $s \in S$. The requirement that $\mathcal{C}_s(\rho)$ is separable implies that ρ, when expressed in the basis $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s$, has no coherence in $\boldsymbol{m}$. Consider the projection,

$$\Pi^{(s)}_{\boldsymbol{m}} := \sum_{\boldsymbol{j},\lambda} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s\langle \boldsymbol{j}, \lambda; \boldsymbol{m}|.$$

The condition for separability is equivalent to the requirement that $[\rho, \Pi^{(s)}_{\boldsymbol{m}}] = 0$ for all $\boldsymbol{m}$ (see Proposition 24).

The set of operators, $H_i^{(s)} := U(s)\, H_i\, U(s)^\dagger$, are all diagonal in the new basis,

$$H_i^{(s)}\, |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s = \boldsymbol{m}_i\, |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s,$$

and form a representation for new Cartan operators. It follows that $H_i^{(s)} = \sum_{\boldsymbol{m}} \boldsymbol{m}_i\, \Pi^{(s)}_{\boldsymbol{m}}$. Thus, if $\mathcal{C}_s(\rho)$ is separable, ρ must satisfy

$$[\,\rho, H_i^{(s)}] = 0, \quad i = 1, \ldots, \ell.$$

But this is true for all $s \in S$ (including the identity e, where $H_i = H_i^{(e)}$). Every X_a can be constructed from the commutators of $H_i^{(s)}$, once all the $H_i^{(s)}$ for all $s \in S$ are included. It follows that the state ρ commutes with all the generators X_a, and consequently, with all the elements of the group as well. In other words, the state is G-invariant.

□

Next, we see how entanglement of the embedded state changes under G-covariant transformations of the original state. This, in turn, enables us to relate the asymmetry features of the original state to the ensuing entanglement.

4.2 Constructing Asymmetry Monotones From Entanglement Monotones

Roughly speaking, Propositions 23 and 25 imply that the evolution of asymmetry can be simulated by the evolution of entanglement. In particular, we can define asymmetry monotones for the states acting on $\mathscr{H}$ in terms of the entanglement monotones of the states acting on $\mathscr{W}$ to which they are mapped.

Definition 31. *For every bipartite entanglement monotone E, we define a family of asymmetry monotones, a monotone for each $g \in G$, as,*

$$A_E^g : \mathcal{B}(\mathscr{H}) \to \mathbb{R}^+ : \rho \mapsto E\left(\mathcal{C}_g(\rho)\right). \tag{4.20}$$

The following proposition ensures that A_E^g is indeed an asymmetry monotone, assuming that E is an entanglement monotone.

Proposition 26. *Consider an entanglement monotone E. If $\rho \mapsto^{\mathcal{E}_{cov}} \sigma$ is possible, then for every $g \in G$,*

$$E\left(\mathcal{C}_g(\rho)\right) \geq E\left(\mathcal{C}_g(\sigma)\right). \tag{4.21}$$

Remark. A similar inequality holds in the case of non-deterministic G-covariant CP-maps for the average of E, assuming E is an ensemble monotone (see Section 2.4).

Proof. The result follows directly from the definition 30 and the extension of proposition 23 to all isometries $\mathcal{C}_g$. □

As not all asymmetric states are taken to entangled states, the asymmetry monotone A_E^g is not faithful, even if E is itself a faithful entanglement monotone. However, proposition 25 allows us to define a faithful asymmetry monotone from the monotones A_E^g.

Proposition 27. *The function*

$$A_E^{sup} := \sup_{g\in G} A_E^g, \tag{4.22}$$

where $\sup_{g\in G}$ *stands for the supremum taken over all g in G, is a faithful asymmetry monotone, provided E is a faithful entanglement monotone.*

Replacing the supremum above by the maximum over the finite number of elements in $S \subset G$ over the finite number of elements in $S \subset G$ (see Proposition 25) will also lead to a faithful asymmetry monotone. The supremum of the finite number of elements in $S \subset G$ (see Proposition 25) is the same as their maximum. For example, if $G = SU(2)$, the function

$$\max_{\hat{\mathrm{n}}\in\{\hat{z},\,\hat{x}\}} A_E^{\hat{\mathrm{n}}}$$

is an asymmetry monotone.

4.2.1 Unitary Transformation

If the CP-map is reversible, *i.e.* a unitary operation, then the condition of the monotonicity for the monotones (4.20) must be true in both directions, which in turn implies that the monotone functions must remain constant.

Proposition 28. *Consider an entanglement monotone E. If $\rho \overset{\mathcal{E}_{cov}}{\leftrightarrow} \sigma$ is a reversible G-covariant transformation, then for every $g \in G$, A_E^g is a conserved quantity; i.e.*

$$E\left(\mathcal{C}_g(\rho)\right) = E\left(\mathcal{C}_g(\sigma)\right). \tag{4.23}$$

Thus, for closed systems governed by a symmetric Hamiltonian, every entanglement monotone E leads to new conserved quantities, $\{A_E^g\}_{g\in G}$. For a Hamiltonian that is symmetric with respect to the group G, the expectation values of the generators of G are also conserved quantities. However, unlike A_E^g, for open systems these expectation values are not behaving monotonically.

Chapter 5

Applications and examples

In the present chapter, we introduce specific monotones and case studies as examples in order to demonstrate how the results we developed in Chapter 4 can be applied to various problems in the resource theory of asymmetry.

5.1 The pure-state standard form

First, we show how pure states can be transformed to a standard form that contains all the information relevant for determining the asymmetry of the state and no redundancies. In particular, as G-covariant transformations are not restricted on how they act on the multiplicity spaces, no measure of the strength of the resource can depend on the changes that affect the multiplicity indices. The standard form of the state has no explicit non-trivial dependence on the multiplicity indices. We have already already seen the standard form of pure states in the case of the group $U(1)$. The standard forms of pure states for the groups $U(1)$ and $SU(2)$ were determined in [37]. Here, we present the form for a general semi-simple compact Lie group.

Recall that the system's Hilbert space can be expressed as the direct sum $\mathscr{H} = \bigoplus_{\boldsymbol{j}} \mathscr{H}_{\boldsymbol{j}}$, with $\boldsymbol{j}$ labelling the irreps of G (2.37). Recall as well that the eigenstates $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle$ form a basis for $\mathscr{H}_{\boldsymbol{j}}$, where $\boldsymbol{m}$ denotes the ℓ-dimensional weight vectors, $\boldsymbol{j}$ is the highest weight as well as the index labelling the irrep itself, and λ labels the multiplicity. We now define $\mathscr{H}_{\boldsymbol{j},\boldsymbol{m}}$ as the subspace spanned by the basis states for fixed $\boldsymbol{j}$ and $\boldsymbol{m}$, *i.e.* $\mathscr{H}_{\boldsymbol{j},\boldsymbol{m}} := \operatorname{span}\{|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\}_{\lambda}$. Operations on multiplicity spaces are unaffected by the G-SSR, and, as a result, any pure state can be transformed via G-covariant unitary transformations to a standard form. Consider the pure state

$$|\psi\rangle = \sum_{\boldsymbol{j},\boldsymbol{m}} c_{\boldsymbol{j},\boldsymbol{m}} \, |\psi_{\boldsymbol{j},\boldsymbol{m}}\rangle, \tag{5.1}$$

where $|\psi_{\boldsymbol{j},\boldsymbol{m}}\rangle \in \mathscr{H}_{\boldsymbol{j},\boldsymbol{m}}$ are normalized states, and let $p_{\boldsymbol{j},\boldsymbol{m}} := |c_{\boldsymbol{j},\boldsymbol{m}}|^2$. We apply the Gram-Schmidt process to extend $|\psi_{\boldsymbol{j},\boldsymbol{m}}\rangle$ to a full orthonormal basis $\{|\psi_{\boldsymbol{j},\boldsymbol{m}}\rangle\} \cup \{|\phi_{\boldsymbol{j},\lambda;\boldsymbol{m}}\rangle\}_\lambda$ spanning the subspace $\mathscr{H}_{\boldsymbol{j},\boldsymbol{m}}$. The unitary transformation

$$U := \sum_{\boldsymbol{j}} \left(\frac{c^*_{\boldsymbol{jm}}}{|c_{\boldsymbol{jm}}|} |\boldsymbol{j}, 0; \boldsymbol{m}\rangle\langle\psi_{\boldsymbol{j},\boldsymbol{m}}| + \sum_{\lambda\neq 0} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle\langle\phi_{\boldsymbol{j},\lambda;\boldsymbol{m}}| \right), \tag{5.2}$$

is G-covariant, in fact it is G-invariant, and takes the state $|\psi\rangle$ to the standard form

$$|\psi_0\rangle = \sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{j},\boldsymbol{m}}} \, |\boldsymbol{j}; \boldsymbol{m}\rangle, \tag{5.3}$$

where $|\boldsymbol{j}; \boldsymbol{m}\rangle$ is our shorthand notation for the fixed choice of the multiplicity index, namely the state $|\boldsymbol{j}, 0; \boldsymbol{m}\rangle$.

Of course, as we mentioned in Section 4.1.1, the choice of weights is not unique. So the standard form is always defined relative to a choice of the weights, and we have in fact a class of standard forms, each associated with a member of the group. From Eq. (4.16) it follows that

$$|\psi_0\rangle_g = \sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{j},\boldsymbol{m};g}} \, |\boldsymbol{j}; \boldsymbol{m}\rangle_g. \tag{5.4}$$

As before, the state in Eq. (5.3) is in the standard form associated with the identity element e, in which case we omit the identity label.

Definition 32. *The weight spectrum of a state $|\psi\rangle$ associated with a group element $g \in G$ is the set*

$$spec^{(g)}_{\boldsymbol{m}}(\psi) := \left\{ \boldsymbol{m} \,\middle|\, |\psi\rangle = \sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{j},\boldsymbol{m};g}} \, |\boldsymbol{j}; \boldsymbol{m}\rangle_g, \; p_{\boldsymbol{j},\boldsymbol{m};g} > 0 \right\}, \tag{5.5}$$

ie. the set of the weight labels $\boldsymbol{m}$ that label the kets in the standard form of $|\psi\rangle$.

We are now ready to present our examples and discuss some applications of the results of Chapter 4 in various case studies.

5.2 Entanglement-based asymmetry monotones

We now review in more detail some examples of asymmetry monotones that are constructed from entanglement monotones through the class of LOCC simulating isometries. Many totally new asymmetry monotone can be constructed from entanglement monotones using the isometry $\mathcal{C}$. Here we introduce a few such monotones for the first time. One uses the negativity of entanglement, and the other uses the logarithmic negativity [70, 97].

5.2.1 The negativity of entanglement as a measure of asymmetry

Negativity of entanglement is an important measure of entanglement with many applications. As our first example of an entanglement-based monotone, we use negativity of entanglement to construct a new asymmetry monotone:

Definition 33. *The negativity of asymmetry is defined as,*

$$A_N(\rho) := \frac{\| \mathcal{C}(\rho)^\Gamma \|_1 - 1}{2}, \tag{5.6}$$

and the logarithmic negativity of asymmetry is

$$A_{LN}(\rho) := \log \| \mathcal{C}(\rho)^\Gamma \|_1, \tag{5.7}$$

where Γ *denotes partial transpose and* $\| \bullet \|_1$ *is the 1-norm*

$$\| \rho \|_1 = Tr \sqrt{\rho^\dagger \rho}. \tag{5.8}$$

Both negativity and logarithmic negativity are particular useful monotones as they are very easily computable for all states, pure or mixed. Note however that the negativity and the logarithmic negativity do not reduce to entropy functions for pure states.

For pure states, the negativity of asymmetry can be expressed in a very simple closed form. As we saw in Section 5.1, every pure state can be brought to the standard form by G-covariant transformations. Consider the pure state, $|\psi\rangle = \sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{j},\boldsymbol{m}}}\, |\boldsymbol{j};\boldsymbol{m}\rangle$, in the standard form of Eq. 5.3. The norm of the partial transpose is

$$\| \mathcal{C}\left(|\psi\rangle\langle\psi|\right)^{\Gamma} \|_1 = \left(\sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{jm}}}\right)^2 . \tag{5.9}$$

It follows that the logarithmic negativity of asymmetry is equal to

$$A_{LN}\left(|\psi\rangle\langle\psi|\right) = 2\log\left(\sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{jm}}}\right). \tag{5.10}$$

After simplifying the equations, the negativity of asymmetry can be expressed as

$$A_N\left(|\psi\rangle\langle\psi|\right) = \sum_{\boldsymbol{j}\neq\boldsymbol{j}',\boldsymbol{m}\neq\boldsymbol{m}'} \sqrt{p_{\boldsymbol{jm}}\, p_{\boldsymbol{j}'\boldsymbol{m}'}}. \tag{5.11}$$

An important feature of a monotone like the negativity is that it applies, by definition, only to bipartite states. There is no sense in performing a partial transpose on the state of a single system. Similarly, the mutual information is essentially in terms of correlations of two or more systems. Interestingly, however, applied to the image states of the isometry, such monotones capture information about some aspect of the original *unipartite* state. Yet, it is hard to see how the same information would be accessible in any other way beside mapping the original states to bipartite image states.

5.3 Measures based on distance

Monotones based on how far states are from the set of non-resources are known as distance measures [92]. The geometric intuition here can apply to various resources, not just entanglement. If the resource is entanglement, then the more entangled a state is, the further away it is from the set of separable states. The 'distance' between any two states ρ and σ is measured by a function $D(\rho, \sigma)$ with distance-like properties (e.g. $D(\rho, \sigma) \geq 0$ with equality if and only if $\sigma = \rho$). The function D, however, need not be literally a metric. All is needed is that D preserve the partial order, and that $D(\rho, \rho) = 0$

for all ρ. The function D need not satisfy the triangle inequality, for instance, and it need not even be symmetric. The distance-based monotone is defined as the minimum distance to the target set Q:

$$E_D(\rho) := \inf_{\sigma \in \mathrm{Q}} D(\rho, \sigma). \tag{5.12}$$

In the case of entanglement, the target set is the set SEP of separable states. Unlike the monotones in the previous section, distance-based asymmetry monotones can also be defined directly by choosing the target set Q to be the set of G-invariant states. A different set of asymmetry monotones can, however, be defined indirectly in terms of distance-based entanglement monotones. How the two sets of monotones compare is an important question. Here we introduce one important example of a distance-based monotone.

If the function $D(\rho, \sigma) = \mathrm{Tr}\left[\rho \log \rho - \rho \log \sigma\right]$ is the relative entropy (2.72), then E_D above is called the relative entropy of entanglement (REE) (2.71). The REE has many nice properties and it plays a crucial role in the theory of entanglement [48, 71].

Just as in the previous subsection, we can use Eq. (4.20) to define an asymmetry monotone that is based on the REE. We call this monotone the relative entropy of asymmetry (REA). However, unlike the monotones in the previous subsection, distance-based monotones of asymmetry can also be defined directly by choosing the target set Q to be the set of G-invariant states. In this case, if D is taken to be the relative entropy then the resulting monotone is the G-asymmetry [35, 88]. How the G-asymmetry is related the REA is an important question which we discuss here only partially. A more detailed study of the comparison is left for future work.

5.3.1 The Relative Entropy of Asymmetry

As discussed above, an important and widely studied entanglement distance monotone is the REE

$$E_R(\rho) = \min_{\sigma\in\mathrm{SEP}} S\left(\rho \parallel \sigma\right), \tag{5.13}$$

where the relative entropy $S\left(\rho \parallel \sigma\right)$ (2.72) is the distance function and where the infimum can be replaced with a minimum. The relative entropy is not symmetric and does not preserve the triangle inequality. Following Section 4.2, we can define a class of asymmetry monotones

$$A_R^g(\rho) := E_R\left(\mathcal{C}_g(\rho)\right), \quad \forall g \in G, \tag{5.14}$$

and we can define the relative entropy of asymmetry (REA) to be the faithful monotone obtained from the class of asymmetry monotones.

Definition 34. *The relative entropy of asymmetry (REA) is the monotone,*

$$A_R^{max}(\rho) := \max_{s\in S} A_R^s(\rho), \tag{5.15}$$

where the finite subgroup $S \subset G$ was defined by the property in Eq. (4.19).

From the discussion in Section 4.2 it follows that $A_R^{\max}$ is faithful, *i.e.* $A_R^{\max}(\rho) = 0$ if and only if ρ is G-invariant.

5.3.2 Comparison with G-asymmetry

As we discussed before, choosing the set INV of G-invariant states as the target set Q for the states acting on $\mathscr{H}$ leads to a measure known as the G-asymmetry [88] or, alternatively, the relative entropy of frameness [35]

$$A_G := \min_{\sigma\in\mathrm{INV}} S\left(\rho \parallel \sigma\right) = S\left(\mathcal{G}(\rho)\right) - S(\rho). \tag{5.16}$$

Here, $\mathcal{G}(\rho)$ is the twirling operation discussed in Eq. (2.36) of Section 2.2.

In order to compare G-asymmetry with REA, let us first consider a slightly different function, also based on the relative entropy of entanglement but with a different target set relative to which the distance is minimized. Each isometry $\mathcal{C}_s$, for $s \in S$, leads in

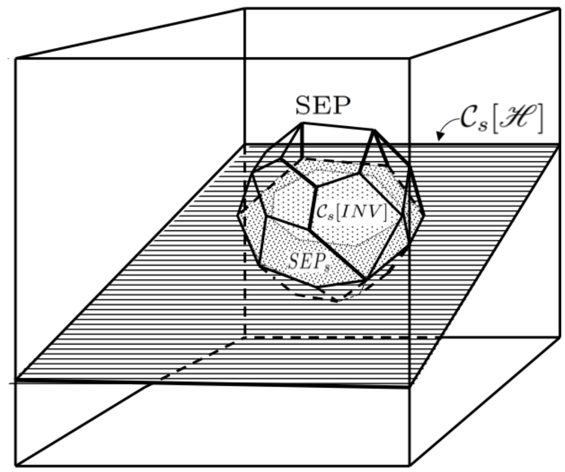

Figure 5.1: A schematic depiction of the space of bipartite states. SEP_s is the intersection of the set of separable states, SEP, with the image of the $\mathcal{C}_s$-isometry denoted here as $\mathcal{C}_s[\mathscr{H}]$. The image of the set of G-invariant states under $\mathcal{C}_s$, denoted as $\mathcal{C}_s[\text{INV}]$, is a strict subset of SEP_s.

general to a strict distinct subset of SEP that act on $\mathscr{H} \otimes \mathscr{H}_B$. We denote the set by SEP_s. That is, SEP_s is the intersection of SEP with the image of $\mathcal{C}_s$ (see Figure 5.1). We also denote the image of the set of G-invariant states under $\mathcal{C}_s$ as $\mathcal{C}_s[\text{INV}]$. Note that if G is not Abelian, then $\mathcal{C}_s[\text{INV}]$ is a strict subset of SEP_s[1]. For example, as we saw earlier, SEP_s also contains product states $|\tilde{\phi}\rangle = |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s \otimes |\boldsymbol{m}\rangle$ that are the images of the states $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s$. Yet, the eigenstates $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s$ are not G-invariant when $\boldsymbol{j} \neq 0$. We

[1] If G is Abelian, then all separable states in SEP_s are images of invariant states and thus $\mathcal{C}_s[\text{INV}] = \text{SEP}_s$ (see Appendix B).

now define the function A_R^{s*} as

$$A_R^{s*}(\rho) := \min_{\sigma \in \mathcal{C}_s[\mathrm{INV}]} S\left(\mathcal{C}_s(\rho) \parallel \sigma\right). \tag{5.17}$$

A_R^{s*} can, in general, be greater than $A_R^{\max}$ but it can never be smaller.

Proposition 29. *For every $s \in S$, A_R^{s*} are greater than or equal to the REA:*

$$A_R^{\max}(\rho) \leq A_R^{s*}(\rho), \quad \forall \rho \in \mathcal{B}(\mathscr{H}). \tag{5.18}$$

Proof. For any given $s \in S, \mathcal{C}_s[\mathrm{INV}] \subset \mathrm{SEP}_s \subseteq \mathrm{SEP}$. It follows that $A_R^s \leq A_R^{s*}$, since A_R^s is obtained by minimizing the relative entropy over the larger set SEP that includes $\mathcal{C}_s[\mathrm{INV}]$. As this is true for all $s \in S$, A_R^{s*} is greater than or equal to the maximum $A_R^{\max}$ too. □

The isomorphism between the two sets INV and $\mathcal{C}_s[\mathrm{INV}]$ implies that the minimum taken over $\mathcal{C}_s[\mathrm{INV}]$ in the definition of $A_R^{s*}(\rho)$ coincides with the minimum of G-asymmetry A_G in Eq. (5.16). By this we mean that the separable state that minimizes the relative entropy in Eq. (5.17) is the image, under the isometry $\mathcal{C}_s$, of the invariant state that minimize the relative entropy in Eq. (5.16).

To see this, consider the spectral decomposition of states ρ and σ acting on $\mathscr{H}$, namely, $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ and $\sigma = \sum_i q_i|\phi_i\rangle\langle\phi_i|$. Recall that $\mathcal{C}_s$, being an isometry, preserves the inner product between pure states[2]. It follows that the spectral decomposition of the image states are $\mathcal{C}_s(\rho) = \sum_i p_i|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ and $\mathcal{C}_s(\sigma) = \sum_i q_i|\tilde{\phi}_i\rangle\langle\tilde{\phi}_i|$, where $|\tilde{\psi}\rangle$, and $|\tilde{\phi}\rangle$ are themselves the images of $|\psi\rangle$ and $|\phi\rangle$, *i.e.*, $|\psi\rangle \mapsto^{\mathcal{C}_s} |\tilde{\psi}\rangle$, $|\phi\rangle \mapsto^{\mathcal{C}_s} |\tilde{\phi}\rangle$. Hence, for every two states ρ and σ, the two relative entropies $S(\rho \parallel \sigma)$ and $S\left(\mathcal{C}_s(\rho) \parallel \mathcal{C}_s(\sigma)\right)$ must be equal. Two corollaries follow:

Corollary 30. *For every $s \in S$, the functions A_R^{s*} and A_G are identical, $A_R^{s*} = A_G$.*

[2] In fact, as is apparent from definition 29, the isometry $\mathcal{C}_s$ merely 'repeats' the weight label $\boldsymbol{m}$ for each eigenket $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s$ by attaching to it the ket $|\boldsymbol{m}\rangle$, *i.e.* $|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s \mapsto |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle_s \otimes |\boldsymbol{m}\rangle$.

Corollary 31. *The G-asymmetry is greater than or equal to the REA.*

$$A_R^{\max}(\rho) \leq A_G(\rho), \;\; \forall \rho \in \mathcal{B}(\mathscr{H}). \tag{5.19}$$

The relationship between G-asymmetry and the REA goes deeper than what we have discussed so far, and our discussion here must be viewed only as an introductory treatment of the subject. We leave the more complete discussion to future works.

5.4 Case study: Entanglement-based asymmetry monotones versus information-based asymmetry measures

In this section, we compare the asymmetry monotones based on entanglement as we have defined in this thesis with the information-based asymmetry monotones already studied in the context of asymmetry resources. By information-based asymmetry monotones here we mean monotones that are defined as the difference of an information measure between a state and the state's uniform twirling.

$$A_I(\rho) = \mathcal{I}\left(\mathcal{G}(\rho)\right) - \mathcal{I}(\rho), \tag{5.20}$$

where $\mathcal{I}(\rho)$ is a function measuring in some ways the information content of a state. The most important example of such a measure is the von-Neumann entropy function. An important example of such measures is of course the G-asymmetry.

Consider the following two standard pure states:

$$|\psi_1\rangle = \sqrt{p_1}\,|1/2;1/2\rangle + \sqrt{p_2}\,|1/2;-1/2\rangle + \sqrt{p_3}\,|1;1\rangle + \sqrt{p_4}\,|1;0\rangle \tag{5.21}$$

$$|\psi_2\rangle = \sqrt{p_1+p_2}\,|1/2;1/2\rangle + \sqrt{p_3+p_4}\,|1;1\rangle. \tag{5.22}$$

The two states have the same outcome after the twirling operation,

$$\rho_0 = (p_1+p_2)\,\rho_{\mathscr{H}_{1/2}} + (p_3+p_4)\,\rho_{\mathscr{H}_1}, \tag{5.23}$$

where $\rho_{\mathscr{H}_j}$ denotes the normalized projection to the subspace $\mathscr{H}_j$ (2.37). However, their images under the $\mathcal{C}$ isometry have different Schmidt coefficients, namely $\{p_1, p_2, p_3, p_4\}$ and $\{p_1 + p_2, p_3 + p_4\}$ respectively.

Hence, information-based asymmetry monotones such as the entropy function defined by uniform twirling cannot detect the difference between the asymmetry of two such pure states. The entropy of both initial pure states is zero, and the entropy of the twirled states are the same, simply because the twirled states themselves are the same. However, asymmetry monotones based on bipartite entanglement monotones need not give the same asymmetry value to the two states as their Schmidt coefficients are different. Thus, the entanglement-based monotones can specify when one such state is more asymmetric than the other, and, for example, can be transformed to the other one by covariant transformations without violating the asymmetry.

As an example, let $p_1 = 1/4$, $p_2 = 1/4$, $p_3 = 1/6$ and $p_4 = 1/3$. The G-asymmetry (or the relative entropy of frameness) of either one of the two states is

$$\begin{aligned} A_G\left(|\psi_1\rangle\langle\psi_1|\right) &= A_G\left(|\psi_2\rangle\langle\psi_2|\right) \\ &= S\left(\rho_0\right) - 0 = 0.5\log_2 4 + 0.5\log_2 6 \simeq 2.29, \end{aligned} \tag{5.24}$$

where ρ_0 is the state in (5.23). The negativity of asymmetry (5.11), on the other hand, is very different for the two states:

$$\begin{aligned} A_N\left(|\psi_1\rangle\langle\psi_1|\right) &\simeq 1.47, \\ A_N\left(|\psi_2\rangle\langle\psi_2|\right) &= 0.50, \end{aligned} \tag{5.25}$$

implying, among other things, that $|\psi_2\rangle$ cannot evolve to $|\psi_1\rangle$ under $SU(2)$-covariant transformations.

5.5 Case study: Vidal monotones and inequivalent pure-state asymmetry resources

An important class of bipartite entanglement monotones for pure states are the monotones known as Vidal monotones [95] (see theorems 11 and 12 in Section 2.3.5.). We already defined the equivalent of Vidal monotones for the case of $U(1)$-asymmetry. We now define Vidal's asymmetry monotones for a general semi-simple compact Lie group G. For the rest of this section, we assume that all pure states belong to a finite-dimensional subspace $\mathscr{H}_d \subseteq \mathscr{H}$ of dimension d.

Definition 35. *Let $|\psi\rangle \mapsto^{\mathcal{C}_g} |\tilde{\psi}\rangle_g$. The functions*

$$A_k^g(|\psi\rangle) := E_k(|\tilde{\psi}\rangle_g), \;\; k = 1, \cdots, d, \tag{5.26}$$

are the set of Vidal asymmetry monotones of $|\psi\rangle$, where E_k are the Vidal entanglement monotones of definition 16 in Section 2.3.5.

For a bipartite pure state $|\psi\rangle = \sum_{\boldsymbol{j},\boldsymbol{m}} \sqrt{p_{\boldsymbol{j}\boldsymbol{m};g}}\, |\boldsymbol{j};\boldsymbol{m}\rangle_g$ in the standard form of (5.3), the Vidal monotones are equal to

$$A_k^g\left(|\psi\rangle\right) = \sum_{i=k}^{d} p_{\downarrow i;g}, \tag{5.27}$$

where $p_{\downarrow i;g} \in \boldsymbol{p}_{\downarrow g}\left(|\psi\rangle\right)$, and $\boldsymbol{p}_{\downarrow g}\left(|\psi\rangle\right) := (p_{\downarrow 1;g}, \cdots, p_{\downarrow d;g})$ is the d-tuple comprised of the amplitudes $\{p_{\boldsymbol{j},\boldsymbol{m};g}\}$ of the state $|\psi\rangle$ ordered in decreasing order $p_{\downarrow 1;g} \geq \cdots \geq p_{\downarrow d;g}$.

Consider the states $|\psi_1\rangle = |\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}$ and $|\psi_2\rangle = |\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}$. The two states are known to be inequivalent resources, in the sense that transforming one to the other is impossible given the symmetry restrictions, even with probability less than one [37,61]. For example, in the case of the group $SU(2)$, each state corresponds to the system in question singling out a different spatial orientation. Rotating from one orientation to the other requires a reference frame for orientation that would break the rotational symmetry [37].

We now show that the same conclusion can be reached from the majorization condition of pure-bipartite-state transformations under LOCC (see Section 2.3.5), or equivalently by applying what we have called the Vidal asymmetry monotones in this section.

First, we consider the image states under the isometry $\mathcal{C}_{g_1}$. The state $|\psi_1\rangle$ is mapped to the product state

$$\mathcal{C}_{g_1}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}\right) = |\boldsymbol{j};\boldsymbol{m}\rangle_{g_1} \otimes |\boldsymbol{m}\rangle. \tag{5.28}$$

Following Eq. (4.16), we have

$$|\boldsymbol{j},\lambda;\boldsymbol{m}\rangle_{g_2} = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g_2 g_1^{-1})\, |\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle_{g_1}, \tag{5.29}$$

so that the state $|\psi_2\rangle$ is mapped to

$$\mathcal{C}_{g_1}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}\right) = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g_2 g_1^{-1})\, |\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle_{g_1} \otimes |\boldsymbol{m}'\rangle. \tag{5.30}$$

Clearly, the state in (5.28), being a product state, cannot be transformed under LOCC to the state in (5.30) with any probability. But since $\mathcal{C}_{g_1}$ is a LOCC-simulating isometry by Definition 28 of Section 4.1, the original state $|\psi_1\rangle$ cannot be transformed to $|\psi_2\rangle$ by G-covariant CP-maps either, even not with a non-zero probability.

On the other hand, using the mapping $\mathcal{C}_{g_2}$ instead we get to the opposite situation, where,

$$\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}\right) = \sum_{\boldsymbol{m}'} D^{(\boldsymbol{j})}_{\boldsymbol{m},\boldsymbol{m}'}(g_1 g_2^{-1})\, |\boldsymbol{j},\lambda;\boldsymbol{m}'\rangle_{g_2} \otimes |\boldsymbol{m}'\rangle, \tag{5.31}$$

and

$$\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}\right) = |\boldsymbol{j};\boldsymbol{m}\rangle_{g_2} \otimes |\boldsymbol{m}\rangle. \tag{5.32}$$

By the same arguments, $\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}\right)$ cannot be transformed to $\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}\right)$, and consequently, $|\psi_2\rangle$ cannot be transformed to $|\psi_1\rangle$ with any non-zero probability either.

Of course, this situation is a special case were the amplitudes of $\mathcal{C}_{g_1}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}\right)$ do not majorize those of $\mathcal{C}_{g_1}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}\right)$ and $\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_2}\right)$ do not majorize those of $\mathcal{C}_{g_2}\left(|\boldsymbol{j};\boldsymbol{m}\rangle_{g_1}\right)$. Thus, we have

$$\begin{cases} 0 &= A_1^{g_1}\left(|\psi_1\rangle\right) < A_1^{g_1}\left(|\psi_2\rangle\right) \\ 0 &= A_1^{g_2}\left(|\psi_2\rangle\right) < A_1^{g_2}\left(|\psi_1\rangle\right). \end{cases} \tag{5.33}$$

More generally, Vidal monotones can be employed to determine whether a given pure-state to pure-state transformation is forbidden under the symmetry.

5.6 Case study: Bounds on G-covariant state discrimination

In this section, we consider the task of state discrimination by G-covariant transformations. We take advantage of the results of the papers by Hayashi *et al.* [39, 40]. By state discrimination we mean the task of performing a measurement on a system to find out which one of a set of states the system is in. Discriminating states has significant applications in cryptographic protocols [12], channel capacities [41,99], and distributed quantum information processing [21]. Given the restriction to G-covariant measurements, it is natural to expect that asymmetric states are more difficult to distinguish than G-invariant ones, as part of their characteristics is not discernible by covariant measurements.

We assume we have a system whose Hilbert space is finite-dimensional. Let D be the dimension of the Hilbert space. Also we assume we are given a set of states $\mathcal{S} = \{\rho_1, \cdots, \rho_s\}$ that the system is guaranteed to be in. We say that the state ρ_i from the set can be discriminated from the rest of the states in S with certainty, if there exists a POVM whose outcome correctly identifies the label i with probability one whenever the system is in fact in state ρ_i.

Here, we investigate situations where a POVM $\{M_i\}$ exists that satisfies the following conditions:

$$\sum_i M_i = I, \tag{5.34}$$

$$0 \leq M_i \leq I, \tag{5.35}$$

$$\mathrm{Tr}\left(M_i\, \rho_i\right) = 1, \;\; i = 1, \cdots, s, \tag{5.36}$$

$$M_i \in \mathrm{INV}. \tag{5.37}$$

The last condition 5.37 ensures that the POVM elements are G-invariant. We can restate the problem in terms of the images of the mapping $\mathcal{C}_g$ for some $g \in G$. In that case, the problem becomes that of discriminating with certainty the states in the set $\tilde{\mathcal{S}} = \{\mathcal{C}_g(\rho_1), \cdots, \mathcal{C}_g(\rho_s)\}$ by performing a POVM of the form of Eq. (4.6) in Section 4.1.1. As every $\mathcal{C}_g$ is a LOCC-simulating isometry, the POVM performed on the image states of the isometry is comprised of LOCC measurements.

Hayashi *et al.* have studied the problem of state discrimination where the POVM are LOCC [39,40]. In other words, they consider $\left\{\tilde{M}_i\right\}$ that satisfies the following alternative conditions instead:

$$\sum_i \tilde{M}_i = I, \tag{5.38}$$

$$0 \leq \tilde{M}_i \leq I, \tag{5.39}$$

$$\mathrm{Tr}\left(\tilde{M}_i\, \rho_i\right) = 1, \;\; i = 1, \cdots, s, \tag{5.40}$$

$$\tilde{M}_i \in \mathrm{SEP}. \tag{5.41}$$

(Condition 5.41 is a necessary condition for POVM elements that are LOCC [84].). They were able to give upper bounds on the size of the set $\tilde{\mathcal{S}}$ in terms of the averages of well known distance-based measures of entanglement:

$$N \leq D/\overline{r_E\left(\mathcal{C}_g(\rho_i)\right)} \leq D/\overline{2^{E_{\mathrm{R}}(\mathcal{C}_g(\rho_i))+S(\rho_i)}} \leq D/\overline{2^{G(\mathcal{C}_g(\rho_i))}}, \tag{5.42}$$

where we denote the average of a set of quantities $\{x_i\}$ by $\bar{x}_i := 1/N \sum_i x_i$, N is the total number of states in the set $\mathcal{S}$, and where $G(\rho)$ is the geometric entanglement (2.70), $E_R(\rho)$ is the relative entropy of entanglement (2.71), $S(\rho)$ is the von Neumann entropy and $r_E(\rho)$ is the global robustness of entanglement (2.73) (also note that $S(\rho_i) = S\left(\mathcal{C}_g(\rho_i)\right)$ because of the simple form of the mapping $\mathcal{C}_g$.). This is the main result of Hayashi *al.* reported in [39].

We can presently rewrite the inequalities in (5.42) in terms of functions of the initial states ρ_i instead of the image states $\mathcal{C}_g(\rho_i)$. Thus we get the bounds

$$N \leq D/\overline{r_A^s(\rho_i)} \leq D/\overline{2^{A_{\mathrm{R}}^s(\rho_i)+S(\rho_i)}} \leq D/\overline{2^{G_A^s(\rho_i)}}, \tag{5.43}$$

equivalent to the bounds derived by Hayashi *et al.*, but now for the case of state discrimination by G-invariant measurements. We already defined the relative entropy of asymmetry (REA) as $A_R^s(\rho) = E_R(\mathcal{C}_s(\rho))$ in (5.14). Based on our method of constructing asymmetry monotones through the isometry $\mathcal{C}_s$, we define the other two entanglement monotones in a similar way:

Definition 36. *The global robustness of asymmetry is defined in terms of the global robustness of entanglement, r_E, as* $r_A^s(\rho) : \mathscr{H} \to \mathbb{R}^+ : \rho \mapsto r_E(\mathcal{C}_s(\rho))$.

Definition 37. *The geometric asymmetry is defined in terms of the geometric entanglement G as* $G_A^s(\rho) : \mathscr{H} \to \mathbb{R}^+ : \rho \mapsto G(\mathcal{C}_s(\rho))$.

Note that the geometric entanglement is a monotone only when applied to pure states. Similarly, as the isometry $\mathcal{C}_s$ maps only pure states to bipartite pure states, the geometric asymmetry is likewise a pure-state asymmetry monotone. Thus, in cases where all the states ρ_i in $\mathcal{S}$ are pure states, the above bounds are all in terms of asymmetry monotones. As we saw, this result is the direct analogue of the case of LOCC-state discrimination studied in [39, 40].

Chapter 6

Other entanglement-based selection rules and conservation laws

In this section, we consider a different kind of isometry that is used often in symmetry and reference-frames related work [8]. For example, the optimal input states in quantum estimation strategy for the action of a symmetry group are shown to be coherent superpositions of maximally entangled states, where the entanglement is between the irrep-carrying subspaces and the multiplicity subspaces [19].

The isometry that maps to a tensor-product structure between irrep-carrying and multiplicity spaces is quite natural to consider, but as we will see, in general, it is not a LOCC-simulating isometry. Nevertheless, we will show that it still leads to new and independent necessary conditions for the manipulation of asymmetric states.

We start by considering the Hilbert space decomposition of Eq. (2.37). Irreps carrying subspaces $\mathscr{H}_{\boldsymbol{j},\lambda}$ for fixed $\boldsymbol{j}$ are equivalent. Their direct sum

$$\mathscr{H}_{\boldsymbol{j}} := \bigoplus_{\lambda} \mathscr{H}_{\boldsymbol{j},\lambda} \tag{6.1}$$

is isomorphic to $\mathscr{H}_{\boldsymbol{j}} \cong \mathscr{M}_{\boldsymbol{j}} \otimes \mathscr{N}_{\boldsymbol{j}}$, where $\mathscr{M}_{\boldsymbol{j}}$ carries the irrep labelled by $\boldsymbol{j}$, and $\mathscr{N}_{\boldsymbol{j}}$ is the so called multiplicity space carrying the trivial representation of the group [8]. It follows that $\mathscr{H} \cong \mathscr{W}_{\mathcal{L}}$, where

$$\mathscr{W}_{\mathcal{L}} := \bigoplus_{\boldsymbol{j}} \mathscr{M}_{\boldsymbol{j}} \otimes \mathscr{N}_{\boldsymbol{j}}. \tag{6.2}$$

In [8] the isomorphism of $\mathscr{H}$ and $\mathscr{W}_{\mathcal{L}}$ was assumed implicitly, but now we explicitly introduce the isometry connecting them.

Definition 38. *Let* $\{|\boldsymbol{j},\boldsymbol{m}\rangle\}_{\boldsymbol{m}}$ *and* $\{|\boldsymbol{j},\lambda\rangle\}_{\lambda}$ *be basis states spanning the spaces* $\mathscr{M}_{\boldsymbol{j}}$

and $\mathscr{N}_{\boldsymbol{j}}$, respectively. We define $\mathcal{L} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{W}_{\mathcal{L}})$ as the isometry that maps

$$|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \mapsto^{\mathcal{L}} |\boldsymbol{j}, \boldsymbol{m}\rangle \otimes |\boldsymbol{j}, \lambda\rangle. \tag{6.3}$$

Note that $\mathscr{W}_{\mathcal{L}} \subset \mathscr{M} \otimes \mathscr{N}$, where $\mathscr{M} := \bigoplus_{\boldsymbol{j}} \mathscr{M}_{\boldsymbol{j}}$ and $\mathscr{N} := \bigoplus_{\boldsymbol{j}} \mathscr{N}_{\boldsymbol{j}}$. Therefore, states in the image of $\mathcal{L}$ (*i.e.* states in $\mathscr{W}_{\mathcal{L}}$) can be viewed as bipartite states. Moreover, if ρ is a G-invariant state, then from Eq. (3.8) it follows that

$$\mathcal{L}(\rho) = \sum_{\boldsymbol{j},\lambda} p_{\boldsymbol{j},\lambda} \left(\sum_{\boldsymbol{m}} |\boldsymbol{j}, \boldsymbol{m}\rangle\langle \boldsymbol{j}, \boldsymbol{m}| \right) \otimes |\boldsymbol{j}, \lambda\rangle\langle \boldsymbol{j}, \lambda|, \tag{6.4}$$

which is a separable state (see also [8]). Similarly, any coherent superposition of states with different values of $\boldsymbol{j}$

$$|\phi\rangle = \sum_{\boldsymbol{j},\boldsymbol{m},\lambda} c_{\boldsymbol{j},\lambda,\boldsymbol{m}} |\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle, \tag{6.5}$$

is mapped to the entangled state

$$|\tilde{\phi}\rangle = \sum_{\boldsymbol{j},\boldsymbol{m},\lambda} c_{\boldsymbol{j},\lambda,\boldsymbol{m}} \, |\boldsymbol{j}, \boldsymbol{m}\rangle \otimes |\boldsymbol{j}, \lambda\rangle. \tag{6.6}$$

Thus, $\mathcal{L}$ satisfies conditions (2) and (3) in Definition 28 of a LOCC-simulating isometry. However, $\mathcal{L}$ is not a LOCC-simulating isometry since it does not in general satisfy condition (1) of Definition 28, as we show now for the group $G = SU(2)$.

6.1 $\mathcal{L}$ is not a LOCC-simulating isometry

We now show that the entanglement of the bipartite states in the image of the isometry $\mathcal{L}$ can in fact be increased by covariant transformations. Consider the 1/2-spin state $\Psi = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |1/2; 1/2\rangle$ in the standard form. Note that $\mathcal{L}(\Psi)$ is a product state. Using Eq. (2.46), we show that the map $\mathcal{E}_{1/2}$ takes Ψ to a state whose image is entangled. We only deal with fixed α in (2.46), so we can remove it from our notation as well. We consider the operator sum representation of the irreducible SU(2)-covariant map $\mathcal{E}_{1/2}$

consisting of two Kraus operators $K_{1/2,1/2}$, and $K_{1/2,-1/2}$. Because of the freedom in the choice of $SU(2)$-covariant Kraus operators, we can choose them such that they act on $|\psi\rangle$ up to a normalization factor as

$$\begin{aligned} K_{1/2,1/2}|\psi\rangle &\propto |1;1\rangle \xrightarrow{\mathcal{L}} |1;1\rangle \otimes |1\rangle, \\ K_{1/2,-1/2}|\psi\rangle &\propto |1;0\rangle + |0;0\rangle \xrightarrow{\mathcal{L}} |1;0\rangle \otimes |1\rangle + |0;0\rangle \otimes |0\rangle. \end{aligned} \tag{6.7}$$

The state $\mathcal{L}\left(\mathcal{E}_{1/2}(\Psi)\right)$ is an equal mixture of the two states in the r. h. s. of Eq. (6.7) and is thus an entangled state. It follows that the transformation

$$\mathcal{L}(\Psi) \mapsto \mathcal{L}\left(\mathcal{E}_{1/2}(\Psi)\right) \tag{6.8}$$

cannot be accomplished by LOCC.

6.2 Necessary conditions for the manipulation of asymmetric states

Our motivation for introducing the isometries between the original and the Kronecker product Hilbert spaces is to learn about G-covariant transformations. In particular, we study how the entanglement of the image states changes. In order to better understand how the entanglement changes under the isometry $\mathcal{L}$, we now focus on the form of the maps that act on the image states and that mimic G-covariant transformations. The Wigner-Eckart theorem implies that, up to a projection to the subspace $\mathscr{W}_{\mathcal{L}} \subset \mathscr{M} \otimes \mathscr{N}$ of Eq. (6.2), those maps are separable maps, *i.e.* of the form

$$\tilde{\mathcal{E}}_{\text{sep}}(\bullet) = \sum_x \tilde{V}_x \otimes \tilde{K}_x(\bullet)\tilde{V}_x^\dagger \otimes \tilde{K}_x^\dagger. \tag{6.9}$$

To see this, let $\Pi_{\mathscr{W}_{\mathcal{L}}}$ denote the projection to the $\mathscr{W}_{\mathcal{L}}$-space. Every G-covariant transformation can be constructed from a set of irreducible tensor operators $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$. So we need only consider how $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ are mimicked in the $\mathscr{W}_{\mathcal{L}}$-space. If ρ is mapped to σ by $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ (σ is in general subnormalized), then $\mathcal{L}(\rho)$ is mapped to $\mathcal{L}(\sigma)$ by the operator

$$\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha} := \tilde{V}_{\boldsymbol{J},\boldsymbol{M}} \otimes \tilde{K}_{\boldsymbol{J},\alpha}, \tag{6.10}$$

followed by $\Pi_{\mathscr{W}_\mathcal{L}}$. The matrix elements of $\tilde{V}_{\boldsymbol{J},\boldsymbol{M}}$ and $\tilde{K}_{\boldsymbol{J},\alpha}$ are, following the Wigner-Eckart theorem, equal to the CG coefficient and the reduced matrix respectively,

$$\langle \boldsymbol{j}_2, \boldsymbol{m}_2 | \tilde{V}_{\boldsymbol{J}\boldsymbol{M}} | \boldsymbol{j}_1, \boldsymbol{m}_1 \rangle = \left(\begin{array}{cc|c} \boldsymbol{j}_1 & \boldsymbol{J} & \boldsymbol{j}_2 \\ \boldsymbol{m}_1 & \boldsymbol{M} & \boldsymbol{m}_2 \end{array} \right), \tag{6.11}$$

$$\langle \boldsymbol{j}_2, \lambda_2 | \tilde{K}_{\boldsymbol{J},\alpha} | \boldsymbol{j}_1, \lambda_1 \rangle = \langle \boldsymbol{j}_2, \lambda_2 \, \| \, K_{\boldsymbol{J},\alpha} \, \| \, \boldsymbol{j}_1, \lambda_1 \rangle. \tag{6.12}$$

Again, here we consider only simply-reducible groups. For the generalization of the results of this section to all semi-simple compact Lie groups see Appendix A.

To see why the projection $\Pi_{\mathscr{W}_\mathcal{L}}$ must follow the tensor product of Eq. (6.10) consider two states ρ and σ such that $\rho \mapsto^{\mathcal{E}} \sigma$, where $\mathcal{E}$ is a G-covariant transformation. The support of the states $\mathcal{L}(\rho)$ and $\mathcal{L}(\sigma)$ is spanned by the states of the form $|\boldsymbol{j}, \boldsymbol{m}\rangle \otimes |\boldsymbol{j}, \boldsymbol{\lambda}\rangle$, where the irrep label $\boldsymbol{j}$ is always the *same* in both kets in the tensor product. Suppose that $K_{\boldsymbol{J},\boldsymbol{M},\lambda}$ is one of the Kraus operators of $\mathcal{E}$, which means that $\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha}$ (6.10) is one of the Kraus operators of the corresponding map $\tilde{\mathcal{E}}_{\text{sep}}$ (6.9). Suppose also that the Clebsch-Gordan coefficients in (6.11) is non-zero for both triplets $(\boldsymbol{j}, \boldsymbol{J}, \boldsymbol{j}_1)$ and $(\boldsymbol{j}, \boldsymbol{J}, \boldsymbol{j}_2)$, where $\boldsymbol{j}_1 \neq \boldsymbol{j}_2$. In other words, $\boldsymbol{J}$ 'couples' $\boldsymbol{j}$ to both $\boldsymbol{j}_1$ and $\boldsymbol{j}_2$. It now follows that the state $\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha} \, \mathcal{L}(\rho) \, \tilde{K}^\dagger_{\boldsymbol{J},\boldsymbol{M},\alpha}$ has support containing states of the form $|\boldsymbol{j_1}, \boldsymbol{m}\rangle \otimes |\boldsymbol{j_2}, \boldsymbol{\lambda}\rangle$ and $|\boldsymbol{j_2}, \boldsymbol{m}\rangle \otimes |\boldsymbol{j_1}, \boldsymbol{\lambda}\rangle$, *ie.* tensor-product of two states with *different* irrep labels. However such states are outside the image space of the mapping $\mathcal{L}$ and therefore, the state

$$\tilde{\sigma}' := \tilde{\mathcal{E}}_{\text{sep}} \left(\mathcal{L}(\rho) \right) \tag{6.13}$$

is not equal to the image state $\mathcal{L}(\sigma)$:

$$\tilde{\sigma}' \neq \mathcal{L}(\sigma). \tag{6.14}$$

In order to retrieve $\mathcal{L}(\sigma)$ we must project the state $\tilde{\sigma}'$ back to the image space $\mathscr{W}_\mathcal{L}$.

The entanglement of the image states can be increased only because of the projection $\Pi_{\mathscr{W}_{\mathcal{L}}}$ in Eq. (6.10). We can express the projection as $\Pi_{\mathscr{W}_{\mathcal{L}}} = \sum_{\boldsymbol{j}} \Pi_{\boldsymbol{j}}$, where

$$\begin{aligned} \Pi_{\boldsymbol{j}} =& \Pi_{\mathscr{M}_{\boldsymbol{j}}} \otimes \Pi_{\mathscr{N}_{\boldsymbol{j}}} \\ :=& \sum_{\boldsymbol{m}} |\boldsymbol{j},\boldsymbol{m}\rangle\langle \boldsymbol{j},\boldsymbol{m}| \otimes \sum_{\lambda} |\boldsymbol{j},\lambda\rangle\langle \boldsymbol{j},\lambda|. \end{aligned} \tag{6.15}$$

Responsible for creating or increasing the entanglement are the cross terms $\Pi_{\boldsymbol{j}}$ and $\Pi_{\boldsymbol{j}'}$ acting on both sides of $\mathcal{L}(\rho)$ as it is mapped to

$$\mathcal{L}(\rho) \mapsto \Pi_{\mathscr{W}_{\mathcal{L}}} \tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha} \mathcal{L}(\rho)\ \tilde{K}^{\dagger}_{\boldsymbol{J},\boldsymbol{M},\alpha} \Pi_{\mathscr{W}_{\mathcal{L}}}. \tag{6.16}$$

In order to get rid of the cross terms, we proceed as follows: Suppose for a given G-covariant CP-transformation $\mathcal{E}$, mapping ρ to the state σ, the corresponding map on the bipartite state is

$$\mathcal{L}(\sigma) = \tilde{\mathcal{E}}\left[\mathcal{L}(\rho)\right] = \Pi_{\mathscr{W}_{\mathcal{L}}} \left(\tilde{\mathcal{E}}_{\text{sep}}\left[\mathcal{L}(\rho)\right]\right) \Pi_{\mathscr{W}_{\mathcal{L}}}, \tag{6.17}$$

where $\tilde{\mathcal{E}}_{\text{sep}}$ has an operator sum representation in terms of Kraus operators defined in Eq. (6.10). If instead we consider the convex sum of transformations,

$$\begin{aligned} \mathcal{L}(\rho) \mapsto \bar{\sigma} :=& \sum_{\boldsymbol{j}} \Pi_{\boldsymbol{j}} \mathcal{L}(\sigma) \Pi_{\boldsymbol{j}} \\ =& \sum_{\boldsymbol{j}} \Pi_{\boldsymbol{j}} \tilde{\mathcal{E}}\left[\mathcal{L}(\rho)\right] \Pi_{\boldsymbol{j}} \\ =& \sum_{\boldsymbol{j}} \Pi_{\boldsymbol{j}} \left(\tilde{\mathcal{E}}_{\text{sep}}\left[\mathcal{L}(\rho)\right]\right) \Pi_{\boldsymbol{j}}, \end{aligned} \tag{6.18}$$

then the overall map remains a separable one. Note that the $\Pi_{\boldsymbol{j}}$ are themselves separable. In fact, the transformation in (6.18) can be implemented by LOCC. The reason is this: the superoperator $\tilde{\mathcal{E}}_{\text{sep}}$ is comprised of operators $\tilde{V}_{\boldsymbol{J},\boldsymbol{M}} \otimes \tilde{K}_{\boldsymbol{J},\alpha}$. The projections $\Pi_{\mathscr{M}_{\boldsymbol{j}}} \tilde{V}_{\boldsymbol{J},\boldsymbol{M}}$ are unitary operators acting on the irrep-subspace $\mathscr{M}_{\boldsymbol{j}}$, as their matrix elements are simply the CG-coefficients corresponding to a change of basis in $\mathscr{M}_{\boldsymbol{j}}$. Thus, the whole transformation can be implemented by a series of local measurements by Alice, corresponding to operators $\Pi_{\mathscr{N}_{\boldsymbol{j}}}\tilde{K}_{\boldsymbol{J},\alpha}$, followed by the unitaries $\Pi_{\mathscr{M}_{\boldsymbol{j}}}\tilde{V}_{\boldsymbol{J},\boldsymbol{M}}$ performed by Bob.

It follows that the average entanglement of the state $\tilde{\sigma}$ cannot exceed the entanglement of the initial state $\mathcal{L}(\rho)$. We state the result in the following proposition.

Proposition 32. *Let E be an ensemble entanglement monotone. We further assume that E is faithful and convex. The G-covariant transformation $\rho \mapsto \sigma$ is possible only if the following condition holds:*

$$E\left(\mathcal{L}(\rho)\right) \geq E(\bar{\sigma}), \tag{6.19}$$

where $\bar{\sigma}$ is defined in Eq. (6.18).

Proof. The proposition is an immediate consequence of the fact that (6.18) is LOCC. □

Can we restate the condition of Eq. (6.19) in terms of new asymmetry monotones? Let us define the average initial state as,

$$\bar{\rho} := \sum_{\boldsymbol{j}} \Pi_{\boldsymbol{j}}\mathcal{L}(\rho)\,\Pi_{\boldsymbol{j}}. \tag{6.20}$$

Clearly, the entanglement $E(\mathcal{L}(\rho)) \geq E\left(\bar{\rho}\right)$. But does $E\left(\bar{\rho}\right)$ exceed $E\left(\bar{\sigma}\right)$ as well? If this were true, then we could still define an ensemble asymmetry monotone as $A_E^{\text{ave}}(\rho) := E\left(\bar{\rho}\right)$. However, that is not the case. Consider the group $G = SU(2)$, and let $\rho = |\phi\rangle\langle\phi|$, where,

$$|\phi\rangle := \frac{1}{\sqrt{2}}|3/2; 1/2\rangle + \frac{1}{\sqrt{2}}|1/2; 1/2\rangle.$$

The image state, $\mathcal{L}(\rho) = |\tilde{\phi}\rangle\langle\tilde{\phi}|$, where

$$|\tilde{\phi}\rangle := \frac{1}{\sqrt{2}}|3/2; 1/2\rangle \otimes |3/2\rangle + \frac{1}{\sqrt{2}}|1/2; 1/2\rangle \otimes |1/2\rangle$$

is an entangled state.

Also consider the irreducible $SU(2)$-covariant CP-map $\mathcal{E}_{1/2}$. The state $\bar{\rho}$ is a separable state, whereas the state $\bar{\sigma}$ of Eq. (6.18) is entangled. In other words,

$$E(\bar{\sigma}) \nleq E(\bar{\rho}) = 0.$$

Note that, in accordance with Proposition 32, it is still true that $0 < E(\bar{\sigma}) \leq E(\mathcal{L}(\rho))$.

In summary, proposition 32 provides a necessary condition that all G-covariant transformations must satisfy. Let us call such a necessary condition a *general selection rule*. What we have shown is that the general selection rule in proposition 32 is not expressible in terms of asymmetry monotones of the initial and final states, even though it is expressible in terms of the entanglement of their image states. This is an example of how asymmetry monotones are not the only relevant quantities in the study of the consequences of symmetries.

6.3 Conserved quantities

If we further restrict ourselves to *reversible* G-covariant transformations, still more interesting results can be deduced from the $\mathcal{L}$-isometry. Unitary operations have only one Kraus operator. If G is non-Abelian, G-covariant unitaries exist only among G-covariant transformations labeled by the identity representation, $\boldsymbol{J} = 0$, denoted by $\mathcal{E}_{0,\alpha} = \mathcal{K}_{0,0,\alpha}$ (We consider the case of Abelian groups in Appendix B.).

The unitary $\mathcal{K}_{0,0,\alpha}$ maps each subspace $\mathcal{H}_{\boldsymbol{j}}$ in (6.1) to itself, and the corresponding bipartite operator $\tilde{K}_{0,0,\alpha}$ has the form

$$\tilde{K}_{0,0,\alpha} = \left(\sum_{\boldsymbol{j}} \Pi_{\mathscr{M}_{\boldsymbol{j}}} \right) \otimes \tilde{K}_{0,\alpha}. \tag{6.21}$$

The above form is a direct consequence of the CG-coefficients in Eq. (6.11) for the case where $\boldsymbol{J} = \boldsymbol{M} = 0$.

Substituting for $\mathcal{E}_{1/2}$ in Eq. (6.17) shows that in this case the overall projection $\Pi_{\mathscr{W}_\mathcal{L}}$ into the subspace $\mathscr{W}_\mathcal{L}$ can be dropped, because $\tilde{K}_{0,0,\alpha}$ maps $\mathscr{W}_\mathcal{L}$ to itself. Equivalently, $\Pi_{\mathscr{W}_\mathcal{L}}\Pi_{\boldsymbol{j}} = \Pi_{\boldsymbol{j}}$, so that,

$$\Pi_{\mathscr{W}_\mathcal{L}}\tilde{K}_{0,0,\alpha} = \tilde{K}_{0,0,\alpha}.$$

The operator $\tilde{K}_{0,0,\alpha}$ is of course a local unitary. It thus follows that for every reversible G-covariant transformation $\mathcal{E}$, the entanglement of the image state in Eq. (6.17) remains constant. In other words, we have identified a conserved quantity.

Proposition 33. *For reversible G-covariant transformations, $\mathcal{E}_{0,\alpha}$, the function,*

$$L(\rho) := E\left(\mathcal{L}(\rho)\right), \tag{6.22}$$

is a conserved quantity.

As a simple example, we consider the group $SU(2)$, and a system of three half-integer spin systems. From the addition of angular momenta we know that the Hilbert space of the three systems can be decomposed as

$$\mathscr{H} = \mathscr{H}_{1/2} \oplus \mathscr{H}_{1/2} \oplus \mathscr{H}_{3/2}, \tag{6.23}$$

where $\mathscr{H}_{1/2}$ and $\mathscr{H}_{3/2}$ are Hilbert spaces of systems of half-integer and three-half integer spins, respectively. The space $\mathscr{H}_{1/2}$ comes with multiplicity two and $\mathscr{H}_{3/2}$ comes with multiplicity one. Consider for example the pure state

$$|\psi\rangle = \sqrt{p_1}|1/2, 1; 1/2\rangle + \sqrt{p_2}|1/2, 2; 1/2\rangle + \sqrt{p_3}|1/2, 2; -1/2\rangle + \sqrt{p_4}|3/2, 1; 1/2\rangle. \tag{6.24}$$

Let us denote the state in vector notation in the basis $\{|j, \lambda; m\rangle\}$ for $j = 1/2; \lambda = 1, 2; m = \pm 1/2$ and $j = 3/2; \lambda = 1; m = \pm 3/2, \pm 1/2$, respectively, as

$$|\psi\rangle \leftrightarrow \left[\sqrt{p_1}, \sqrt{p_2}, 0, \sqrt{p_3}, 0, \sqrt{p_4}, 0, 0\right]^\top. \tag{6.25}$$

Now suppose $|\psi\rangle$ transforms under, for example, the $SU(2)$-invariant unitary

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \cos\theta_1 & -e^{\imath\phi_1}\sin\theta_1 \\ e^{-\imath\phi_1}\sin\theta_1 & \cos\theta_1 \end{pmatrix} \bigoplus \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes \left(e^{\imath\phi_2}\right) \quad (6.26)$$

to the state

$$\begin{aligned} |\phi\rangle =& \sqrt{p_1}(\cos\theta_1 + e^{-\imath\phi_1}\sin\theta_1)|1/2,1;1/2\rangle + \sqrt{p_2}(\cos\theta_1 - e^{\imath\phi_1}\sin\theta_1)|1/2,2;1/2\rangle + \\ & \sqrt{p_3}(\cos\theta_1 - e^{\imath\phi_1}\sin\theta_1)|1/2,2;-1/2\rangle + \sqrt{p_4}e^{\imath\phi_2}|3/2,1;1/2\rangle. \end{aligned} \quad (6.27)$$

The corresponding image states under the mapping $\mathcal{L}$ are

$$\begin{aligned} |\tilde{\psi}\rangle =& \sqrt{p_1}|1/2,1/2\rangle|1/2,1\rangle + \sqrt{p_2}|1/2,1/2\rangle|1/2,2\rangle + \sqrt{p_3}|1/2,-1/2\rangle|1/2,2\rangle + \\ & \sqrt{p_4}|3/2,1/2\rangle|3/2,1\rangle, \end{aligned} \quad (6.28)$$

and

$$\begin{aligned} |\tilde{\phi}\rangle =& \sqrt{p_1}(\cos\theta_1 + e^{-\imath\phi_1}\sin\theta_1)|1/2,1/2\rangle|1/2,1\rangle + \sqrt{p_2}(\cos\theta_1 - e^{\imath\phi_1}\sin\theta_1)|1/2,1/2\rangle|1/2,2\rangle + \\ & \sqrt{p_3}(\cos\theta_1 - e^{\imath\phi_1}\sin\theta_1)|1/2,-1/2\rangle|1/2,2\rangle + \sqrt{p_4}e^{\imath\phi_2}|3/2,1/2\rangle|3/2,1\rangle, \end{aligned} \quad (6.29)$$

respectively, and the local unitary $\tilde{U}$ whose matrix form in the corresponding basis states $\{|j,m\rangle \otimes |j,\lambda\rangle\}$ is

$$\tilde{U} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \bigotimes \begin{pmatrix} \cos\theta_1 & -e^{\imath\phi_1}\sin\theta_1 & 0 \\ e^{-\imath\phi_1}\sin\theta_1 & \cos\theta_1 & 0 \\ 0 & 0 & e^{\imath\phi_2} \end{pmatrix} \quad (6.30)$$

maps $|\tilde{\psi}\rangle$ to $|\tilde{\phi}\rangle$. Moreover the Schmidt coefficients of both states are $\{p_1 + p_2, p_3, p_4\}$, which means that all bipartite-entanglement measures for the two states $|\tilde{\psi}\rangle$ and $|\tilde{\phi}\rangle$ are equal, as the bipartite entanglement of a pure state is a function of its Schmidt numbers only. For example, the entropy of entanglement of both states is equal to the Shannon entropy $H(\{p_1 + p_2, p_3, p_4\})$, where the Shannon entropy of a probability distribution $\{p_i\}$ is equal to $H(\{p_i\}) = \sum_i p_i \log_2 p_i$.

Thus, we derive new conservation laws for closed systems. The new conservation laws are not of the form of the expectation value of a generator of a Hamiltonian symmetry, but are instead in terms of entanglement monotones. In the case of open systems and irreversible transformations, the conservation law is replaced with a general selection rule, again in terms of entanglement monotones.

Chapter 7

Concluding Remarks

7.1 Summary of results

We showed that G-covariant transformations for a semi-simple compact Lie group can be simulated by LOCC transformations on bipartite states. Our method involves first mapping the Hilbert space of the system to a subset of a larger Hilbert space comprised of a tensor product of two Hilbert spaces. The respective class of isometries maps G-invariant states to separable states, and at least some non-G-invariant resource states to entangled states. Furthermore, the image, under the isometry, of two states that are mapped one to the other by a G-covariant transformation are related by a LOCC transformation. We termed such an isometry a LOCC-simulating isometry. Thus, the entanglement of the image states does not increase as the states transform under G-covariant transformations. The entanglement can thus be used to quantify the asymmetry of the original states.

Every entanglement monotone can be adapted to define an asymmetry monotone through the isometry. Moreover, the monotonicity condition provides new selection rules that can help specify whether a G-covariant transformation between any given two states exists. In the special case of reversible G-covariant transformations, the monotones remain constant and thus introduce new conserved quantities, in addition to well known conserved quantities that follow from the quantum analogues of Noether's theorem. In other words, we have shown that every entanglement monotone leads to a conservation law under reversible transformations of closed systems. Moreover, some entanglement monotones like the negativity are easily calculable for all states.

In addition, we introduced a different isometry that, although not a LOCC-simulating isometry, still captures some aspects of the asymmetry that are related to bipartite entanglement. New selection rules that are not given in terms of asymmetry monotones can, nevertheless, be expressed in terms of the entanglement of the image states.

7.2 Discussion

The present thesis contains two major innovations. First, the notion of using local operations to simulate symmetric dynamics. Second, the idea of applying the well known and well-studied resource theory of entanglement to a totally different resource theory. We discuss the significance of these innovations in this section, as well as the impact they have on the field of symmetry and, more generally, on quantum information theory.

Symmetric time evolutions described by covariant transformations are based on group structures, invariant subspaces and representation theory. It is not evident, at first, that such structures have any connections to local operations and tensor products of two or more systems. However, the link exists, and once found, is actually very simple. The exact form that G-covariant transformations take can be very complicated, depending on the specific, idiosyncratic features of each particular group, or the particular features of the representation of the group that is carried by the states of the system. Yet, the effect of an irreducible covariant operator on a ket labeled by the weight $\boldsymbol{m}$ of the algebra, $|\boldsymbol{m}\rangle$ (ignoring the other labels), is a simple translation by some fixed amount $\boldsymbol{M}$, $|\boldsymbol{m}\rangle \rightarrow |\boldsymbol{m}+\boldsymbol{M}\rangle$. Its significance lies in the fact that *all* semi-simple Lie groups act this way. It is what they all have in common.

Thus, the local operators that simulate the G-covariant transformations exploit a common feature of semi-simple compact Lie groups, namely, how the weights are transformed. All the idiosyncratic features of specific groups are left out in our approach.

In this lies the strength of the method, as it applies equally to all semi-simple compact Lie groups and links them all to a sub-class of local operations. In turn, this enables entanglement theory, as the resource theory arising from the restriction to LOCC, to be applied to the study of covariant transformations irrespective of the symmetry group involved.

The significance of the connection lies in the strength and richness of entanglement theory. Entanglement has been the focus of intense study and plays a central role in quantum information theory. This fact is reflected in the abundance of well investigated entanglement measures and monotones, each of which can now be used to extract information about the asymmetry of quantum states. An important consequence is the realization that, for closed systems, entanglement serves as a conserved quantity or a constant of motion.

Although we approach entanglement as a resource theory of the interconversion of states under the restriction of operations to LOCC, entanglement is ultimately a type of correlation between two systems. It becomes a resource when the systems are separated from each other so that operations have to be, by necessity, local. The asymmetry as a resource is primarily due to lack of information. This is specially evident when viewed in the context of lack of shared reference frames. The restriction to covariant transformations comes about because information about the alignment of the reference frame is not known. If the knowledge is somehow attained, the restriction is lifted. Not so in the case of entanglement and local operators. Separation between two systems is a physical restriction independent of our state of knowledge. It is interesting that the results of the present thesis implies that the information-dependent resource theory of asymmetry can be encoded in the correlations of two physically separated systems.

Of course, the process of gaining the alignment information can be modelled physically too. Recall first that once the reference frame is included as a dynamical physical system to which one can assign a state, then the joint state of the system plus the reference frame must necessarily be represented as a twirled and therefore symmetric state (for a more detailed discussion see Section 1.4). Lack of information about the reference frame alignment corresponds to tracing out the reference frame system that results in invariant reduced density operators and an effective superselection rule. Gaining information about the reference frame, on the other hand, corresponds to coupling to the reference frame and performing a measurement on it to determine its state. As the target system and the reference frame are described by a joint (invariant) state, this process can be equivalently modelled by a joint measurement on the system plus the reference frame state that picks out a state of the reference frame and the state of the system corresponding to it from among the ensemble of states that appear in the twirling operation. As a result, the twirled state is replaced and updated to the state after the measurement, and the superselection rule restriction is lifted [8].

Naturally, the specific features of the covariant maps that are ignored and left out could still contain important information about the dynamic symmetry and can effect how the states alter through time. Most of that information is lost in the mapping to local operations by a single isometry, *i.e.* the $\mathcal{C}_g$ for a single $g \in G$. However, a state can be mapped by two or more different isometries to two or more different bipartite states. For example, as we saw in Definition 30 of Section 4.1.2, a state can be mapped to a product state by one choice of $\mathcal{C}_g$, and the same state can be mapped to an entangled state by a different choice of $\mathcal{C}_g$. The entanglement features of the different image states is in general dependent on the specific structure of the group. So, when all, or a sufficient number, of isometries are considered together, more specific details of the group structure and the dynamic consequences of those details would reflect in the ensuing entanglement of the image states. Different groups will lead to different conditions and restrictions.

More broadly, our results apply to quantum information theory in general. In the absence of shared frames of reference, G-covariant operations are the only feasible transformations. As quantum networks grow larger and the demands for distributed quantum computation becomes more ubiquitous, one can foresee situations where quantum networks are so large and their nodes so distant that different nodes in the network do not share alignment between their local reference frames. An example is a network involving satellites in orbit, constantly moving and changing their spatial alignments with respect to each other and to stationary stations on earth. In all such scenarios, the consequences of the resulting superselection rule on quantum information tasks must be taken into account. Asymmetry monotones help determine how states transform under G-covariant maps, and, therefore, also what information tasks one can perform in the absence of shared references in such networks.

Another situation in quantum information theory where resource theories of asymmetry can be applied are in noisy channels where the noise has a certain symmetry. Mathematically, the noise is represented by the action of a unitary operator, sampled randomly from a set of unitary operations that form a group. However, the model assumes that the same unitary operator acts on all the qubits in the system that pass through the channel. Physically, this condition corresponds to a common source of noise, like a phase shift or a common change of polarization induced on all the photons passing through an optical fiber due to the imperfections in the inner structure of the fiber.

Finally, the restriction to G-covariant operations has applications in quantum cryptography, quantum data hiding and secret sharing as well. Two or more parties who share private reference frames can lift the restriction, whereas other parties, including potential eavesdroppers, who do not have access to this resource, still remain bound by the superselection rule. Asymmetry monotones quantify the strength of such resources and therefore can help identify optimal protocols for tasks that involve private frames, or can be used to set bounds on what can be achieved. The short case study in Section 5.6

is just a simple example of such an application.

7.3 Open Questions and future Work

There are various directions one can go from here. First, we saw in Section 4.1.2 that due to the freedom in the choice of isometry $\mathcal{C}_g$ for different values of $g \in G$, different image states result, with different entanglement properties depending on the specific features of the symmetry group. On the other hand, in our method, we arrive at conditions for the transition between two states by investigating the conditions on how entangled states transform under LOCC. What can entanglement considerations tell us about the specifics of the G-covariant transformations that come from the detailed structure of G? For example, if we confine our attention to transition of pure states to pure states, then as mentioned in Section 2.3.5, the majorization of the Schmidt coefficients of the final state by the coefficients of the initial state is the necessary and sufficient condition for the transition to go through. If we apply the majorization condition to the images of the initial and final states for different isometries $\mathcal{C}_g$, would we retrieve the exact form of the corresponding G-covariant transformation?

It would also be interesting to compare and contrast the consequences of the method introduced here with an information theoretic approach based on the study of the generalized G-asymmetry monotones, where the twirling operation is performed with respect to an arbitrary probability distribution defined over the group [59]. In a sense, our approach and the approach based on the G-asymmetry are complementary. If the results of the general G-asymmetry monotones can be derived from the entanglement-based approach here, one important advantage of our method would be that only a finite number of isometries are sufficient to access the information about asymmetry that can be captured by entanglement.

A second line of study concerns the case of finite groups. It is already known that a version of the Wigner-Eckart theorem exists for finite groups, albeit of a much more complicated form [55]. If the form of the Wigner-Eckart theorem for finite groups can be utilized to construct similar LOCC-simulating isometries, then entanglement theory can be directly applied to finite groups as well.

Third, we did not study the case of many-copy transformations and asymptotic limits. Many questions of interest can be asked in this respect, including additivity of the measure and possible applications to the problem of distillation of asymmetry resources.

We can also look at the links between entanglement and asymmetry highlighted in our work from the opposite direction: What do asymmetry measures and concepts tell us about entanglement of states? Asymmetry monotones, like the G-asymmetry or number variance, remain monotone functions of bipartite states under a restricted subsets of LOCC transformations, namely LOCC operations that are of the form of the isometry maps we introduced. For example, as we saw in Section 5.3.2, both the REA and G-asymmetry are distance measures, in terms of the relative entropy function, and change monotonically under those LOCC operations that have a Kraus decomposition of the form specified in Eq. (4.6). Yet they are not, in general, the same measure for a given state. Where does the difference come from? Similarly, we can ask what role do separable states that are not images of invariant states play in the theory of entanglement. Can they be understood as a separate kind of resource? It might even be the case that asymmetries of finite groups can be mapped to multipartite entangled states and not just bipartite ones. In that case, what we already know about the asymmetry of finite groups can shed light on, and perhaps help resolve, many open problems that still exist in multipartite entanglement theory.

Finally, a fifth direction for future research suggested by our result is to look for similar conditions in other resource theories. For example, the restriction to Gaussian operations results in a new resource theory where non-Gaussian states are resources [29]. Another example is thermodynamics. Already, connections between thermodynamics, viewed as a resource theory, and entanglement have been demonstrated [44,46,47]. Thermodynamics has been recognized as an energy preserving resource theory where transformations are restricted to operations that do not increase the total energy [46]. If the restricted set of operations in any of those resource theories can be simulated in a similar fashion by local operations, then it would be possible to employ entanglement theory to the study the resource theory.

Appendix A

The generalized Wigner-Eckart theorem

The main results of the thesis can be extended to the general case where the tensor product of the group's Lie algebra is not simply reducible. An algebra H is not simply reducible when the algebra has outer multiplicities, *i.e.* multiplicities arising due to the coupling of the irreps. We now consider the general form of the Wigner-Eckart theorem,

$$\langle \boldsymbol{j}', \lambda'; \boldsymbol{m}' | K_{\boldsymbol{J},\boldsymbol{M},\alpha} | \boldsymbol{j}, \lambda; \boldsymbol{m} \rangle = \sum_{\mu} \left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}', \mu \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array} \right) \langle \boldsymbol{j}', \lambda' \parallel K_{\boldsymbol{J},\alpha} \parallel \boldsymbol{j}, \lambda \rangle_{\mu}, \tag{A.1}$$

where μ is the outer multiplicity index for the irrep $[\boldsymbol{j}']$ due to the coupling,

$$[\boldsymbol{j}] \otimes [\boldsymbol{J}] \mapsto [\boldsymbol{j}'].$$

Here, we have used the symbol $[\boldsymbol{j}]$ to denote the representation labeled by $\boldsymbol{j}$, and similarly for other representations. The terms $\left(\begin{array}{cc|c} \boldsymbol{j} & \boldsymbol{J} & \boldsymbol{j}', \mu \\ \boldsymbol{m} & \boldsymbol{M} & \boldsymbol{m}' \end{array} \right)$ are the general Clebsch-Gordan coefficients, depending in general on the outer multiplicity μ in addition to the irrep and weight labels.

If the transformation $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ is unitary, still $\boldsymbol{J}$ and $\boldsymbol{M}$ must be the labels of the identity representation, $\boldsymbol{J} = \boldsymbol{M} = 0$. Coupling to the identity representation never results in outer multiplicities. Thus, the results for G-covariant unitaries in the paper is valid for the general case.

A.0.1 The Set of Isometries $\{\mathcal{C}_g\}$

All the Clebsch-Gordan coefficients are identically zero unless, as before, the weights labelling the bra and the ket, and the tensor operator satisfy the relation

$$\boldsymbol{m} + \boldsymbol{M} = \boldsymbol{m}'.$$

It follows that as far as the weights are concerned, the same translation operator as in Eq. (4.7) applies to all the terms in the r. h. s. of (A.1), and thus the same set of isometries $\mathcal{C}$ and $\mathcal{C}_g$ in the definitions 29 and 30 of Section 4.1 respectively, still satisfy all the conditions of a LOCC-simulating isometry in 28.

A.0.2 The Isometry $\mathcal{L}$

The situation is more complicated as far as the isometry $\mathcal{L}$ is concerned. The existence of outer multiplicities implies that we must define new Hilbert spaces to embed the Hilbert space, *i.e.* Hilbert spaces that include the outer multiplicities in the label of their basis states. Let

$$\mathscr{M} = \operatorname{span}\left\{|\boldsymbol{j}, \mu; \boldsymbol{m}\rangle\right\}_{\boldsymbol{j},\mu,\boldsymbol{m}},$$

be the space spanned by the basis states $|\boldsymbol{j}, \mu; \boldsymbol{m}\rangle$. Here, $\boldsymbol{j}$ and $\boldsymbol{m}$ are, as before, the irrep label and the weight label respectively. We have included an additional label μ, ranging over $\mu = 0, \ldots, \infty$, that we will later relate to the outer multiplicities, as we shall shortly see. Similarly, let

$$\mathscr{N} = \operatorname{span}\left\{|\boldsymbol{j}, \mu; \lambda\rangle\right\}_{\boldsymbol{j},\mu,\lambda},$$

where λ is the label for the (initial) irrep multiplicities. Also, let $\mathscr{M}_{\boldsymbol{j}} = \operatorname{span}\left\{|\boldsymbol{j}, 0; \boldsymbol{m}\rangle\right\}_{\boldsymbol{m}}$, and $\mathscr{N}_{\boldsymbol{j}} = \operatorname{span}\left\{|\boldsymbol{j}, 0; \lambda\rangle\right\}_{\lambda}$. Finally, let

$$\mathscr{W}_{\mathcal{L}} := \bigoplus_{\boldsymbol{j}} \mathscr{M}_{\boldsymbol{j}} \otimes \mathscr{N}_{\boldsymbol{j}}.$$

As before, we can define the isometry $\mathcal{L}$ by specifying how it acts on the basis states.

Definition 39. $\mathcal{L} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{W}_{\mathcal{L}})$ *is the isometry that maps,*

$$|\boldsymbol{j}, \lambda; \boldsymbol{m}\rangle \mapsto^{\mathcal{L}} |\boldsymbol{j}, 0; \boldsymbol{m}\rangle \otimes |\boldsymbol{j}, 0; \lambda\rangle. \tag{A.2}$$

Clearly, $\mathscr{W}_{\mathcal{L}} \subset \mathscr{M} \otimes \mathscr{N}$, and thus the states in the image of $\mathcal{L}$ (*i.e.* states in $\mathscr{W}_{\mathcal{L}}$) are bipartite states. Let $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ be an irreducible G-covariant operator. The operator acting on $\mathscr{M} \otimes \mathscr{N}$ that mimics $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$ can again be expressed as a separable state followed by a projection onto the image subspace $\mathscr{W}_{\mathcal{L}}$. Assume ρ is mapped to (a in general subnormalized) σ by $K_{\boldsymbol{J},\boldsymbol{M},\alpha}$. $\mathcal{L}(\rho)$ is then mapped to $\mathcal{L}(\sigma)$ by the operator

$$\tilde{K}_{\boldsymbol{J},\boldsymbol{M},\alpha} := \tilde{V}_{\boldsymbol{J},\boldsymbol{M}} \otimes \tilde{K}_{\boldsymbol{J},\alpha}, \tag{A.3}$$

followed by $\Pi_{\mathscr{W}_{\mathcal{L}}}$. The general form of the Wigner-Eckart theorem (A.1) implies

$$\begin{aligned} \langle \boldsymbol{j}_2, \mu_2; \boldsymbol{m}_2 | \, \tilde{V}_{\boldsymbol{J}\boldsymbol{M}} \, | \boldsymbol{j}_1, \mu_1; \boldsymbol{m}_1 \rangle &= \left(\begin{array}{cc|c} \boldsymbol{j}_1 & \boldsymbol{J} & \boldsymbol{j}_2, \mu_2 \\ \boldsymbol{m}_1 & \boldsymbol{M} & \boldsymbol{m}_2 \end{array} \right), \\ \langle \boldsymbol{j}_2, \mu_2; \lambda_2 | \, \tilde{K}_{\boldsymbol{J},\alpha} \, | \boldsymbol{j}_1, \mu_1; \lambda_1 \rangle &= \langle \boldsymbol{j}_2, \lambda_2 \parallel K_{\boldsymbol{J},\alpha} \parallel \boldsymbol{j}_1, \lambda_1 \rangle_{\mu_2}. \end{aligned} \tag{A.4}$$

Note that the r. h. s. does not depend on the value of μ_1 in either equation. The projection $\Pi_{\mathscr{W}_{\mathcal{L}}}$ is $\Pi_{\mathscr{W}_{\mathcal{L}}} = \sum_{\boldsymbol{j},\mu} \Pi_{\boldsymbol{j},\mu}$, where

$$\begin{aligned} \Pi_{\boldsymbol{j},\mu} :=& \Pi_{\mathscr{M}_{\boldsymbol{j}}} \otimes \Pi_{\mathscr{N}_{\boldsymbol{j}}} \\ :=& \sum_{\boldsymbol{m}} |\boldsymbol{j}, 0; \boldsymbol{m}\rangle\langle \boldsymbol{j}, \mu; \boldsymbol{m}| \otimes \sum_{\lambda} |\boldsymbol{j}, 0; \lambda\rangle\langle \boldsymbol{j}, \mu; \lambda|. \end{aligned} \tag{A.5}$$

for a given G-covariant CP-map $\mathcal{E}$ acting on ρ, the corresponding map on the bipartite state is

$$\tilde{\mathcal{E}}\left[\mathcal{L}(\rho)\right] = \Pi_{\mathscr{W}_{\mathcal{L}}} \left(\tilde{\mathcal{E}}_{\text{sep}}\left[\mathcal{L}(\rho)\right] \right) \Pi_{\mathscr{W}_{\mathcal{L}}}, \tag{A.6}$$

where $\tilde{\mathcal{E}}_{\text{sep}}$ has an operator sum representation in terms of Kraus operators defined in Eq. (6.10). The map $\tilde{\mathcal{E}}\left[\mathcal{L}(\rho)\right]$ is still not a LOCC-simulating CP-map. The cross terms $\Pi_{\boldsymbol{j}}, \mu$ and $\Pi_{\boldsymbol{j}',\mu'}$ acting on both sides of $\mathcal{L}(\rho)$ render the overall CP-map a non-separable one. However, here too, we can destroy the cross terms by applying a set of projections $\Pi_{\boldsymbol{j},\mu}$ separately on both sides and then taking the average of the maps as follows,

$$\begin{aligned} \mathcal{L}(\rho) \mapsto \bar{\sigma} &= \sum_{\boldsymbol{j},\mu} \Pi_{\boldsymbol{j},\mu} \, \tilde{\mathcal{E}}\left[\mathcal{L}(\rho)\right] \, \Pi_{\boldsymbol{j},\mu} \\ &= \sum_{\boldsymbol{j},\mu} \Pi_{\boldsymbol{j},\mu} \left(\tilde{\mathcal{E}}_{\text{sep}}\left[\mathcal{L}(\rho)\right] \right) \Pi_{\boldsymbol{j},\mu}. \end{aligned} \tag{A.7}$$

The overall map is separable now.

Not all symmetry groups in physics are simply-reducible. An important example is the group $SU(3)$ that plays a major role in high energy and particle physics. Here, we have demonstrated that our method of applying entanglement theory and using entanglement monotones and measures is general enough to cover such groups as well. We now have generalized the results of Chapter 4 beyond simply-reducible groups and to all semi-simple compact Lie groups.

Appendix B

Abelian Lie groups

The irreducible representations of Abelian groups are 1-dimensional. The irrep label is the highest weight. The 1-dimensional irreps have only one weight. Thus, the irrep label and the weight label are the same. We use the label n for the irreps of an Abelian group, and to conform to the notation of the rest of the thesis, we label the basis states as $|n,\lambda;n\rangle$. We presently show that the results of the thesis are greatly simplified in the case of Abelian groups. In particular, we show that the isometries $\mathcal{C}_g$ are all equivalent to each other, and are furthermore equivalent to the isometry $\mathcal{L}$.

Definition 40. *$\mathcal{C}:\mathcal{B}(\mathscr{H})\to\mathcal{B}(\mathscr{W}_{\mathcal{L}})$ is the isometry that maps*

$$|n,\lambda;n\rangle \mapsto^{\mathcal{C}} |n,\lambda;n\rangle\otimes|n\rangle. \tag{B.1}$$

Definition 41. *$\mathcal{L}:\mathcal{B}(\mathscr{H})\to\mathcal{B}(\mathscr{W}_{\mathcal{L}})$ is the isometry that maps*

$$|n,\lambda;n\rangle \mapsto^{\mathcal{L}} |n;n\rangle\otimes|n;\lambda\rangle. \tag{B.2}$$

First, note that the action of a group element on the basis kets is to merely add a phase,

$$U(g)|n,n,\lambda\rangle = e^{\imath\theta_{g,n}}|n,n,\lambda\rangle.$$

Thus, the definition 30 of $\mathcal{C}_g$ implies

$$\mathcal{C}_g=\mathcal{C},\ \ \forall g\in G. \tag{B.3}$$

The form of irreducible G-covariant transformations is also simplified to

$$\langle n',\lambda';n'|K_{N,N,\alpha}|n,\lambda;n\rangle = \delta_{n',n+N}\langle n',\lambda'\parallel K_{N,\alpha}\parallel n,\lambda\rangle, \tag{B.4}$$

or equivalently

$$K_{N,N,\alpha} = \sum_n c^{(N,\alpha)}_{n,\lambda,\lambda'} \, |n+N, \lambda'; n+N\rangle\langle n, \lambda; n|, \tag{B.5}$$

where $c^{(N,\alpha)}_{n,\lambda,\lambda'} = \langle n', \lambda' \parallel K_{N,\alpha} \parallel n, \lambda\rangle$.

Assume ρ is mapped to (a generally subnormalized) σ by $K_{J,M,\alpha}$. The isometry $\mathcal{C}(\rho)$ is then mapped to $\mathcal{C}(\sigma)$ by the operator

$$\tilde{K}^{\mathcal{C}}_{N,N,\alpha} = K_{N,N,\alpha} \otimes \sum_n |n+N\rangle\langle n|. \tag{B.6}$$

On the other hand, $\mathcal{L}(\rho)$ is then mapped to $\mathcal{L}(\sigma)$ by the operator

$$\tilde{K}^{\mathcal{L}}_{N,N,\alpha} = \\ \sum_n |n+N; n+N\rangle\langle n; n| \otimes \sum_n c^{(N,\alpha)}_{n,\lambda,\lambda'} \, |n+N; \lambda'\rangle\langle n; \lambda|. \tag{B.7}$$

The operators $\tilde{K}^{\mathcal{C}}_{N,N,\alpha}$ can be implemented by a LOCC-transformation, as the $\mathcal{C}$ is a LOCC-simulating isometry. Now, interestingly, the simulating operator of the second isometry, $\tilde{K}^{\mathcal{L}}_{N,N,\alpha}$ is implementable by LOCC-transformations as well. So in the case of the Abelian groups, the isometry $\mathcal{L}$ is also a LOCC-simulating isometry. In fact, the forms of $\tilde{K}^{\mathcal{C}}_{N,N,\alpha}$ and $\tilde{K}^{\mathcal{L}}_{N,N,\alpha}$ are similar, both comprised of the tensor product of a copy of the original G-covariant operator $K_{N,N,\alpha}$ and a translation operator. Thus, the isometry

$$|n, \lambda; n\rangle \otimes |n\rangle \mapsto |n; n\rangle \otimes |n; \lambda\rangle$$

maps LOCC-transformations to equivalent LOCC transformations. In this sense, the two isometries $\mathcal{C}$ and $\mathcal{L}$ are equivalent.

The image state under either isometry is an entangled state if and only if the initial state has no coherence in n, *i.e.* if the state is a coherent superposition of states with different values of n. On the other hand, states acting on the original Hilbert space $\mathscr{H}$ with no coherence in n are the G-invariant states, and the twirling operation destroys the coherence in n.

Proposition 34. *If G is an Abelian group, then the image state $\mathcal{C}(\rho)$ (or equivalently $\mathcal{L}(\rho)$) is a separable state if and only if the initial state $\rho \in \mathcal{B}(\mathscr{H})$ is G-invariant.*

Finally, as a corollary we note that the average state $\bar{\sigma}$ of Eq. (6.18) is a separable state and has no entanglement.

Bibliography

[1] Y. Aharonov and L. Susskind. Charge superselection rule. *Phys Rev.*, 155:1428–1431, 1967.

[2] A. Ambainis, H. Buhrman, Y. Dodis, and H. Roehrig. Multiparty quantum coin flipping. In *Proceedings of* 19^{th} *IEEE Annual Conference on Computational Complexity*, 2004.

[3] L. E. Ballentine. *Quantum Mechanics: A Modern Development.* World Scientific Publishing Co. Pte. Ltd., Singapore, 1998.

[4] S. D. Bartlett, T. Rudolph, B. C. Sanders, and P. S. Turner. Degradation of a quantum directional reference frame as a random walk. *J. Mod. Opt.*, 54:2211, 2007.

[5] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Decoherence-full subsystems and the cryptographic power of a private shared reference frame. *Phys. Rev. A*, 70:032307, 2004.

[6] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Degradation of a quantum reference frame. *New J. Phys.*, 8:58, 2006.

[7] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Dialogue concerning two views on quantum coherence: Factist and fictionist. *Int. J. Quantum Inf.*, 4:17–43, 2006.

[8] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79:555–609, 2007.

[9] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner. Quantum communication using a bounded-size quantum reference frame. *New J. Phys.*, 11:063013,

2009.

[10] S. D. Bartlett and H. M. Wiseman. Entanglement constrained by superselection rules. *Phys. Rev. Lett.*, 91:097903, 2003.

[11] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[12] C. H. Bennet and G. Brassard. *Quantum Cryptography: Public key distribution and coin tossing.* In *IEEE International Conference on Computers, Systems and Signal*, IEEE Press, New York, 1984.

[13] C. H. Bennett. Quantum information and computation. *Phys. Today*, 137:24–30, 1995.

[14] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys Rev Lett.*, 70:1895–1899, 1993.

[15] N. Byers. E. Noether's discovery of the deep connection between symmetries and conservation laws. In *Israel Mathematical Conference Proceedings*, volume 12, September 1999.

[16] M. A. Caprio, K. D. Sviratcheva, and A. E. McCoy. Racah's method for general subalgebra chains: Coupling coefficients of SO(5) in canonical and physical bases. *J. Math. Phys.*, 51:093518, 2010.

[17] M. Chaichian and R. Hagedorn. *Symmetries in Quantum Mechanics from Angular Momentum To Supersymmetry.* Institute of Physics Publishing, Bristol and Philadelphia, 1997.

[18] J-Q. Chen. *Group Representation Theory for Physicists.* World Scientific Publishing Co. Pte. Ltd., Singapore, 1989.

[19] G. Chiribella. *Optimal Estimation of Quantum Signals in the Presence of Symmetry.* PhD thesis, Università Degli Studi Di Pavia, 2006.

[20] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. Efficient use of quantum resources for the transmission of a reference frame. *Phys. Rev. Lett.*, 93:180503, 2004.

[21] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. *Phys. Rev. A*, 59:4249–4254, 1999.

[22] D. Deutsch. The church-turing principle and the universal quantum computer. *Proc. Roy. Soc. London, Ser. A*, 400:97–117, 1985.

[23] C. Doescher and M. Keyl. An introduction to quantum coin-tossing. arXiv:0206088 [quant-ph], 2002.

[24] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 41:777–780, 1935.

[25] M. El-Batanouny and F. Wooten. *Symmetry and Condensed Matter Physics A Computational Approach.* Cambridge University Press, New York, 2008.

[26] A. Faessler, T. S. Kosmas, and G. K. Leontaris, editors. *Symmetries in Intermediate and High Energy Physics*, volume XVI. Springer-Verlag, 2000.

[27] S. Ferrara, R. Fioresi, and V.S. Varadarajan, editors. *Supersymmetry in Mathematics and Physics, UCLA Los Angeles, USA 2010.* Springer-Verlag Berlin Heidelberg, 2011.

[28] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[29] C. Giedke and J. I. Cirac. The characterization of gaussian operations and distillation of gaussian states. *Phys. Rev. A*, 66:032316, 2002.

[30] R. Goodman and N. R. Wallach. *Representations and Invariants of the Classical Groups*. Cambridge University Press, 1998.

[31] G. Gour. Family of concurrence monotones and its applications. *Phys. Rev. A*, 71:012318, 2005.

[32] G. Gour. Mixed state entanglement of assistance and the generalized concurrence. *Phys. Rev. A*, 72:042318, 2005.

[33] G. Gour. Entanglement of collaboration. *Phys. Rev. A.*, 74:052307, 2006.

[34] G. Gour. Quantum resource theories. IOP conference, Bhubaneswar, India, January 2010. Illustration adopted from the accompanying presentation by with permission from the presenter.

[35] G. Gour, I. Marvian, and R. W. Spekkens. Measuring the quality of a quantum reference frame: the relative entropy of frameness. *Phys. Rev. A*, 80:012307, 2009.

[36] G. Gour, B. C. Sanders, and P. S. Turner. Time-reversal frameness and superselection. *J. Math. Phys.*, 50:102105, 2009.

[37] G. Gour and R. W. Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New J. Phys.*, 10:033023, 2008.

[38] D. C. Harris and M. D. Bertolucci. *Symmetry and Spectroscopy*. Oxford University Press, 1978.

[39] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani. Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication. *Phys. Rev. Lett.*, 96:040501, 2006.

[40] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani. Entanglement of multiparty stabilizer, symmetric, and antisymmetric states. *Phys. Rev. A*, 77:012104, 2008.

[41] P. Hayden and C. King. Correcting quantum channels by measuring the environment. *Quantum Information and Computation*, 5:156–160, 2005.

[42] A. S. Holevo. Statistical problems in quantum physics. In *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, volume 330, pages 104–119. Springer-Verlag, Berlin-Heidelberg, 1973.

[43] M. Horodecki. Entanglement measures. *Quantum Information and Computation*, 1:3–26, 2001.

[44] M. Horodecki. Quantum entanglement: Reversible path to thermodynamics. *Nature Physics*, 4:833–834, 2008.

[45] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Phys. Rev. Lett.*, 84:2014–2017, 2000.

[46] M. Horodecki and J. Oppenheim. Fundamental limitations for quantum and nano thermodynamics. arXiv:1111.3834v1 [quant-ph], 2011.

[47] M. Horodecki, J. Oppenheim, and R. Horodecki. Are the laws of entanglement theory thermodynamical? *Phys. Rev. Lett.*, 89:240403, 2002.

[48] R. Horodecki, R. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, 2009.

[49] L. M. Ioannou and M. Mosca. Public-key cryptography based on bounded quantum reference frames. arXiv:0903.5156v3 [quant-ph], 2009.

[50] D. Jonathan and M. B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Phys. Rev. Lett.*, 83:1455–1458, 1999.

[51] S. J. Jones, H. M. Wiseman, S. D. Bartlett, J. A. Vaccaro, and D. T. Pope. Entanglement and symmetry: A case study in superselection rules, reference frames, and beyond. *Phys. Rev. A*, 74:062313, 2006.

[52] I. Kassal, J. D. Whitfield, A. Perdomo-Ortiz, M. Yung, and A. Aspuru-Guzik. Simulating chemistry using quantum computers. *Annu. Rev. Phys. Chem.*, 62:185–207, May 2011.

[53] M. Keyl. Fundamentals of quantum information theory. *Physics Reports*, 369(5):431–548, 2002.

[54] A. Kitaev, D. Mayers, and J. Preskill. Superselection rules and quantum protocols. *Phys. Rev. A*, 69:052326, 2004.

[55] G. F. Koster. Matrix elements of symmetric operators. *Phys. Rev.*, 109:227–231, 1958.

[56] S. Lloyd. Universal quantum simulators. *Science*, 273:1073–1078, 2000.

[57] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997.

[58] H.-K. Lo, T. Spiller, and S. Popescu. *Introduction to Quantum Computation and Information*. World Scientific, Singapore, 1998.

[59] I. Marvian. A generalization of Noether's theorem and the information-theoretic approach to the study of symmetric dynamics. In *PIAF Workshop Brisbane*, 1-3 December 2010.

[60] I. Marvian and R. W. Spekkens. Pure state asymmetry. arXiv:1105.1816v1 [quant-ph], 2011.

[61] I. Marvian and R. W. Spekkens. The theory of manipulations of pure state asymmetry I: basic tools and equivalence classes of states under symmetric operations. arXiv:1104.0018v1 [quant-ph], 2011.

[62] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptography-Proceedings of Crypto'96*, pages 343–357. Springer-Verlag, New York, 1996.

[63] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.

[64] W. M. McClain. *Symmetry Theory in Molecular Physics with Mathematica*. Springer Science+Business Media, LLC, 2009.

[65] W. Miller. *Symmetry Groups and their Applications*. Academic Press, New York, 1972.

[66] K. Mølmer. Optical coherence: A convenient fiction. *Phys. Rev. A*, 55:3195–3203, 1997.

[67] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2000.

[68] E. Noether. Invariante Variationsprobleme. *Nachr. d. König. Gesellsch. d. Wiss. zu Göttingen, Math-phys. Klasse*, 1918:235–257, 1918.

[69] E. Noether and M. A. Tavel. Invariant variation problems. *Transport Theory and Statistical Physics.*, 1:186–207, 1971.

[70] M. B. Plenio. Logarithmic negativity: A full entanglement monotone that is not convex. *Phys. Rev. Lett.*, 95:090503, 2005.

[71] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quant. Inf. Comput.*, 7:1–51, 2007.

[72] R. C. Powell. *Symmetry, Group Theory, and the Physical Properties of Crystals*. Springer Science+Business Media, LLC, 2010.

[73] W. Rindler. *Relativity Special, General, and Cosmological*. Oxford University Press Inc., New York, 2006.

[74] D. J. S. Robinson. *A Course in the Theory of Groups*, volume 80. Springer-Verlag New York, Inc., 1980.

[75] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn. Universal state inversion and concurrence in arbitrary dimensions. *Phys. Rev. Lett.*, 64:042315, 2001.

[76] B. C. Sanders, S. D. Bartlett, T. Rudolph, and P. L. Knight. Photon-number superselection and the entangled coherent-state representation. *Physical Rev. A*, 68:042329, 2003.

[77] E. Schrödinger. Probability relations between separated systems. *Math. Proc. Cambridge*, 32:446–452, 1936.

[78] E. Schrödinger and M. Born. Discussion of probability relations between separated systems. *Math. Proc. Cambridge*, 31:555–563, 1935.

[79] N. Schuch, F. Verstraete, and J. I. Cirac. Nonlocal resources in the presence of superselection rules. *Phys. Rev. Lett.*, 92:087904, 2004.

[80] N. Schuch, F. Verstraete, and J. I. Cirac. Quantum entanglement theory in the presence of superselection rules. *Phys. Rev. A*, 70:042310, 2004.

[81] M. Skotiniotis and G. Gour. Alignment of reference frames and an operational interpretation for the G-asymmetry. *New J. Phys.*, 14:073022, 2012.

[82] M. S. Sozzi. *Discrete Symmetries and CP Violation*. Oxford University Press, 2008.

[83] A. Szabo and N. S. Ostlund. *Modern Quantum Chemistry: Introduction to Advanced Electronic Structure Theory*. Dover Publications, Inc., Mineola, New York, 1989.

[84] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Hiding bits in bell states. *Phys. Rev. Lett.*, 86:5807–5810, 2001.

[85] B. Toloui and G. Gour. Simulating symmetric time evolution with local operations. *New J. Phys.*, 14:123026, 2012.

[86] B. Toloui, G. Gour, and B. C. Sanders. Constructing monotones for quantum phase references in totally dephasing channels. *Phys. Rev. A*, 84:022322, 2011.

[87] W. Tung. *Group Theory in Physics: An Introduction to Symmetry Principles, Group Representation, and Special Functions in Classical and Quantum Physics*. World Scientific, Singapore, 2003.

[88] J. A. Vaccaro, F. Anselmi, H. M. Wiseman, and K. Jacobs. Tradeoff between extractable mechanical work, accessible entanglement, and ability to act as a reference system, under arbitrary superselection rules. *Phys. Rev. A*, 77:032114, 2008.

[89] S. J. van Enk. Quantifying the resource of sharing a reference frame. *Phys. Rev. A*, 71:032339, 2005.

[90] V. Vedral. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.*, 74:197–234, 2002.

[91] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, 1998.

[92] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275–2279, 1997.

[93] F. Verstraete and J. I. Cirac. Quantum nonlocality in the presence of superselection rules and data hiding protocols. *Phys. Rev. Lett.*, 91:010404, 2003.

[94] F. Verstraete and J. I. Cirac. Nonlocal resources in the presence of superselection rules. *Phys. Rev. Lett.*, 92:087904, 2004.

[95] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355–376, 2000.

[96] G. Vidal and R. Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59:141–155, 1999.

[97] G. Vidal and R. F. Werner. A computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002.

[98] J. von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton University Press, 1955.

[99] J. Watrous. Bipartite subspaces having no bases distinguishable by local operations and classical communication. *Phys. Rev. Lett.*, 95:080505, 2005.

[100] T. Wei and P. M. Goldbart. Geometric measure of entanglement for multipartite quantum states. *Phys. Rev. A*, 68:042307, 2003.

[101] A. J. Weir. *Lebesgue Integration and Measure.* Cambridge University Press, 1973.

[102] H. Weyl. Über die asymptotische Verteilung der Eigenwerte. *Nachr. Königl. Ges. Wiss. Göttingen*, pages 110–117, 1911.

[103] G. A. White, J. A. Vaccaro, and H. M. Wiseman. The consumption of reference resources. In *AIP Conference Proceedings*, volume 1110, page 79, 2009.

[104] G. A. White, J. A. Vaccaro, and H. M. Wiseman. Optimal reference states for maximum accessible entanglement under the local-particle-number superselection rule. *Phys. Rev. A*, 79:032109, 2009.

[105] G. C. Wick, A. S. Wightman, and E. P. Wigner. The intrinsic parity of elementary particles. *Phys. Rev.*, 88:101–105, 1952.

[106] N. Wiebe, D. W. Berry, P. Høyer, and B. C. Sanders. Simulating quantum dynamics on a quantum computer. *J. Phys. A: Math. Theor.*, 44:445308, 2011.

[107] E. P. Wigner. Conservation laws in classical and quantum physics. *Prog. Theor. Phys. II*, 19:437–440, 1954.

[108] C. P. Williams. *Explorations in Quantum Computing*. Springer-Verlag, 2011.

[109] H. M. Wiseman and J. A. Vaccaro. The entanglement of indistinguishable particles shared between two parties. *Phys. Rev. Lett.*, 91:097902, 2003.

[110] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, 1998.

[111] B. G. Wybourne. *Classical Groups for Physicists*. John Wiley & Sons, United States of America, 1974.

[112] K. Yasumoto, editor. *Electromagnetic Theory and Applications for Photonic Crystals*. Taylor & Francis Group, LLC, 2006.

[113] C. Zalka. Simulating quantum systems on a quantum computer. *Proc. Roy. Soc. London*, 46:877–879, 1998.

[114] D. Zhelobenko. *Translations of Mathematical Monographs: Principal Structures and Methods of Representation Theory*, volume 228. American Mathematical Society, 2004.