Symmetry, Asymmetry and Quantum Information

by

Iman Marvian Mashhad

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

It is impossible to overstate the importance of symmetry in physics and mathematics. Symmetry arguments play a central role in a broad range of problems from simplifying a system of linear equations to a deep role in organizing the fundamental principles of physics. They are used, for instance, in Noether's theorem to find the consequences of symmetry of a dynamics. For many systems of interest, the dynamics are sufficiently complicated that one cannot hope to characterize their evolution completely, whereas by appealing to the symmetries of the dynamical laws one can easily infer many useful results.

In part I of this thesis we study the problem of finding the consequences of symmetry of a (possibly open) dynamics from an information-theoretic perspective. The study of this problem naturally leads us to the notion of asymmetry of quantum states. The asymmetry of a state relative to some symmetry group specifies how and to what extent the given symmetry is broken by the state. Characterizing these is found to be surprisingly useful to constrain which final states of the system can be reached from a given initial state. Another motivation for the study of asymmetry comes from the field of quantum metrology and relatedly the field of quantum reference frames. It turns out that the degree of success one can achieve in many metrological tasks depends only on the asymmetry properties of the state used for metrology. We show that some ideas and tools developed in the field of quantum information theory are extremely useful to study the notion of asymmetry of states and therefore to find the consequences of symmetry of an open or closed system dynamics.

In part II of this thesis we present a novel application of symmetry arguments in the field of quantum estimation theory. We consider a family of multi-copy estimation problems wherein one is given n copies of an unknown quantum state according to some prior distribution and the goal is to estimate certain parameters of the given state. In particular, we are interested to know whether collective measurements are useful and if so to find an upper bound on the amount of entanglement which is required to achieve the optimal estimation. We introduce a new approach to this problem by considering the symmetries of the prior and the symmetries of the parameters to be estimated. We show that based on these symmetries one can find strong constraints on the amount of entanglement required to implement the optimal measurement. In order to infer properties of the optimal estimation procedure from the symmetries of the parameters and the prior we come up with a generalization of Schur-Weyl duality. Just as Schur-Weyl duality has many applications to quantum information theory and quantum algorithms so too does this generalization. In this thesis we explore some of these applications.

Acknowledgements

First and foremost, I would like to express my deep and sincere gratitude to my co-supervisor and friend Robert Spekkens for his support and guidance. It is hard for me to find the words to fully express my respect for him. His influence on my life goes well beyond my academic career. Also, I would to thank my supervisor Michele Mosca for his support and wisdom throughout these four years.

I appreciate my thesis committee members Andrew Doherty, Andrew Childs and Marco Piani for providing useful comments on my PhD thesis.

I have been lucky to have helpful discussions on the topics presented in this thesis with many great researchers. This lengthy list includes, but is certainly not limited to, Robert Mann, Carl Caves, Hideo Mabuci, Easwar Magesan, Lana Sheridan, Aram Harrow, Daniel Gottesman, Stephen Bartlett, Terry Rudolph, Paolo Zanardi, John Preskill, Barry Sanders, Howard Wiseman, Patrick Hayden, Sarah Croke, Sandu Popescu, John Watrous, Ignacio Cirac, Ben Schumacher and Marcus Mueller. In particular, I acknowledge a lot of stimulating conversations with my collaborator and friend Giulio Chiribella.

I would like to thank Gilad Gour and Barry Sanders for inviting me to the Institute for Quantum Information Science at the university of Calgary twice. I acknowledge a lot of hot and fruitful discussions with Gilad Gour and his group members Michael Skotiniotis, Borzumehr Toloui and Yuval Sanders. Also, I would like to thank Carl Caves, Hideo Mabuci, John Preskill, Giulio Chiribella, Howard Wiseman and Stephen Bartlett for inviting me to their institutes.

During my studies at Waterloo I have been fortunate to work at the Perimeter Institute for theoretical physics and the Institute for Quantum Computing. Working at these institutes made my PhD studies and my life much more enjoyable and fruitful. I am deeply indebted for the resources they have provided me. Also, I thank Mike and Ophelia Lazaridis, who gave me their support through the Mike and Ophelia Lazaridis Fellowship for four years.

Finally, I would like to thank my friends and family. I owe a debt of gratitude to my wonderful friends in Waterloo who have all enriched my life in one way or another. Special thanks to dear Yasaman for being so wonderful and supportive. Last but not least, I would like to thank my parents for all their love and support throughout my life.

Table of Contents

List of Figures

Overview

Symmetric dynamics and asymmetry of states

Symmetry arguments are ubiquitous in physics. Finding the consequences of symmetries in dynamics is a subject with broad applications in physics, from the smallest scales in high energy scattering experiments, to the largest scales in astrophysical observations. Their prominence stems from the fact that for many systems of interest, the dynamics are sufficiently complicated that one cannot hope to characterize their evolution completely, whereas by appealing to the symmetries of the dynamical laws one can easily infer many useful results.

Suppose that the only thing one knows about a complicated quantum dynamics, which is possibly open, is that it has a particular symmetry. What does this imply about the evolution of the system's state? Alternatively, suppose one is given a description of an initial quantum state and a possible final state for a system. Can the first evolve to the second by symmetric dynamics? These sorts of problems arise in many physical contexts. For instance, they are clearly important in any situation wherein one might apply Noether's theorem (which infers conservation laws from symmetries in the case of closed dynamics). To answer them, it is useful to study the *asymmetry properties of a state*, that is, those properties which specify how and to what extent the given symmetry is broken by the state. If the dynamical equations are invariant under a symmetry group of transformations then there are constraints on how the asymmetry properties can change. For instance, the final state can only break the symmetry in ways in which it was broken by the initial state, and its measure of asymmetry can be no greater than that of the initial state. In other words, *symmetric dynamics cannot generate asymmetry.*

Another motivation for the study of asymmetry is the problem of characterizing and classifying *quantum reference frames* (see [1] for a review). A quantum reference frame sent from a party, called Alice, to a distant party, called Bob, is a quantum system which

informs Bob about Alice's choice of reference frame. For example, by sending a large spin prepared in $\hat{z}$ direction relative to her own local frame, Alice can inform Bob about how she has chosen the $\hat{z}$ axis in her local frame or similarly by sending a coherent state she can inform Bob about the phase of her clock. Bob may use this quantum system to acquire information about the description of Alice's frame relative to his own local frame or may use it to prepare states and perform operations whose descriptions are only given relative to Alice's local frame, such as rotating a given system around Alice's $\hat{z}$ axis. So in this sense a quantum reference frame can be thought as a *resource* which carries information about one party's local frame and therefore the performance of any given state as a quantum reference frame is determined by the information carried by the state about that party's local conventions.

In the example of lack of shared Cartesian frame, it is clear that if Bob does not know anything about Alice's local frame then he cannot perform an operation whose description is only given relative to Alice's local frame unless the operation is invariant under rotation. In this sense, Bob is effectively under a *superselection rule*, i.e. he can only prepare states and perform operations which have rotational symmetry. A quantum reference frame that Alice sends to Bob breaks this rotational symmetry and allows him to perform operations or prepare states which are not invariant under rotation.

From this discussion we can see that the relevant property of a state which determines its performance as a quantum reference frame is its *asymmetry* relative to a symmetry group. So in some situations the asymmetry of states can be considered as a resource which cannot be generated under symmetric dynamics, similar to the fact that the entanglement is a resource which cannot be generated by local operations and classical communication (LOCC). In the *resource theory of entanglement*, to classify entangled states one is often interested to know whether a given state can be transformed to the other under LOCC operations. Similarly, here in the *resource theory of asymmetry* one central question is whether a given state can evolve to the other under an open or closed dynamics which has a particular symmetry and the properties of a state which are relevant to answer this question are called the *asymmetry properties* of the state. For almost any question that one might pose about entanglement, one can ponder the analogous question for asymmetry. The resource perspective has been an extremely useful method for organizing results about entanglement, so one may expect the same to be true of asymmetry as well. We explain more about this point of view to asymmetry in section 2.2.

In some previous works in the context of quantum reference frames, the asymmetry has been called the *frameness* of the state [16, 6]. Therefore, all the results about the manipulation of reference frames and their frameness are in fact results about the asymmetry of states. In particular, [16] presents a systematic study of the manipulations of

pure state asymmetry for groups $U(1)$ and Z_2 and also presents some partial results for the case of $SO(3)$. In this thesis, using a different approach based on characterizing the equivalence classes of asymmetries of pure states, we are able to generalize the results in [16] significantly and to extend their scope to arbitrary compact Lie groups and finite groups.

From the above example of Alice sending a quantum reference frame to Bob, it is clear that there is another way to think about the notion of asymmetry: In this point of view, the asymmetry of state ρ relative to a group, say the group of rotations, is the property of the state which specifies the performance of the code $\Omega \in SO(3) \to U(\Omega)\rho U^\dagger(\Omega)$ for encoding information about a randomly chosen rotation Ω (where $U(\cdot)$ is the unitary representation of rotation on the Hilbert space of the system). This simple observation implies that some tools and ideas from quantum information theory can be used for the study of the asymmetry properties of states and thus can be used to find the consequences of the presence of symmetry in a dynamics.

For instance, we show that using an arbitrary information monotone such as the Holevo quantity or the relative Renyi entropy, one can build *asymmetry monotones*, functions from states to real numbers which quantify the amount of symmetry breaking of any given state, such that the value of these functions are non-increasing under symmetric dynamics. So even if the only thing we know about a (possibly open) dynamics is that it has a particular symmetry, then using these measures of asymmetry we can find constraints on the possible final states of the time evolution according to its initial state: a final state is possible only if it has equal or less asymmetry than the initial state. On the other hand, for closed system dynamics, each asymmetry monotone is a conserved quantity under the symmetric dynamics, i.e. a constant of the motion. It turns out that, for transitions between mixed states, the conserved quantities one obtains in this way are generally independent of those prescribed by Noether's theorem and therefore impose new constraints.

It is worth pointing out a few more motivations for a systematic study of the asymmetry properties of states. One is the study of symmetry-breaking. For instance, if a system is observed to undergo dynamics that breaks a symmetry and there are different candidates for the origin of this asymmetry, such as an asymmetric perturbation in the Hamiltonian or fluctuations induced by an asymmetric state of the environment, then having a framework for quantifying the asymmetry of a state and characterizing different classes thereof can be useful in judging the relative likelihood of these different explanations.

Another important motivation comes from the field of *quantum metrology*, wherein one explores the use of quantum techniques to achieve greater precision for a variety of different kinds of parameter estimation tasks [14]. High-precision clocks, gyroscopes and

accelerometers are prominent examples, for which achieving a quantum improvement in precision would have significant applications for the rest of physics. The parameter to be estimated for such tasks is an unknown element of a group. For instance, the task of aligning a pair of Cartesian reference frames by transmitting a system that breaks rotational symmetry and estimating its orientation is clearly of this sort (see [1] for a review of this topic). The degree of success one can achieve in any such task is clearly a function of the asymmetry properties of the state that is transmitted, so a systematic study of these properties can help to develop optimal protocols and strategies for dealing with practical constraints such as noise.

Generalization of Schur-Weyl duality with applications in quantum estimation

During the research on quantum reference frames, we realized that the intuition about quantum reference frames and more generally about observers with uncorrelated local frames is useful to solve a totally different problem. The problem is about parameter estimation where one is given multiple copies of a quantum state and the goal is to estimate some parameter(s) of state such as the expectation value of one or more observables. In particular, one interesting question is whether entangled measurements can have any advantages over unentangled measurements.

For instance, consider a multi-copy estimation problem in the following form: "A pure state of a *qudit* [1] system is randomly chosen according to the Haar measure and n copies of the state is prepared and is given to us. Our goal is to estimate a function of the chosen state where the function can be expressed as the expectation value of qudit observables $\{A_i\}$ or any other operator in the algebra generated by them. Also, the figure of merit to evaluate the performance of our estimation procedure is such that it can be expressed only in terms of observables $\{A_i\}$ (for instance, the mean squared error of estimating the expectation value of some observable $A_0 \in \{A_i\}$). "

Now assume Alice and Bob each use their own personal convention to associate observables with operators in the Hilbert space of a system and assume that each observer is not aware of the other's convention. All they know is that for the particular set of operators $\{A_i\}$, the observable which is described by operator A_i relative to Alice's convention is also described by operator A_i relative to Bob's convention. But having this amount of agreement between two observers is sufficient to make sure that they agree on the description

[1] A quantum system with Hilbert space isomorphic to $\mathbb{C}^d$.

of the above multi-copy estimation problem. Now the intuition is that if two observers can agree on the description of this estimation problem they should also be able to agree on the description of an optimal estimation strategy. So the optimal measurement can be chosen to be in the set of measurements on n qudits for which Alice and Bob can agree on their description. It is straightforward to see that on n qudits Alice and Bob can agree on the description of all observables which are in the algebra generated by the n fold product of observables $\{A_i\}$ and the canonical representation of the permutation group of degree n. One intuitively expects that there cannot be any other observable for which they agree on its description. Trying to prove this intuition led us to a generalization of Schur-Weyl duality which works for specific subgroups of the unitary group which we call *gauge groups*. Any gauge group can be thought as the set of all unitaries which commute with a certain set of observables. For instance, in the above scenario, the set of all unitaries which can describe the relation between Alice's and Bob's conventions are the set of all unitaries which commute with $\{A_i\}$ and so this set is a gauge group.

A particularly interesting consequence of this new duality is when the support of the total state of n systems is restricted to the symmetric or anti-symmetric subspace (as it is in the case of the above estimation problem). In this case the *global symmetry* of measurements with respect to a gauge group can be promoted to the *local symmetry* with respect to that gauge group in the following sense: if a measurement is invariant under the collective action of a gauge group then there exists a measurement which is invariant under the local actions of that gauge group on each individual system, which has exactly the same statistics for all states whose supports are restricted to the symmetric/anti-symmetric subspace.

Based on these ideas, we introduce a new method to study the multi-copy estimation problems in which one first specifies the set of all observables which are required to describe the single copy problem and then conclude that the optimal measurement on multiple copies should have local symmetry with respect to the gauge group of these observables. But the local symmetry of a measurement with respect to a non-trivial gauge group implies a bound on the amount of entanglement which is required to implement the measurement. In particular, if the gauge group under consideration is the group of all unitaries which commute with a set of commuting observables, then local symmetry of a measurement with respect to that gauge group implies that this measurement can be implemented by independent local measurements on each system followed by a classical processing on the outcomes of these measurements.

Given that the class of estimation problems for which this result applies is very large, it represents a dramatic expansion, relative to previously known results, in the scope of problems for which we can easily determine the optimal measurement. Furthermore, in

the previous results where independent measurements on each copy were shown to be optimal, such as Ref. [67], the reasoning was rather *ad hoc*. It was not clear what feature of the estimation problem implied the sufficiency of such measurements. By contrast, this approach follows a clear methodology – we are determining the consequences of the gauge symmetries of the estimation problem.

Finally, as Schur-Weyl duality has many different applications in quantum information one may expect some other applications for this new generalization of Schur-Weyl duality. An example of such applications, which we present in this thesis, is to find the noiseless subsystems of n qudits.

Outline

This thesis presents the results of four related projects.[2]

1. Information theoretic approach to the study of symmetric dynamics and asymmetry monotones
2. Modes of asymmetry: Fourier Analysis for the study of linear covariant maps
3. Pure state asymmetry
4. A generalization of Schur-Weyl duality with applications in quantum estimation

The results of the first two projects are still unpublished. The results of the third and fourth projects are presented in [2, 3] and [4] respectively. [3]

In the following we give a short summary of the contents of each chapter.

Part I

Chapter 1: In this chapter we explain some preliminary notions and introduce the notations we use in the rest of part I. We define the notion of *projective unitary representations of groups* as the mathematical way to represent symmetry transformations on the

[2] These projects are all done in collaboration with Robert W. Spekkens.

[3] During my PhD, I have also contributed in two other published papers on quantum reference frames and asymmetry monotones [5, 6].

Hilbert space of systems. We also define the notion of symmetric dynamics or *G-covariant channels*, i.e. the channels which have symmetry with respect to a group G and then we present two physically motivated examples of dynamics which have U(1) symmetry. Furthermore we give more precise descriptions of the problems we are studying in part I.

Chapter 2: In this chapter we give a mathematical definition of the notion of asymmetry of states. The main idea in this definition is that asymmetry cannot be generated by symmetric dynamics and so we postulate that two states have the same asymmetry with respect to a group G, or are *G-equivalent* iff each of them can be transformed to the other by a G-covariant channel. We also introduce a dual point of view to the notion of asymmetry in which one can understand asymmetry in terms of information theoretic concepts. We show that these two approaches to asymmetry, i.e. the approach based on the symmetric dynamics and the information theoretic approach lead to equivalent characterizations of asymmetry. Finally, we discuss the analogies between the study of asymmetry and the study of entanglement as two examples of resource theories.

Chapter 3: In this chapter we introduce the notion of *asymmetry monotones* or measures of asymmetry. These quantify the amount of asymmetry of states relative to a given symmetry group. Based on the information theoretic point of view to asymmetry introduced in chapter 2, we give a recipe for constructing asymmetry monotones from information monotones, the functions which quantify the amount of information that can be transferred using a particular encoding of information. Asymmetry monotones are useful tools to find the consequences of symmetry of an open system dynamics; they provide simple constraints on the possible final states of an open system dynamics based on the symmetry of the dynamics. We present an example of these constraints which proves the existence of a non-trivial lower bound on the entropy generation in an open system dynamics with symmetry. On the other hand, in any closed system dynamics with symmetry, any asymmetry monotone is a constant of motion. We prove that in the case of closed system dynamics of mixed states the conservation of any non-trivial asymmetry monotone gives constraints which are stronger than the constraints imposed by the standard conservation laws implied by Noether's theorem.

Chapter 4: We start this chapter by a quick review of the notion of *irreducible tensor operators*. Then, based on this notion we introduce a simple and useful representation for all linear super-operators which have a certain symmetry. This representation basically specifies the action of a super-operator on a basis in the operator basis which is formed from irreducible tensor operators. Then, we review two other previously known representations of symmetric channels: the Kraus representation of symmetric channels and Stinespring dilation of symmetric channels. We provide a new constructive proof for the Stinespring dilation theorem of symmetric channels. This theorem asserts that any symmetric time

evolution can be realized by coupling the system to an environment which is initially in a symmetric state via a unitary which is also symmetric.

Chapter 5: In this chapter, we introduce the notion of *modes of asymmetry* and the *mode decomposition* of a state. Roughly speaking, different modes of asymmetry are different ways that a state can break a given symmetry. If for a given symmetry group, a state does not have a particular mode of asymmetry then under a dynamics which does not break that symmetry it can never evolve to a state which has that mode of asymmetry. Mathematically the existence of different independent modes follows from the two properties of linearity of a time evolution and its symmetry together. We also introduce asymmetry monotones which quantify the amount of asymmetry in each specific mode. Finally, we study the problem of simulating a non-symmetric time evolution or measurement using a symmetric dynamics and a *quantum reference frame* and we show that the mode decompositions of states and channels provide a powerful insight for the study of this problem.

Chapter 6: In this chapter we focus on the study of the asymmetry of pure states. We show that for a pure state ψ and a symmetry group G, all the asymmetry properties of the state are specified by the *characteristic function* of the state, defined as $\chi_\psi(g) \equiv \langle\psi|U(g)|\psi\rangle$ where $g \in G$ and U is the unitary representation of interest. Based on this observation, and using the Stinespring dilation theorem for symmetric channels (reviewed in chapter 4) we find the necessary and sufficient condition under which two pure states have the same asymmetry relative to any connected compact Lie group. We also prove a slightly weaker result in the case of finite groups and Lie groups which are not connected. Characteristic functions also allow us to easily identify the conditions for one pure state to be converted to another by symmetric operations (in general irreversibly) for the various paradigms of single-copy transformations: deterministic, state to ensemble, stochastic and catalyzed.

Part II

Chapter 7: In this chapter we review some preliminary notions we use in the part II of the thesis and introduce the notations. In particular, we review some properties of finite dimensional operator algebras, the notion of commutant of an algebra and the notion of the centralizer of a subgroup of a group. Furthermore, we review the notion of dual reductive pairs and present the standard Schur-Weyl duality as an example.

Chapter 8: In this chapter we present the generalization of Schur-Weyl duality. We start by defining and characterizing the notion of gauge groups. Then, based on this, we introduce new dual reductive pairs acting on the space $(\mathbb{C}^d)^{\otimes n}$ and show that the standard

Schur-Weyl duality is indeed a special case of these new dual reductive pairs. Next we consider the symmetric and anti-symmetric subspaces of $(\mathbb{C}^d)^{\otimes n}$ and show that a stronger form of the duality holds in these subspaces. We also show that the assumptions we have made, i.e. the restriction to the gauge groups and the restriction to the symmetric and anti-symmetric subspaces, are essential to have these dualities.

Chapter 9: In this chapter we present two examples of applications of the generalization of Schur-Weyl duality. The first example shows application of this result for finding noiseless subsystems. The second example is of an application of the stronger form of duality in the symmetric and anti-symmetric subspaces. We first study the notions of global and local symmetry of measurements and show that the local symmetry of measurements can put a bound on the amount of entanglement which is required to perform a measurement. Then, we use the duality to prove that the global symmetry of a measurement with respect to a gauge group can be promoted to a local symmetry, i.e. for any many measurement with global symmetry we find a measurement with local symmetry which generates the same statistics for all states in the symmetric (anti-symmetric subspaces). This result is the seed of the results of the next two chapters on the estimation theory.

Chapter 10: In this chapter we introduce a framework for the study of a family of multi-copy estimation problems, in which one is given several copies of the same qudit state according to some known prior distribution and the goal is to estimate some parameters about that qudit state. The quality of estimation is evaluated with respect to a given figure of merit. Then, we use the result of the previous chapter about promoting the global symmetry of a measurement to the local symmetry to find conditions which guarantee that a measurement with local symmetry can achieve the optimal estimation in a multi-copy estimation problem in this family. Roughly speaking, these conditions are based on the symmetries of the prior and the symmetries of the parameters to be estimated. The fact that there exists an optimal measurement for the estimation problem with local symmetry with respect to a gauge group, puts a bound on the maximum entanglement which is required for the optimal estimation.

Chapter 11: In this chapter we consider a different family of estimation problems where one is given a *single* copy of a pair of qudits and the goal is to compare the state of these two qudits. For example, we are given state $\rho_L \otimes \rho_R$ according to some prior and we are interested to find the optimal strategy for estimating $|\mathrm{tr}(\rho_L A) - \mathrm{tr}(\rho_R A)|$ for some qudit observable A. We use the result of chapter 9 on promoting the global symmetry of measurements to the local symmetry to find the general form of the optimal estimation strategy for this family of estimation problems.

Chapter 12: In this chapter we elaborate on the problem we presented in the overview

about two independent observers using different conventions to describe quantum systems and show that the generalization of Schur-Weyl duality naturally arises in the study of this problem.

Part I

Symmetric dynamics and Asymmetry of states

Chapter 1

Symmetric operations

1.1 Preliminaries

A *symmetry transformation* is a transformation which leaves the physical objects, structures or dynamics unchanged. Group theory provides the mathematical language to describe symmetries. One can easily see that the set of symmetries of an object form a group: they are closed because if one takes a symmetry of the object, and then applies another symmetry, the total transformation will still leave the object unchanged and so is a symmetry. Furthermore, the identity transformation always leaves the object unchanged and so is a symmetry of the object. The associativity is a result of the fact that symmetries can be thought of as maps on a space, and composition of maps is associative. Finally, if a transformation leaves the object unchanged, undoing that transformation also leaves it unchanged and so the inverse of a symmetry is also a symmetry.

In quantum theory the action of any symmetry transformation should be described by a unitary or anti-unitary acting on the Hilbert space of the system. This follows from the fact that a symmetry transformation can always be interpreted as a change of reference frame or convention and this change should not affect the physically observable properties. In particular, it should not affect the distinguishability of states. Then, it follows from a well-known theorem [1] by Wigner [9] that any such transformation is represented by a unitary or an anti-unitary operator on the Hilbert space of the system such that an arbitrary density operator ρ is mapped by the symmetry transformation to the density

[1] **Theorem:** Let T be a surjective map from a complex Hilbert space to itself such that $|\langle T\phi|T\psi\rangle| = |\langle\phi|\psi\rangle|$ for all pure state ψ and ϕ. Then T has the form of $T\psi = e^{i\theta(\psi)}V\psi$ where $\theta(\psi)$ is an arbitrary real function and V is either a unitary or anti-unitary operator.

operator $V\rho V^\dagger$ for some unitary or anti-unitary operator V. In the first part of this thesis we do not consider symmetry transformations, such as time-reversal, that are represented by anti-unitary operators. Therefore, any symmetry we consider here is represented by a unitary acting on the Hilbert space of the system.

Let G be a group describing a set of symmetry transformations or a *symmetry* for short. Then the action of each group element $g \in G$ should be described by a unitary $U(g)$. It follows that for consistency it should hold that for any pair of group elements g_1 and g_2 in group G

$$U(g_2g_1)\rho U^\dagger(g_2g_1) = U(g_2)\left(U(g_1)\rho U^\dagger(g_1)\right)U^\dagger(g_2) \tag{1.1}$$

Since this should hold for any arbitrary state ρ one can conclude that

$$U(g_2g_1) = \omega(g_2, g_1)U(g_2)U(g_1) \tag{1.2}$$

where $\omega(g_2, g_1)$ is a phase factor, i.e. $|\omega(g_2, g_1)| = 1$. This means that a symmetry described by group G should be represented by *a projective unitary representation of group G*. The phase factor $\omega(g_1, g_2)$ is called the *cocycle* of the representation. We denote a specific projective unitary representation of G by the set of unitaries $\{U(g), g \in G\}$ or by the map $g \to U(g)$. In the specific case where the cocycle $\omega(g_1, g_2)$ is constant and equal to one, the representation is called *(non-projective) Unitary representation*. At the end of this section we provide a short list of some useful properties of projective unitary representations of compact Lie groups and finite groups. For a helpful review of this topic we refer to chapter 2 of Giulio Chiribella's thesis [10].

We will frequently use the unitary super-operator notation to represent the action of groups. For any group G and any projective unitary representations $g \to U(g)$ we define the super-operator

$$\mathcal{U}_g(X) = U(g)XU^\dagger(g). \tag{1.3}$$

So under the symmetry transformation $g \in G$ the state ρ will be mapped to $\mathcal{U}_g(\rho)$.

The representation of the fundamental symmetries of nature, such as the symmetries of space-time, are part of the specification of a physical system. For example, on a system with a two-dimensional Hilbert space the group of all rotations in the three-dimensional real space $\mathbb{R}^3$, i.e. the group SO(3), can have two different representations: the trivial representation where the action of symmetry transformations leaves all states unchanged and the non-trivial representation corresponding to the spin-half representation of SO(3). These two different representations of SO(3) describe totally different systems with different physical properties.

For most symmetries, such as the fundamental symmetries of space-time, the representation of the symmetry on a composite systems is the *collective representation*: if the

projective unitary representation of a symmetry transformation $g \in G$ on the systems with the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are $U_A(g)$ and $U_B(g)$ respectively, then the projective unitary representation of that symmetry transformation on the Hilbert space of the composite system with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is $U_A(g) \otimes U_B(g)$. In this thesis we always assume that the representation of the symmetry on the joint system is the collective representation.

1.1.1 Short review of projective unitary representations

In this section we list some useful definitions and properties of projective unitary representations of groups which we use in this thesis.

Two projective unitary representations of a group, $g \to U(g)$ acting on space $\mathcal{H}$ and $g \to V(g)$ acting on space $\mathcal{K}$, are *equivalent* iff there exists an isometry $T : \mathcal{H} \to \mathcal{K}$ such that $TT^\dagger = \mathbb{I}_\mathcal{K}$ and $T^\dagger T = \mathbb{I}_\mathcal{H}$, where $\mathbb{I}_\mathcal{K}$ and $\mathbb{I}_\mathcal{H}$ are the identity operators on $\mathcal{K}$ and $\mathcal{H}$ respectively, and $\forall g \in G :\ TU(g)T^\dagger = V(g)$.

Consider an arbitrary projective unitary representation of a group on a space. We say a subspace of this space is *invariant* under the action of group, if under the action of any arbitrary element of the group any vector in the subspace is mapped to a vector in this subspace.

A representation on a space is called an *irreducible* representation (*irrep* for short) if there is no proper subspace of the space (i.e. a nonzero subspace which is not equal to the total space) which remains invariant under the action of the group. Equivalent irreps can be grouped in the same equivalence class, labeled by the Greek index μ.

Note that the unitarity of a projective unitary representation implies that all the irreps which show up in that representation should have the same cocycle. Any two projective unitary representations $g \to U(g)$ and $g \to V(g)$ which have the same cocyle, i.e. $U(g_1)U(g_2) = \omega(g_1, g_2)U(g_1 g_2)$ and $V(g_1)V(g_2) = \omega(g_1, g_2)V(g_1 g_2)$ for a cocycle $\omega(g_1, g_2)$ are said to be in the same *factor system.*

Theorem 1 *Any projective unitary representation of a finite or a compact Lie group can be decomposed into a direct sum of a discrete number of finite dimensional projective unitary irreps which are all in the same factor system.*

Suppose $\{U(g) : g \in G\}$ is a projective unitary representation of a finite or compact Lie group G on the Hilbert space $\mathcal{H}$. Then, the decomposition of this representation to

irreps suggests the following decomposition of the Hilbert space

$$\mathcal{H} = \bigoplus_{\mu} \mathcal{M}_\mu \otimes \mathcal{N}_\mu, \tag{1.4}$$

where μ labels inequivalent unitary projective irreps in the same factor system, $\mathcal{M}_\mu$ is the subsystem on which $\{U(g) : g \in G\}$ acts like irrep μ of G and $\mathcal{N}_\mu$ is the subsystem associated to the multiplicities of representation μ (the dimension of $\mathcal{N}_\mu$ is equal to the number of multiplicities of the irrep μ in this representation). Then $U(g)$ can be written as

$$U(g) = \bigoplus_{\mu} U_\mu(g) \otimes \mathbb{I}_{\mathcal{N}_\mu} \tag{1.5}$$

where $U_\mu(g)$ acts on $\mathcal{M}_\mu$ irreducibly and where $\mathbb{I}_{\mathcal{N}_\mu}$ is the identity operator on the multiplicity subsystem $\mathcal{N}_\mu$.

Now by Schur's lemmas it follows that any operator A which commutes with all unitaries $\{U(g) : g \in G\}$ should be in the following form

$$A = \bigoplus_{\mu} \mathbb{I}_{\mathcal{M}_\mu} \otimes A_{\mathcal{N}_\mu}, \tag{1.6}$$

where $A_{\mathcal{N}_\mu}$ acts on $\mathcal{N}_\mu$.

Theorem 2 *For a finite or compact Lie group G, let $\{g \to U^{(\mu)}(g)\}$ be the set of all inequivalent projective unitary irreps which are in the same factor system. Consider the matrix elements of all these unitary matrices as a set of functions from G to $\mathbb{C}$ denoted by $\{U^{(\mu)}_{i,j}\}$. Then, they satisfy the following orthogonality relations*

$$\int_G dg \; U^{(\mu)}_{i,j}(g)\overline{U}^{(\nu)}_{k,l}(g) = \frac{\delta_{\mu,\nu}\delta_{i,k}\delta_{j,l}}{d_\mu} \tag{1.7}$$

where dg is the unique Haar measure over the group, bar denotes the complex conjugate and d_μ is the dimension of irrep μ. Furthermore, in the case of finite groups any function from G to $\mathbb{C}$ can be expanded as a linear combination of these functions. Also, in the case of compact Lie groups any continuous function from G to $\mathbb{C}$ can be uniformly approximated as a linear combination of these matrix elements.

This expansion of functions in terms of the matrix elements of projective unitary irreps is called the *generalized Fourier transform*. Note that for each cocycle of a group G there

exists a notion of generalized Fourier transform in which the functions over the group are expanded in terms of the matrix elements of the projective unitary irreps which all have that cocycle, and therefore are all in the same factor system. As we have defined above, (non-projective) unitary representations are a specific case of projective unitary representations for which the cocycle is trivial. So in particular, for any compact Lie group or finite group there is a unique generalized Fourier transform which corresponds to the (non-projective) unitary irreps of the group, i.e. the irreps for which the cocycle is trivial.

In many cases the cocycle of a projective unitary representation can be *lifted* in the sense that one can redefine the unitaries $\{U(g) : g \in G\}$ by multiplying them by a phase such that the new unitaries form a (non-projective) unitary representation of group and so the cocycle will be trivial. This is the case for all finite dimensional representations of simply connected Lie groups such as SU(2), the group of unitaries acting on $\mathbb{C}^2$ with determinant one. [2]. On the other hand, for Lie groups which are not simply connected such as SO(3), the cocycle cannot always be lifted. This is the case for all irreps of SO(3) with half-integer spin; they all have the same cocycle and this cocycle cannot be lifted. But, on the other hand, for all irreps of SO(3) with integer spin the cocycle is trivial and so they are all unitary irreps of SO(3).

This discussion implies that in the case of SO(3) there are two different notions of Fourier transform: One for the basis formed by the matrix elements of half-integer spin representations and the other for integer spin representations.

1.2 Symmetries of states

For any given symmetry group, there are some states which are invariant under some or all symmetry transformations in the group. For example, for any symmetry and for any representation of the symmetry, the completely mixed state is invariant under all symmetry transformations.

Definition 3 *The* symmetry subgroup *of a state ρ relative to the group G, denoted $Sym_G(\rho)$,*

[2] To see this first note that by redefining the cocycle one can always choose unitaries $\{U(g)\}$ to have determinant equal to one. Then by looking to the determinant of both sides of the Eq. (1.2) one finds that for all $g_1, g_2 \in G$, it holds that $\omega^d(g_1, g_2) = 1$ where d is the dimension of representation and so the values of $\omega(g_1, g_2)$ is discrete. Then using a simple continuity argument one can show that in the case of simply connected Lie groups the cocycle $\omega(g_1, g_2)$ should be constant and equal to one and so the cocycle can be lifted.

is the subgroup of G under which ρ is invariant,

$$Sym_G(\rho) \equiv \{g \in G : \mathcal{U}_g[\rho] = \rho\}. \tag{1.8}$$

If the symmetry subgroup contains only the identity element, it is said to be trivial. In this case, it is often said that the state has *no symmetries* (meaning no nontrivial symmetries). If the symmetry subgroup of a state ρ is the entire group G, so that it is invariant under all symmetry transformations $g \in G$, i.e.

$$\forall g \in G : \mathcal{U}_g(\rho) = \rho, \tag{1.9}$$

then we say that the state is *G-invariant* [3].

1.3 G-covariant operations

We say that a time evolution is *G-covariant* if it commutes with all symmetry transformations in the group G, that is, for any initial state and any symmetry transformation, the final state is independent of the order in which the symmetry transformation and the time evolution are applied [4]. We will sometimes refer to an operation that is G-covariant as a *symmetric* operation. (It is important not to confuse symmetr*y* transformations, which correspond to a particular group action, with symmetr*ic* transformations, which commute with all group actions.) We provide the rigorous form of the notion of G-covariance first for closed system evolutions and then for open system evolutions.

Closed system dynamics are described by unitary operators over the Hilbert space. However, noting that the global phase of a vector in Hilbert space has no physical significance, it is useful to describe the dynamics in terms of its effect on density operators (every parameter of which has physical significance). Closed system dynamics are then described by linear maps $\mathcal{V}$ on the operator space that are of the form $\mathcal{V}[\rho] = V\rho V^\dagger$, where V is a unitary operator. A closed system dynamics associated with the unitary V is G-covariant if

$$\forall g \in G, \forall \rho : VU(g)\rho U^\dagger(g)V^\dagger = U(g)V\rho V^\dagger U^\dagger(g), \tag{1.10}$$

[3] Because a symmetry transformation is defined not only by a group G but also by a representation U of that group, it would be more precise to call the symmetric states "{G,U}-invariant", however, for ease of readability, we do not specify the representation explicitly.

[4] Again, it would be more precise to call the symmetric operators "{G,U}-covariant", however, for ease of readability, we do not specify the representation explicitly.

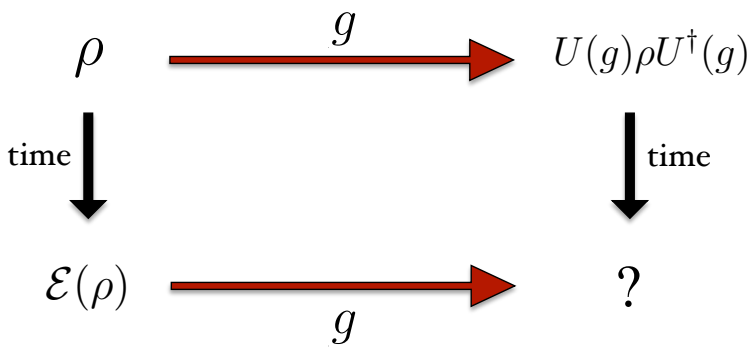

Figure 1.1: A time evolution is called G-covariant if the above transformations commute for all group elements $g \in G$.

or equivalently,

$$\forall g \in G : [\mathcal{V}, \mathcal{U}_g] = 0, \tag{1.11}$$

where $[\mathcal{V}, \mathcal{U}_g] := \mathcal{V} \circ \mathcal{U}_g - \mathcal{U}_g \circ \mathcal{V}$. In other words, the map $\mathcal{V}$ commutes with every element of the (superoperator) representation of the group $\{\mathcal{U}_g : g \in G\}$. This implies that

$$\forall g \in G : VU(g) = U(g)V\omega(g), \tag{1.12}$$

where $\omega(g)$ is a phase factor that can easily be shown to be a 1-dimensional representation of the group. In the case of finite-dimensional Hilbert spaces (which is the case under consideration in this thesis), we can argue that $\omega(g) = 1$ if the closed system dynamics is required to be continuous and symmetric at all times (in contrast to requiring only that the effective operation from initial to final time be symmetric) [20].

This argument justifies the common definition in the literature of when a closed system dynamics respects the symmetry, namely, when

$$\forall g \in G : VU(g) = U(g)V. \tag{1.13}$$

We call any unitary V which satisfies this property a *G-invariant unitary* because $\forall g \in G : U(g)VU^\dagger(g) = V$. More generally, any operator which commutes with the representation of group G on the Hilbert space of the system will be called G-invariant. Clearly, if a Hamiltonian is G-invariant then all the unitaries it generates are G-invariant. Finally, note that if V is an isometry rather than a unitary, then it is said to be G-invariant if $\forall g \in G : VU_{\text{in}}(g) = U_{\text{out}}(g)V$, where $U_{\text{in}}(g)$ and $U_{\text{out}}(g)$ are the representations of the group on the input and output spaces of the isometry.

In general, a system might be *open*, i.e., it may interact with an environment. In this case, the time evolution cannot be described by the Hamiltonian of the system alone. Rather, to describe the time evolution we need the Hamiltonian of system and environment together. In the study of open systems we usually restrict our attention to the situations where the initial state of the system and environment are uncorrelated, in which case we can describe the evolution by a deterministic quantum channel $\mathcal{E}$, that is, a *completely positive*[5], trace-preserving, linear map from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$ where $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ are the input and output Hilbert spaces and $\mathcal{B}(\mathcal{H})$ are the bounded operators on $\mathcal{H}$. After a time evolution described by quantum channel $\mathcal{E}$, the initial state ρ evolves to the final state $\mathcal{E}(\rho)$. Note that a general quantum channel may have input and output spaces that are distinct. This possibility is useful for describing transformations wherein the system of interest may grow (by incorporating into its definition parts of the environment) or shrink (by having some of its parts incorporated into the environment).

We now state the conditions for a general quantum operation (which may represent open or closed system dynamics) to be G-covariant.

Definition 4 (G-covariant operation) *The quantum operation $\mathcal{E}$ is said to be* G-covariant *if*

$$\forall g \in G: \ \mathcal{E}\left(U_{in}(g)(\cdot)U_{in}^{\dagger}(g)\right) = U_{out}(g)\mathcal{E}\left(\cdot\right)U_{out}^{\dagger}(g), \tag{1.14}$$

where $\{U_{in}(g) : g \in G\}$ and $\{U_{out}(g) : g \in G\}$ are the representations of G on the input and output Hilbert spaces of $\mathcal{E}$.

If the input and output spaces are equivalent, so that $\mathcal{E}$ is an automorphism, then the condition of G-covariance can be expressed as

$$\forall g \in G: \ \mathcal{E}\left(U(g)(\cdot)U^{\dagger}(g)\right) = U(g)\mathcal{E}\left(\cdot\right)U^{\dagger}(g), \tag{1.15}$$

or equivalently,

$$\forall g \in G : [\mathcal{E}, \mathcal{U}_g] = 0, \tag{1.16}$$

where $\mathcal{U}_g[\cdot] = U(g)(\cdot)U^{\dagger}(g)$.

As we demonstrate in appendix A.1, any G-covariant operation for which the input and output Hilbert spaces are different can always be modeled by one wherein the input and

[5]Let $\mathcal{K}$ be an arbitrary Hilbert space, $\mathcal{B}(\mathcal{K})$ be the space of bounded linear operators on $\mathcal{K}$ and $\mathbb{I}_{\mathcal{B}(\mathcal{K})}$ be the identity map on $\mathcal{B}(\mathcal{K})$. A map $\mathcal{E}$ from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$ is called *completely positive* if for any Hilbert space $\mathcal{K}$, $\mathcal{E} \otimes \mathbb{I}_{\mathcal{B}(\mathcal{K})}$ is a *positive* map, i.e. it maps positive operators in $\mathcal{B}(\mathcal{H}_{\text{in}}) \otimes \mathcal{B}(\mathcal{K})$ to positive operators in $\mathcal{B}(\mathcal{H}_{\text{out}}) \otimes \mathcal{B}(\mathcal{K})$.

output Hilbert spaces are the same. The reason is that the input and output Hilbert spaces can always be taken to be two different sectors of a single larger Hilbert space, $\mathcal{H}_{\text{in}} \bigoplus \mathcal{H}_{\text{out}}$, and any operation from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$ that is G-covariant relative to the representations $\{U_{\text{in}}(g)\}$ and $\{U_{\text{out}}(g)\}$ can always be extended to an operation on $\mathcal{B}(\mathcal{H}_{\text{in}} \bigoplus \mathcal{H}_{\text{out}})$ that is G-covariant relative to the representation $\{U_{\text{in}}(g) \bigoplus U_{\text{out}}(g)\}$. Similarly, any G-invariant isometry (a reversible operation where the input and output Hilbert spaces may differ) can always be modeld by a G-invariant unitary (where the input and output Hilbert spaces are the same). Again, this is shown in appendix A.1. It follows that without loss of generality, we can restrict our attention in the rest of this thesis to G-covariant operations where the input and output spaces are the same.

Clearly, G-covariant quantum operations include those induced by G-invariant unitaries, that is, operations of the form $\mathcal{V}(\cdot) = V(\cdot)V^\dagger$ where $\forall g \in G : [V, U(g)] = 0$. As another example, consider a channel of the form

$$\mathcal{K} \equiv \int_K dk \; \mathcal{U}_k, \tag{1.17}$$

where K is a subgroup of G and dk is the uniform measure over K. We refer to this as the *uniform twirling over* K [6]. The uniform twirling over any normal subgroup of G is a G-covariant operation. First, recall that if K is a normal subgroup of G then $\forall g \in G : gKg^{-1} = K$, where $gKg^{-1} \equiv \{gkg^{-1} : k \in K\}$. It follows that

$$\forall g \in G : \mathcal{U}_g \circ \mathcal{K} \circ \; \mathcal{U}_{g^{-1}} = \int_K dk \; \mathcal{U}_{gkg^{-1}} = \mathcal{K}, \tag{1.18}$$

and consequently that $\mathcal{K}$ is G-covariant. In particular any group is the normal subgroup of itself, therefore uniform twirling over any group G is a G-covariant channel.

Furthermore, if we couple the object system to an environment using a Hamiltonian which has the symmetry G and if the environment is initially uncorrelated with the system and prepared in a state that is G-invariant, and finally some proper subsystem is discarded, then the total effect of this time evolution is described by a G-covariant quantum operation. (Intuitively this is clear, because there is nothing in such a dynamics that can break the symmetry.)

As it turns out, *every* G-covariant quantum operation can in fact be realized in this way, i.e. by first coupling the system to an uncorrelated environment in a G-invariant state via a G-invariant unitary and secondly discarding a proper subsystem of the total system.

[6] Note that we can implement the time evolution described by the channel $\mathcal{K}$ by choosing one of the unitaries from the set $\{U(k), k \in K\}$ uniformly at random and applying it to the system.

This is sometimes called Stinespring dilation theorem for G-covariant channels and is first proved in [48]. We also provide a different proof of this in section 4.4. This result provides an operational prescription for realizing every such operation.

In the first part of this thesis we study the consequences of the fact that a (possibly open) dynamics has a symmetry. In particular, we are interested to know, for a given initial state of a G-covariant dynamics, which kind of constraints one can put on the possible final states based on the symmetries of dynamics. Equivalently, we are interested to know, for a given pair of states ρ and σ, whether there exists a G-covariant dynamics which transforms ρ to σ or not. We use the notation $\rho \xrightarrow{\text{G-cov}} \sigma$ to show that state ρ can be transformed to state σ under a G-covariant time evolution.

For instance, a simple consequence of the symmetry of dynamics is that every symmetry of the initial state is a symmetry of the final state, i.e.

Proposition 5 *If ρ transforms to σ by a G-covariant quantum operation ($\rho \xrightarrow{G\text{-}cov} \sigma$), then $Sym_G(\rho) \subseteq Sym_G(\sigma)$.*

Proof. If $g_s \in G$ is a symmetry of ρ then $\mathcal{U}_{g_s}(\rho) = \rho$. Since the operation $\mathcal{E}$ taking ρ to σ is G-covariant, it follows that

$$\mathcal{E}(\rho) = \mathcal{E} \circ \mathcal{U}_{g_s}(\rho) = \mathcal{U}_{g_s} \circ \mathcal{E}(\rho)$$

So $\mathcal{U}_{g_s}(\sigma) = \sigma$. ■

In particular, therefore, one cannot generate an asymmetric state starting from a symmetric one, and one cannot transform a state with one kind of asymmetry to a state with another. For instance, rotationally-covariant time evolutions cannot transform a spin pointing along $\hat{z}$ to one pointing along $\hat{x}$.

On the other hand, for any arbitrary pair of G-invariant states ρ and σ there always exists G-covariant channels which transform one to the other. A trivial instance of these G-covariant channels, is the one which discards the input state and generates the G-invariant state σ as the output, i.e. the channel described by

$$\mathcal{E}_\sigma(X) = \text{tr}(X)\sigma \tag{1.19}$$

In part one of this thesis we introduce ideas and tools which enable us to find consequences that are far less obvious. In the rest of this chapter we present two physical examples of channels which are covariant with respect to the group U(1), the group formed by all phases $\{e^{i\theta} : \theta \in (0, 2\pi]\}$.

1.4 Example: U(1)-covariant channels

For concreteness, it is worth examining a specific example of symmetric operations, namely, those that are covariant under a unitary representation of the U(1) group. Here, we present two different physical scenarios in which a restriction to U(1)-covariant channels is natural.

1.4.1 Axially symmetric channels

U(1)-covariant quantum operations are relevant for describing a dynamics which has rotational symmetry around some axis, or *axially symmetric* dynamics. The set of all rotations around a fixed axis forms the group called SO(2) which is isomorphic to the group U(1). So the unitary representation of the rotations around a fixed axis forms a representation of U(1), e.g. if L_z is the operator of angular momentum in the z direction then

$$e^{i\theta} \to e^{i\theta L_z}$$

is a representation of the group $U(1)$. In general the eigenvalues of L_z are degenerate. But to simplify the notation here we assume L_z has no degeneracy. So $\{|m\rangle : m \in \{-j, -j+1, \cdots, j\}\}$, the eigenbasis of L_z, is a basis for the Hilbert space of the system, where j is the angular momentum of the system and so is either half integer or integer and where $L_z|m\rangle = m|m\rangle$ (assuming $\hbar$ is one). Note that in the case of half-integer spins the representation $e^{i\theta} \to e^{i\theta L_z}$ is not a (non-projective) unitary representation, i.e. the cocycle of the representation is non-trivial.

First, we consider the symmetries of a few different states. The state $(|0\rangle + |1\rangle)/\sqrt{2}$ has no symmetries, while the state $(|0\rangle + |2\rangle)/\sqrt{2}$ has a nontrivial symmetry subgroup because it is invariant under a π phase shift. Meanwhile, all the elements of the basis $\{|m\rangle : m \in \{-j, -j+1, \cdots, j\}\}$ are U(1)-invariant states. The set of all states (pure and mixed) that are U(1)-invariant are those which commute with all elements of the set $\{\exp(i\theta L_z) : \theta \in (0, 2\pi]\}$ and so commute with L_z and are therefore diagonal in the $\{|m\rangle : m \in \{-j, -j+1, \cdots j\}\}$ basis.

Next we consider symmetric operations. First note that the U(1)-invariant unitaries are those that are diagonal in the $\{|m\rangle : m \in \{-j, -j+1, \cdots j\}\}$ basis and are therefore of the form

$$V_{\text{U(1)-inv}} = \sum_{m=-j}^{j} e^{i\beta_m} |m\rangle\langle m| \tag{1.20}$$

These unitaries all commute with each other. (Note, however, that if there is multiplicity in the representations, then the U(1)-invariant unitaries have a more complicated structure and do not necessarily commute with each other.)

Now one can easily see that using U(1)-invariant unitaries we cannot transform one arbitrary state to another. For example, we cannot transform $|0\rangle$ to $(|0\rangle+|1\rangle)/\sqrt{2}$: The first state is a symmetric state while the second has some asymmetry. Similarly we can easily see that $(|0\rangle+|1\rangle)/\sqrt{2}$ cannot be transformed to $(|2\rangle+|3\rangle)/\sqrt{2}$ using U(1)-invariant unitaries. However, this transformation *is* possible using a U(1)-covariant channel. Consider the quantum operation $\mathcal{E}$ described by the following Kraus operators:

$$K_0 = \sum_{m=-j}^{j-1} |m+1\rangle\langle m|, \quad \text{and} \quad K_1 = |-j\rangle\langle j|$$

where $K_0^\dagger K_0 + K_1^\dagger K_1 = I$. One can easily check that this quantum operation is invariant under rotations around $\hat{z}$, i.e.

$$\forall \theta \in (0, 2\pi] : \ \mathcal{E}(e^{i\theta L_z} \rho e^{-i\theta L_z}) = e^{i\theta L_z} \mathcal{E}(\rho) e^{-i\theta L_z}. \tag{1.21}$$

Furthermore, it maps the state $(|m-1\rangle+|m\rangle)/\sqrt{2}$ to $(|m\rangle+|m+1\rangle)/\sqrt{2}$ for all $m < j$. So, although the transformation is not possible via U(1)-invariant unitaries, it can be done by U(1)-covariant quantum operations. Similarly we can show that there is a U(1)-covariant quantum operation which transforms $(|m\rangle + |m+1\rangle)/\sqrt{2}$ to $(|m-1\rangle + |m\rangle)/\sqrt{2}$.

1.4.2 Phase-invariant channels in quantum optics

Another physical example of $U(1)$-covariant quantum operations comes from quantum optics (for more discussion see [1]). Consider a harmonic oscillator whose Hilbert space is spanned by the orthonormal basis $\{|n, \alpha\rangle : n \in \mathbb{N}\}$ with the number operator N such that $N|n, \alpha\rangle = n|n, \alpha\rangle$ where n is a nonnegative integer and α labels possible degeneracies. Then the operator which shifts this oscillator in its cycle by phase θ is $\exp(i\theta N)$. For example, this operator transforms the coherent state $|\gamma\rangle$ to $|e^{i\theta}\gamma\rangle$.

Now a quantum operation $\mathcal{E}$ is phase-invariant if

$$\forall \theta \in (0, 2\pi] : \ \mathcal{E}(e^{i\theta N} \rho e^{-i\theta N}) = e^{i\theta N} \mathcal{E}(\rho) e^{-i\theta N}. \tag{1.22}$$

This example shows that for a particular physical scenario, there may be additional constraints on the accessible states and unitaries beyond those that are implied by the

symmetry. For instance, here in this example, unlike the previous example, there is no invariant state which under the action of the symmetry group transforms as $e^{iN\theta}|\psi\rangle = e^{-i\theta}|\psi\rangle$; all eigenvalues of the number operator are non-negative. This is a restriction relative to what occurs for our first example where to realize a particular axially symmetric operation an experimenter can couple the system to an ancilla in state $\{|m\rangle\}$ for arbitrary positive or negative m.

However, it turns out that a restriction of the accessible irreps of U(1) to the nonnegative does not have any impact on the set of operations one can implement – all U(1)-covariant operations are still physically accessible. In other words, any phase-invariant quantum operation can be realized by coupling the system to another ancillary system which is initially in $|n\rangle$ for some non-negative n and the coupling can be chosen to be a phase-invariant unitary. This follows from our constructive proof of Stinespring dilations of G-covariant channels in section 4.4. For the rest of this thesis, we will assume that all G-covariant operations are physically accessible (including in the quantum optics examples).

Chapter 2

Asymmetry of quantum states

The *asymmetry properties* of a state relative to some symmetry group specify how and to what extent the given symmetry is broken by the state. Characterizing these is found to be surprisingly useful for addressing a very common problem: to determine what follows from a system's dynamics (possibly open) having that symmetry. In this chapter we formally define the notion of asymmetry of state and demonstrate that the asymmetry properties of a state can be understood in terms of information-theoretic concepts.

2.1 G-equivalence classes of states under symmetric operations

The first step in characterizing asymmetry is to specify when two states have the same asymmetry. We stipulate that this is the case when the pair of states can be *reversibly interconverted* one to the other by symmetric operations. This defines an equivalence relation among states.

Definition 6 (G-equivalence of states) *Two states, ρ and σ are said to be* G-equivalent *if and only if they are reversibly interconvertible by G-covariant operations, i.e., there exists a quantum operation $\mathcal{E}$ such that*

$$\forall g \in G : [\mathcal{E}, \mathcal{U}_g] = 0, \quad \textit{and} \quad \mathcal{E}[\rho] = \sigma, \tag{2.1}$$

and there exists a quantum operation $\mathcal{F}$ such that

$$\forall g \in G : [\mathcal{F}, \mathcal{U}_g] = 0, \quad \textit{and} \quad \mathcal{F}[\sigma] = \rho. \tag{2.2}$$

(Using the notation we introduced in chapter 1, ρ and σ are G-equivalent iff $\rho \xrightarrow{\text{G-cov}} \sigma$ and $\sigma \xrightarrow{\text{G-cov}} \rho$.)

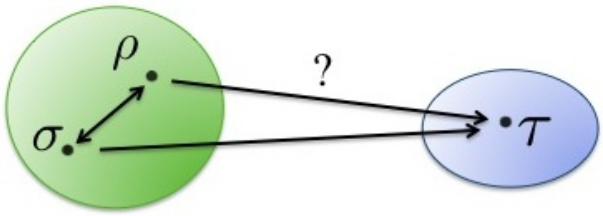

Figure 2.1: A depiction of two G-equivalence classes in the space of all states. Because both $\rho \xrightarrow{\text{G-cov}} \sigma$ and $\sigma \xrightarrow{\text{G-cov}} \rho$ are possible, ρ and σ are in the same class. It follows that if $\rho \xrightarrow{\text{G-cov}} \tau$ then $\sigma \xrightarrow{\text{G-cov}} \tau$.

A complete specification of the G-asymmetry properties of a state is achieved by specifying its G-equivalence class. So, for example specifying G-equivalence class of a state should include a specification of the state's symmetries (indeed, this can be considered to be a condition that must be satisfied by any proposed specification of the asymmetry properties). To see this first note that, as it is highlighted in proposition 5, if ρ can be transformed to σ by a G-covariant quantum operation ($\rho \xrightarrow{\text{G-cov}} \sigma$), then $\text{Sym}_G(\rho) \subseteq \text{Sym}_G(\sigma)$ where $\text{Sym}_G(\rho)$ is the subgroup of G which leaves ρ invariant as defined in 3. So if ρ and σ are G-equivalent, i.e. both $\rho \xrightarrow{\text{G-cov}} \sigma$ and $\sigma \xrightarrow{\text{G-cov}} \rho$ exists then $\text{Sym}_G(\rho) = \text{Sym}_G(\sigma)$.

As another example, if we want to know whether there exists a one-way (deterministic or stochastic) symmetric transformation from one given state to another, all we need to know is the G-equivalence class of the two states; if there exists a symmetric transformation from one member of class I to one member of class II, then there exists a symmetric transformation from every member of class I to every member of class II. So to answer the question of whether a given state can evolve to another state under a G-covariant dynamics, the only properties of the two states which are relevant are their G-asymmetry properties.

The above definition of asymmetry properties is based on the intuition that asymmetry is something which cannot be generated by symmetric time evolutions. We call this the *constrained-dynamical* perspective.

In the constrained-dynamical point of view, we characterized the asymmetry properties of a state as those features that are required to determine whether any pair of states are reversibly interconvertible by symmetric operations.

It seems natural in this point of view, to use dynamical concepts to describe and study asymmetry. For example if the symmetry group under consideration is the rotation group, then we may use angular momentum to describe asymmetry: we know that if the expectation value of any component of the angular momentum is nonzero then the state necessarily breaks the rotational symmetry and so is asymmetric. Moreover according to Noether's theorem, in an isotropic closed time evolution every component of the angular momentum is conserved. We can generalize this result to symmetric reversible transformations on open systems using a Carnot style of argument — in a reversible transformation the environment cannot be a source of angular momentum and therefore if a transformation can be achieved reversibly on the system alone, then it must conserve all components of angular momentum (on pain of allowing a cycle that generates arbitrary amounts of angular momentum). It follows that the expectation value of angular momentum is a function of the G-equivalence class, i.e. it is the same for all states in the same G-equivalence class.

So clearly, the dynamical concepts provide a useful framework for describing asymmetry. In the next section we introduce an alternative point of view to asymmetry which implies that information theoretic concepts are also useful for the study of asymmetry.

2.1.1 Information theoretic point of view to asymmetry

In this section we introduce another perspective to the notion of asymmetry of states which we call it *information-theoretic* perspective. Recall that a quantum state breaks a symmetry, say rotational symmetry, if for some non-trivial rotations, the rotated version of the state is not the same as the state itself, i.e. they are distinguishable. In this case, the ensemble of states corresponding to the orbit of the state under rotations can act as an encoding when the message to be encoded is an element of the rotation group. This suggest that information-theoretic concepts are also useful for the study of asymmetry.

Consider a set of communication protocols in which one chooses a message $g \in G$ according to a measure over the group and then sends the state $\mathcal{U}_g[\rho]$ where ρ is some fixed state. The goal of the sender is to inform the receiver about the specific chosen group element. We claim that the asymmetry properties of a state ρ can be defined as those that determine the effectiveness of using the signal states $\{\mathcal{U}_g[\rho] : g \in G\}$ to communicate a message $g \in G$. To get an intuition for this, note that if ρ is invariant under the effect of some specific group element h then the state used for encoding h would be the same as the state used for encoding the identity element e, $(\mathcal{U}(h)[\rho] = \mathcal{U}(e)[\rho] = \rho)$, such that the message h cannot be distinguished from e. In the extreme case where ρ is invariant under all group elements this encoding does not transfer any information.

So from this point of view, the asymmetry properties of ρ can be inferred from the information-theoretic properties of the encoding $\{\mathcal{U}_g[\rho] : g \in G\}$. To compare the asymmetry properties of two arbitrary states ρ and σ, we have to compare the information content of two different encodings: $\{\mathcal{U}_g[\rho] : g \in G\}$ (encoding I) and $\{\mathcal{U}_g[\sigma] : g \in G\}$ (encoding II). If each state $\mathcal{U}_g[\rho]$ can be converted to $\mathcal{U}_g[\sigma]$ for all $g \in G$, then encoding I has as much or more information about g than encoding II. If the opposite conversion can also be made, then the two encodings have precisely the same information about g. Consequently, in an information-theoretic characterization of the asymmetry properties, it is the reversible interconvertability of the sets (defined by the two states) that defines equivalence of their asymmetry properties.

As it turns out, our two different approaches lead to the same definition of asymmetry properties, as the following lemmas imply.

Lemma 7 *The following statements are equivalent:*
***A**) There exists a G-covariant quantum operation $\mathcal{E}_{G\text{-}cov}$ [as defined in Eq. (1.15)] which maps ρ to σ, i.e., $\mathcal{E}_{G\text{-}cov}(\rho) = \sigma$*
***B**) There exists a quantum operation $\mathcal{E}$ which maps $\mathcal{U}_g[\rho]$ to $\mathcal{U}_g[\sigma]$ for all $g \in G$, i.e.,*

$$\forall g \in G : \quad \mathcal{E}(\mathcal{U}_g[\rho]) = \mathcal{U}_g[\sigma]. \tag{2.3}$$

For pure states, we have

Lemma 8 *The following statements are equivalent:*
***A**) There exists a G-invariant unitary $V_{G\text{-}inv}$ (i.e. $\forall g \in G : \ [V_{G\text{-}inv}, U(g)] = 0$) which maps $|\psi\rangle$ to $|\phi\rangle$, i.e. $V_{G\text{-}inv}|\psi\rangle = |\phi\rangle$.*
***B**) There exists a unitary operation V which maps $U(g)|\psi\rangle$ to $U(g)|\phi\rangle$ for all $g \in G$, i.e.,*

$$\forall g \in G : \quad VU(g)|\psi\rangle = U(g)|\phi\rangle. \tag{2.4}$$

Note that in both of these lemmas, the condition **A** concerns whether it is possible to transform a single state to another under a limited type of dynamics. On the other hand, in the **B** condition, there is no restriction on the dynamics, but now we are asking whether one can transform a *set* of states to another set.

Adopting the latter perspective enables us to use the machinery of quantum information theory to study asymmetry and, via the lemmas, the consequences of symmetric dynamics. We will see examples of this technique in the rest of this thesis. In particular, in chapter 3 we use information theoretic approach to quantify the amount of asymmetry of states.

Furthermore, in chapter 6 we will find the characterization of the G-equivalence classes of pure states using both the constrained-dynamical and the information-theoretic approaches and we will show how these two characterizations are in fact equivalent via the Fourier transform. Also in the next section we explain how these two different perspectives on asymmetry naturally arise in the study of uncorrelated reference frames. First however, we present the proofs of the lemmas.

Proof. (Lemma 7) **A** can be seen to imply **B** by taking $\mathcal{E} = \mathcal{E}_{\text{G-cov}}$. To show the reverse, note that **B** implies the existence of a quantum operation $\mathcal{E}$ which satisfies Eq. (2.3). Now we can define

$$\mathcal{E}' \equiv \int dg\, \mathcal{U}_g^\dagger \circ \mathcal{E} \circ \mathcal{U}_g \tag{2.5}$$

One can then easily check that $\mathcal{E}'$ is a G-covariant operation and that $\mathcal{E}'(\rho) = \int dg\, \mathcal{U}_g^\dagger \circ \mathcal{E} \circ \mathcal{U}_g(\rho) = \int dg\, \mathcal{U}_g^\dagger \circ \mathcal{U}_g(\sigma) = \sigma$, such that we can choose $\mathcal{E}_{\text{G-cov}} = \mathcal{E}'$. So **B** also implies **A**. ■

Proof. (Lemma 8) **A** can be seen to imply **B** by taking $V = V_{\text{G-inv}}$. In the following we prove that **B** also implies **A**. Assume there exists a unitary V such that $\forall g \in G$,

$$VU(g)|\psi\rangle = U(g)|\phi\rangle. \tag{2.6}$$

First note that this implies $|\phi\rangle = V|\psi\rangle$. Furthermore it implies that for all $g, h \in G$ we have

$$\begin{aligned} VU(g)U(h)|\psi\rangle &= \omega(g,h)VU(gh)|\psi\rangle \\ &= \omega(g,h)U(gh)|\phi\rangle \\ &= U(g)U(h)|\phi\rangle \\ &= U(g)VU(h)|\psi\rangle \end{aligned}$$

where we have used the fact that $g \to U(g)$ is a projective representation of G and so $U(g)U(h) = \omega(g,h)U(gh)$ for a phase $\omega(g,h)$. Now suppose Π is the projector to the subspace spanned by all the vectors $\{U(h)|\psi\rangle, \forall h \in G\}$. Then the above equation implies that

$$\forall g \in G: \; VU(g)\Pi = U(g)V\Pi. \tag{2.7}$$

Now by definition of the projector Π it is clear that it commutes with all $\{U(g) : g \in G\}$. So the above equation implies

$$\forall g \in G : [V\Pi, U(g)] = 0. \tag{2.8}$$

The operator $V\Pi$ unitarily maps a subspace of the Hilbert space to another subspace and it commutes with all $\{U(g)\}$. Using lemma 91 we conclude that this G-invaraint isometry can always be extended to a G-invariant unitary $V_{\text{G-inv}}$ such that $V_{\text{G-inv}}\Pi = V\Pi$ and therefore

$$V_{\text{G-inv}}U(g)|\psi\rangle = V\Pi U(g)|\psi\rangle = U(g)|\phi\rangle. \tag{2.9}$$

■

2.1.2 Interpreting the two points of view in terms of uncorrelated reference frames

Interestingly these two points of view to asymmetry naturally arise in the study of a communication scenario when the two distant parties lack a shared reference frame for some degree of freedom.

Specifically, consider a degree of freedom that transforms according to the group G. Passive transformations of the reference frame for this degree of freedom will then also be described by the group G, as will the relative orientation of any two such frames. Consider two parties, Alice and Bob, that each have a local reference frame but where these are related by a group element $g \in G$ that is unknown to either of them. For instance, they might each have a local Cartesian frame, but do not know their relative orientation. (See Ref. [1] for a discussion.)

Now consider the following state interconversion task. Alice prepares a system in the state ρ relative to her local reference frame and sends it, along with a classical description of ρ, to Bob. She also sends him a classical description of a state σ, and asks him to try and implement an operation that leaves the system in the state σ relative to her local frame. In effect, Alice is asking Bob to transform ρ to σ but without the benefit of having a sample of her local reference frame. For instance, she may ask him to transform a spin aligned with her $\hat{z}$-axis to one that is aligned with her $\hat{y}$-axis. We consider how the task is described relative to each of their local frames.

Description relative to Alice's frame. In this case, the initial and final states, ρ and σ, are described relative to Alice's frame. If the operation that Bob implements is described as $\mathcal{E}$ relative to his frame, then it would be described as $\mathcal{U}^\dagger(g) \circ \mathcal{E} \circ \mathcal{U}_g$ relative to Alice's frame by someone who knew which group element g connected their frames. However, since g is unknown to Alice and Bob, they describe the operation relative to Alice's frame by the uniform mixture of such operations, i.e., by $\int dg \mathcal{U}_g \circ \mathcal{E} \circ \mathcal{U}_g^\dagger$. It is straightforward to check that this quantum operation is G-covariant. So all the operations

that Bob can implement are described relative to Alice's frame as G-covariant operations. From this perspective, the interconversion can be achieved only if ρ can be mapped to σ by a G-covariant quantum operation.

Description relative to Bob's frame. The initial state is described as $\mathcal{U}_g[\rho]$ relative to Bob's frame. Bob must implement an operation that transforms this to a state which is described as $\mathcal{U}_g[\sigma]$ relative to his frame. But the group element g that connects Alice's to Bob's frames is unknown, therefore the transformation is required to succeed regardless of g. Bob can implement any operation relative to his own frame and so the set of operations to which he has access is unrestricted. The question, therefore, is whether there exists an operation $\mathcal{E}$ such that $\forall g \in G : \mathcal{E}\left[\mathcal{U}_g[\rho]\right] = \mathcal{U}_g[\sigma]$. In other words, from this perspective the interconversion task can be achieved only if every element of the set $\{\mathcal{U}_g[\rho] \mid g \in G\}$ can be mapped to the corresponding element of $\{\mathcal{U}_g[\sigma] \mid g \in G\}$ by some quantum operation.

We see therefore that the constrained-dynamical and information-theoretic points of view to the manipulation of asymmetry arise naturally as Alice's and Bob's points of view respectively. They constitute the descriptions of a single interconversion task relative to two different reference frames.

2.2 The resource theory point of view

We can think of the study of asymmetry as *a resource theory*. Any resource theory is specified by a convex set of free states and a semi-group of free transformations (which are required to map the set of free states to itself). Any non-free state is called a *resource*. The resource theory is the study of manipulations of resources under the free transformations. As we will explain, there are several types of questions and arguments which are relevant for all resource theories and so this point of view can help to achieve a better understanding of a specific resource theory by emphasizing its analogies with other resource theories.

A well-known example of a resource theory is the theory of entanglement. The free transformations in this case are those which can be implemented by local operations and classical communications (LOCC) (See [15] for a review of entanglement theory). The set of free states is the set of unentangled states. This set is closed under LOCC, i.e. an unentangled state cannot be transformed to an entangled one via LOCC [17]. More generally, given two quantum states one cannot necessarily transform the first one to the second with LOCC. Here the relevant properties of the states which determine whether such a transformation is possible or not are their entanglement properties. In the case of pure bipartite states it is a well-known fact that the entanglement properties of a state are

uniquely specified by its Schmidt coefficients [17]. For example, Nielsen's theorem provides the necessary and sufficient condition for the existence of LOCC operations which transform one given state to another in terms of their Schmidt coefficients [56]. Entangled states are also a resource in the sense that they can be used to implement tasks that are impossible by LOCC and unentangled states alone. For example, one can use entangled states for teleportation, which can be interpreted as consuming a resource (entanglement) to simulate a non-free transformation (a quantum channel) via free transformations (LOCC).

Similarly, we can think of the study of asymmetry relative to a given representation of a group G as a resource theory. In this resource theory the time evolutions which respect the symmetry (G-covariant time evolutions) are free transformations and the states which do not break the symmetry (G-invariant states) are the free states. This is a consistent choice because G-covariant time evolutions form a semi-group under which the set of G-invariant states is mapped to itself. Similarly to entanglement theory, a resource (an asymmetric state) can be used to simulate a non-free transformation (non-G-covariant time evolution) via a free transformation (G-covariant time evolution).

In the resource theory of asymmetry, we seek to classify different types of resources and to find the rules governing their manipulations. For every question in entanglement theory, it is useful to ask whether there is an analogous question in the resource theory of asymmetry. In chapter 6, we will show that all the asymmetry properties of a pure state ψ relative to the group G and the projective unitary representation $\{U(g), g \in G\}$ are specified by its *characteristic function* $\chi_\psi(g) \equiv \langle\psi|U(g)|\psi\rangle$. This is analogous to how all the entanglement properties of a pure bipartite state are specified by its Schmidt coefficients. Also in the next chapter we study *asymmetry monotones* (or measures of asymmetry) a notion which can be thought as the analogous of entanglement monotones.

Asymmetry theory	**Entanglement theory**
Restriction to G-cov	Restriction to LOCC
$\rho \xrightarrow{\text{G-cov}} \sigma$	$\rho \xrightarrow{\text{LOCC}} \sigma$
Asymmetry properties	Entanglement properties
Asymmetry monotones	Entanglement monotones
$\vdots$	$\vdots$

Analogies of asymmetry theory and entanglement theory

Chapter 3

Asymmetry monotones

In this chapter we study *asymmetry monotones* or, equivalently measures of asymmetry. Any asymmetry monotone quantifies how much the symmetry is broken by a given state. As we have mentioned before, they can be thought as the analogous of entanglement monotones in the resource theory of entanglement. The defining property of an asymmetry monotone is that it must be non-increasing under G-covariant time evolutions. This definition captures the intuition that asymmetry is a property of states which cannot be generated by symmetric dynamics.

We introduce a recipe for constructing asymmetry monotones which is based on the information theoretic point of view to asymmetry described in the previous chapter. Using this recipe we find some interesting asymmetry monotones.

Asymmetry monotones can be useful tools for finding the consequences of the symmetries of a dynamics. For open system dynamics, where the standard tools such as Noether's theorem make no predictions, every asymmetry monotone imposes a non-trivial constraint on what state transitions are possible under the symmetric dynamics, namely that the measure of asymmetry of the final state be no larger than that of the initial state. For closed system dynamics, each asymmetry monotone is a conserved quantity under the symmetric dynamics, i.e. a constant of the motion. We show that for transitions between mixed states, the conserved quantities one obtains in this way are generally independent of those prescribed by Noether's theorem and therefore impose new constraints.

3.1 Definition

A G-asymmetry monotone quantifies how much the symmetry described by group G is broken by a given state. Since symmetric dynamics cannot generate asymmetry, any measure of asymmetry should be non-increasing under this type of dynamics. We take this as the defining property of asymmetry monotones.

Definition 9 *A function F from states to real numbers is an asymmetry monotone if $\rho \xrightarrow{G\text{-}cov} \sigma$ implies $F(\rho) \geq F(\sigma)$.*

Here in this definition $\rho \xrightarrow{\text{G-cov}} \sigma$ means that there exists a G-covariant channel which transforms state ρ to state σ. Note that, as the notion of G-covariance of channels depends on the specific representation of the symmetry group G, the G-asymmetry monotones are also defined only when we specify the representation of the symmetry on the space. In other words, one can think of an asymmetry monotone $F(\rho)$ as a function of the density operator and the representation of group together, i.e. $F\left(\rho, g \to U(g)\right)$. This is analogous to the fact that in the entanglement theory one can define an entanglement monotone as a function of states only when the partitioning of a system to the subsystems is specified.

Any pair of G-invariant states can be transformed to each other under G-covariant channels. So with respect to any G-asymmetry monotone all G-invariant states should have the same amount of asymmetry. For any G-asymmetry monotone, we usually adopt the convention that the amount of G-asymmetry of all G-invariant states should be zero . So, in this convention, the asymmetry of any state is non-negative.

Example 10 *Here, we present an example of a family of asymmetry monotones which we call the* Holevo asymmetry monotones *(the reason will become clear later).*

For any arbitrary probability distribution $p(g)$ over a group G, define

$$\Gamma_p(\rho) \equiv S\left(\mathcal{G}_p(\rho)\right) - S(\rho) \tag{3.1}$$

where $S(\sigma) \equiv -tr(\sigma \log \sigma)$ is the von Neumann entropy *of state σ and*

$$\mathcal{G}_p(X) \equiv \int dg\ p(g)\ \mathcal{U}_g(X). \tag{3.2}$$

We prove in section 3.4.3 that for any probability distribution $p(g)$, Γ_p is a G-asymmetry monotone. [1] *Note that for any G-invariant state ρ and any arbitrary probability distribu-*

[1] In the particular case where the probability distribution $p(g)$ is uniform over group G the monotonicity of $\mathcal{G}_p$ under G-covariant channels has been previously proved in [22] using a different type of argumnet.

tion $p(g)$, $\Gamma_p(\rho) = 0$. Also, note that for any probability distribution $p(g)$ which is nonzero for all G, and for any state which breaks the symmetry G, $\Gamma_p(\rho) \neq 0$.

In the case of closed system dynamics (i.e. unitary dynamics) any G-covariant dynamics can be reversed via another G-covariant dynamics: If a unitary V is G-invariant, i.e. $\forall g \in G : [V, U(g)] = 0$, then the unitary $V^\dagger$ is also G-invariant, i.e. $\forall g \in G : [V^\dagger, U(g)] = 0$. This implies that

Proposition 11 *During any closed system dynamics which is invariant under the representation $g \to U(g)$ of symmetry G, any G-asymmetry monotone defined in terms of $g \to U(g)$ is a constant of motion.*

We will show that in the case of mixed states these new constants of motion can put new constraints that are totally independent of the conservation laws that are implied by Noether's theorem. On the other hand, in general when the system is not closed any asymmetry measure puts a necessary condition on the possibility of $\rho \xrightarrow{\text{G-cov}} \sigma$.

3.1.1 Previous work

Previous work on asymmetry monotones has been mostly inspired by the notion of entanglement monotones. The first example of an asymmetry monotone was introduced in [22]. This monotone, which was called the *asymmetry of a state* in [22], is what we call a Holevo asymmetry monotone for the special case where the probability distribution over group is uniform.

Also, earlier related works have been done in the context of bipartite systems where two distant parties are under a U(1)-superselection rule motivated by a particle number conservation law [23, 24]. This superselection rule implies that all the local operations should be invariant under a representation of the group U(1). Then, it is shown in [24] and [23] that adding a superselection rule to a bipartite system leads to an additional resource which can be quantified by a measure called the *superselection induced variance (SiV)*. They show that SiV and entropy of entanglement together completely characterize bipartite pure states in the asymptotic limit.

It is worth emphasizing the difference between the context of the problems studied in [23] and [24] and the problem we study in this thesis. In the problem studied in these papers, the assumption of a superselection rule implies all states and operations that one party has should be symmetric. So, in this context the unipartite problem is trivial.

Since there is no unipartite state that breaks the symmetry it follows that all states can be transformed into each other under the dynamics that are allowed by the superselection rule. But, as is clarified in [16], if the origin of the superslection rule is a *practical* constraint, such as the lack of a shared reference frame, then although the only operations a party can perform locally, may be symmetric operations, nevertheless the states of local systems are not necessarily symmetric and so even in the unipartite case the problem of interconversion of states under allowed operations is non-trivial.

More recently, the notion of asymmetry monotones has been studied in [16] under the name of *frameness monotones*. In this paper the authors provide a classification of different notions of frameness monotones. In this classification the functions which we call *asymmetry monotones* are called *deterministic frameness monotones*. Also, in this paper for specific groups such as Z_2 and $U(1)$, the authors introduce functions from states to real numbers which are non-increasing in any interconversion of a pure state to another pure state under symmetric operations. Because of the restriction to pure states, they are not strictly speaking asymmetry monotones in the terminology of this thesis.

To find more recent works on different aspects of asymmetry monotones also check [26], [27] and [6].

3.2 Are asymmetry monotones convex?

One may think that any asymmetry monotone should be a convex function, i.e.

$$F(p\rho_1 + (1-p)\rho_2) \leq pF(\rho_1) + (1-p)F(\rho_2) \tag{3.3}$$

for any $0 \leq p \leq 1$. The intuition is that mixing states should not increase asymmetry. But it turns out that asymmetry monotones are not necessarily convex. For example, if F_1 and F_2 are two G-asymmetry monotones which are always non-negative for all states then the product F_1F_2 is also a G-asymmetry monotone. Now, one can easily choose monotones F_1 and F_2 such that F_1F_2 is not convex even though F_1 and F_2 might be convex. For example, consider the case of G=SO(3) and consider two monotones Γ_{p_z} and Γ_{p_x} where Γ_{p_z} (Γ_{p_x}) is the Holevo asymmetry monotone in the case of probability distribution p_z (p_x)the uniform distribution over all rotations around the $\hat{z}(\hat{x})$ axis. Then, for all states which are invariant under rotations around the $\hat{z}$ ($\hat{x}$) the value of monotone Γ_{p_z} (Γ_{p_x}) is zero. This implies that for any state which is either invariant under all rotations around the $\hat{z}$ axis or all rotations around $\hat{x}$ axis the monotone $F(\rho) \equiv \Gamma_{p_z}(\rho)\Gamma_{p_x}(\rho)$ is zero. But, the convex combination of a state which is invariant under rotations around the $\hat{z}$ axis and a state which is invariant

under rotations around the $\hat{x}$ can be non-invariant under all rotations. Based on this observation one can show that the monotone defined by $F(\rho) \equiv \Gamma_{p_z}(\rho)\Gamma_{p_x}(\rho)$ is not a convex function.

It is worth mentioning that the intuition that mixing should not increase asymmetry is correct. However, as it is clarified by Plenio in [29] its mathematical statement does not correspond to the convexity of entanglement (or in this case asymmetry) monotones. The right mathematical way to state this condition is the following

$$F\left(p\rho_1 + (1-p)\rho_2\right) \leq F\left(p|1\rangle\langle 1| \otimes \rho_1 + (1-p)|2\rangle\langle 2| \otimes \rho_2\right) \tag{3.4}$$

where $|1\rangle$ and $|2\rangle$ are two orthogonal states of an ancillary system which are invariant under symmetry. This ancilla is used to label the states of system. But since partial trace is a completely positive G-covariant map it follows that for any symmetry G this notion of convexity holds.[2]

3.3 State to ensemble transformations

A state to ensemble time evolution is the one where a given initial state ρ can be transformed to one of the final states $\sigma_i \in \{\sigma_i : \ i = 1 \cdots N\}$ with probability p_i such that at the end of transformation we know which of the possibilities $i \in \{1, \cdots, N\}$ has happened. Any such time evolution can be described by a set of completely positive maps $\{\mathcal{E}_i : \ i = 1 \cdots N\}$ where $\sum_i \mathcal{E}_i$ is a trace preserving channel. Then for an initial state ρ the final state will be $\mathcal{E}_i(\rho)/\mathrm{tr}(\mathcal{E}_i(\rho))$ with the probability $\mathrm{tr}\left(\mathcal{E}_i(\rho)\right)$. A state to ensemble transformation describes the most general physical map which can be realized by applying arbitrary measurements and time evolutions on the system.

We say that a state to ensemble transformation is G-covariant if all the maps $\{\mathcal{E}_i : i = 1 \cdots N\}$ are G-covariant. These kinds of dynamics describe the most general type of dynamics one can realize using *G-invariant resources*, i.e. G-invariant unitaries, ancillas in G-invariant states and G-covariant measurements. In the following we show that any G-asymmetry monotone can be naturally used to study state to ensemble transformations.

[2] This fact about the non-convexity of some resource measures has been previously highlighted in the context of entanglement theory. In [28] Vidal and Werner have observed that logarithmic negativity is not a convex function but, as clarified by Plenio in [29], this does not imply that the logarithmic negativity is not an entanglement monotone. Indeed, in the same paper Plenio proves that the logarithmic negativity *is* an entanglement monotone.

Suppose there exists a G-covariant state to ensemble transformation under which an initial state ρ evolves to the final state σ_i with the probability p_i. We denote this by $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$. For this transformation define the state $\tilde{\sigma}$

$$\tilde{\sigma} \equiv \sum_i p_i |i\rangle\langle i| \otimes \sigma_i \tag{3.5}$$

where the set $\{|i\rangle : i = 1 \cdots N\}$ are orthonormal states in a Hilbert space $\mathcal{H}_{\text{anc}}$ and where the representation of symmetry G on the Hilbert space $\mathcal{H}_{\text{anc}}$ is trivial. Therefore all states $\{|i\rangle : i = 1 \cdots N\}$ are G-invariant.

Then, one can easily see that $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$ is equivalent to the fact that $\rho \xrightarrow{\text{G-cov}} \tilde{\sigma}$. So any necessary (or sufficient) condition on the transformation $\rho \xrightarrow{\text{G-cov}} \tilde{\sigma}$ yields a necessary (or sufficient) condition on $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$. In particular, if f is a G-asymmetry monotone we know that a necessary condition for $\rho \xrightarrow{\text{G-cov}} \tilde{\sigma}$ is that $f(\tilde{\sigma}) \leq f(\rho)$. As we will see in the next example, this will put an interesting necessary condition on the possibility of $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$.

Example 12 *Consider the Holevo asymmetry defined in example 10. The above discussion implies that if* $\rho \xrightarrow{\text{G-cov}} \{q_i, \sigma_i\}$ *then for any probability* $p(g)$ *over group* G *it holds that*

$$\Gamma_p(\tilde{\sigma}) \leq \Gamma_p(\rho), \tag{3.6}$$

where

$$\Gamma_p(\tilde{\sigma}) = S\left(\mathcal{G}_p(\tilde{\sigma})\right) - S\left(\tilde{\sigma}\right) \tag{3.7}$$

We can easily see that

$$S\left(\tilde{\sigma}\right) = \sum_i p_i S(\sigma_i) + H(\{p_i\}) \tag{3.8}$$

where $H(\{p_i\})$ *is the Shannon entropy of the probability distribution* $\{p_i\}$*. On the other hand, since the representation of the symmetry transformation* G *on* $\mathcal{H}_{anc}$ *is trivial, then*

$$\mathcal{G}_p(\tilde{\sigma}) = \sum_i p_i |i\rangle\langle i| \otimes \mathcal{G}_p(\sigma_i), \tag{3.9}$$

and so

$$S\left(\mathcal{G}_p(\tilde{\sigma})\right) = \sum_i p_i S\left(\mathcal{G}_p(\sigma_i)\right) + H(\{p_i\}). \tag{3.10}$$

Equations 3.7, 3.8 and 3.10 together imply that if $\rho \xrightarrow{G\text{-}cov} \{p_i, \sigma_i\}$ *then for any probability distribution* $p(g)$ *it holds that*

$$\sum_i p_i \Gamma_p(\sigma_i) \leq \Gamma_p(\rho) \tag{3.11}$$

3.4 Asymmetry monotones from Information monotones

How can we find nontrivial asymmetry monotones? In the case of rotational symmetry one might expect that the (expectation value of) components of angular momentums are asymmetry monotones: For one, a state with nonzero angular momentum is necessarily non-invariant under some rotation, For another, in closed system dynamics by Noether's theorem angular momentum is conserved, a property that any asymmetry monotone should have. However, it turns out that the expectation value of angular momentum (or any function of it) is *not* an asymmetry monotone. This is demonstrated by the following example: A spin-half system oriented in the +z direction enters an environment which is initially unpolarized. Assume the Hamiltonians which describe the interaction between this system and the environment and the Hamiltonians which describe the interaction of different parts of the environment with each other all have rotational symmetry. Then, this spin-half system can induce magnetic polarization in some regions of the unpolarized environment and so the polarization can be *amplified*. Since the arrived spin-half system is in the $+\hat{z}$ direction then by symmetry the induced polarization should also be in the $+\hat{z}$ direction. This is true because all the interactions are rotationally invariant and initially the environment is unpolarized, therefore the map which describes the final state of environment as a function of the initial state of spin-half system should have rotational symmetry. However in this example, part of the environment may end up with a much higher polarization (or angular momentum) than the spin-half system and so angular momentum cannot be an asymmetry monotone. Thinking in terms of dynamical variables in this example, it is not clear how we can find a quantity to measure asymmetry. Another, more rigorous example, which shows this fact that angular momentum can be amplified is a channel which describes the following procedure: We first estimate the direction of a given spin-half system and then based on this estimation prepare many spin-half systems in that direction. One can easily see that this channel is a rotationally invariant dynamics which increases the absolute value of angular momentum of the input system.

In this section we explain how information theoretic concepts are useful to quantify the asymmetry of states. Consider the following game: We are given a spin-half system in

some unknown direction $\hat{n}$ and our goal is to estimate direction $\hat{n}$. We are allowed to do any process and measurement we like. But a spin-half system cannot specify this direction sharply, and for any measurement we perform, the estimated direction might be far from the real direction $\hat{n}$. In other words, there is a fundamental limit on the *information content* of a finite size quantum system about direction and in particular in the case of spin-half systems this limit is small. The notion of information content is defined in a way that someone who does not know anything about the unknown variable cannot increase it by performing a time evolution on the state. In other words, any measure of information content should be non-increasable under physical processes.

Now reconsider the above example of a spin-half system which enters an unpolarized environment where all the interactions are rotationally invariant. Then the symmetry of the process implies that if a spin-half system was initially aligned in some other direction $\hat{n}$, it would induce polarization in the $\hat{n}$ direction on the environment. Now from this point of view we can conclude that though the environment might end up having a large polarization in $\hat{n}$ direction, its information content about the unknown direction cannot be more than the information content of the spin-half system. This is the key observation: By looking to the measures of information content we can find asymmetry monotones. In the rest of this chapter we present this idea more formally and exploit its consequences.

3.4.1 Information monotones

A function f from pairs of states in the same Hilbert space to real numbers is an information monotone if for any pairs of state ρ_1 and ρ_2 and any quantum channel $\mathcal{E}$ it holds that

$$f\left(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)\right) \leq f\left(\rho_1, \rho_2\right) \tag{3.12}$$

Thinking of $\mathcal{E}$ as an information processing on the unknown input, the above equality can be interpreted as a manifestation of the fact that *information processing cannot increase the information.*

Some information monotones have a natural operational interpretation. For example, for any pair of states ρ_1 and ρ_2 one can imagine a game in which one is given state ρ_1 with probability p and state ρ_2 with probability $1-p$. Then, the maximum probability of successfully distinguishing the given state, i.e. finding whether it is ρ_1 or ρ_2, is by definition an information monotone. [3] However in general, it is not clear if an information monotone defined operationally can be easily calculated. In this chapter we provide a list of three

[3] We discuss more about this specific information later in this chapter.

well-known examples of information monotones: trace distance, relative von Neumann entropy and relative Renyi entropy and use them to construct asymmetry monotones.

Example: Relative (von Neumann) entropy

For any pairs of states ρ_1 and ρ_2 the relative (von Neumann) entropy is defined as

$$S(\rho_1||\rho_2) \equiv \mathrm{tr}\left(\rho_1 \log \rho_1\right) - \mathrm{tr}\left(\rho_1 \log \rho_2\right) \tag{3.13}$$

Note that the right-hand side of the above formula is well-defined only if the support of ρ_1 is a subspace of the support of ρ_2. Otherwise, if part of the support of ρ_1 is outside ρ_2, $S(\rho_1||\rho_2)$ is defined to be $+\infty$.

Then for any quantum channel $\mathcal{E}$ it holds that

$$S\left(\mathcal{E}(\rho_1)||\mathcal{E}(\rho_2)\right) \leq S(\rho_1||\rho_2) \tag{3.14}$$

The relative entropy is closely related to the *Holevo quantity*. The Holevo quantity assigned to any arbitrary ensemble of states $\{p_i, \rho_i\}$ can be defined as

$$\begin{aligned} \gamma\{p_i, \rho_i\} &\equiv \sum_i p_i S\left(\rho_i||\bar{\rho}\right) \\ &= S(\bar{\rho}) - \sum_i p_i S(\rho_i) \end{aligned} \tag{3.15}$$

where $\bar{\rho} \equiv \sum_i p_i \rho_i$. Then, one can easily see that the monotonicity of the relative entropy implies the monotonicity of the Holevo quantity such that for any ensemble $\{p_i, \rho_i\}$ and any any quantum channel $\mathcal{E}$ it holds that

$$\gamma\{p_i, \mathcal{E}(\rho_i)\} \leq \gamma\{p_i, \rho_i\} \tag{3.16}$$

As opposed to the relative entropy $S(\rho_1||\rho_2)$ which is not well-defined if part of the support of ρ_1 is outside ρ_2, the Holevo quantity has this advantage that is well defined for any set of states.

3.4.2 From information monotones to asymmetry monotones

Now we show how these information monotones can be used to construct asymmetry monotones. First note that, as it is emphasized by the lemma 7, if $\rho \xrightarrow{\text{G-cov}} \sigma$ then there exists a (G-covariant) channel which maps states $\mathcal{U}_g(\rho)$ to $\mathcal{U}_g(\sigma)$ for all $g \in G$.

So, if $\rho \xrightarrow{\text{G-cov}} \sigma$ then for any information monotone f and any pair of group elements $g_1, g_2 \in G$ it holds that

$$f(\mathcal{U}_{g_1}(\sigma), \mathcal{U}_{g_2}(\sigma)) \leq f\left(\mathcal{U}_{g_1}(\rho), \mathcal{U}_{g_2}(\rho)\right)$$

So for any fixed $g_1, g_2 \in G$ we can think of

$$F_{g_1,g_2}(\rho) \equiv f\left(\mathcal{U}_{g_1}(\rho), \mathcal{U}_{g_2}(\rho)\right) \tag{3.17}$$

as an asymmetry monotone, i.e.

$$\rho \xrightarrow{\text{G-cov}} \sigma \implies F_{g_1,g_2}(\sigma) \leq F_{g_1,g_2}(\rho).$$

This recipe for constructing G-asymmetry monotones can be easily generalized: If under a G-covariant channel $\mathcal{E}$ state ρ evolves to state σ, then for any probability distribution $p(g)$ over group G the channel $\mathcal{E}$ maps the state $\mathcal{G}_p(\rho)$ to state $\mathcal{G}_p(\sigma)$. So for any information monotone f and for any pair of probability distributions $p(g)$ and $q(g)$ over group G it holds that if $\rho \xrightarrow{\text{G-cov}} \sigma$ then

$$f\left(\mathcal{G}_p(\sigma), \mathcal{G}_q(\sigma)\right) \leq f\left(\mathcal{G}_p(\rho), \mathcal{G}_q(\rho)\right) \tag{3.18}$$

Therefore for any information monotone f and any pair of distributions $p(g)$ and $q(g)$ over group we can define a G-asymmetry monotone

$$F_{p,q}(\rho) = f\left(\mathcal{G}_p(\rho), \mathcal{G}_q(\rho)\right) \tag{3.19}$$

In the following example we show that how based on this argument the relative entropy, as an information monotone, yields the Holevo asymmetry monotone. Later, we present more examples of information monotones and use them to construct asymmetry monotones.

3.4.3 The Holevo asymmetry monotone

Here, we use the above method to construct asymmetry monotones from relative entropy. Consider Eq. (3.19) and assume the information monotone f is relative entropy. First, we consider the specific case where the distribution $p(g)$ is the delta distribution at the identity of group and $q(g)$ is the uniform distribution over the group G (Assuming that the group is *unimodular*, i.e. it has a unique left and right invariant Haar measure.[4]). Let $\mathcal{G}$

[4]Recall that all finite and compact Lie groups are unimodular. So, in particular, G could be any finite or compact Lie group.

be the twirling operation according to the uniform measure over group G. Then the above argument implies that the function

$$\Gamma_{\text{unif}}(\rho) \equiv S\left(\rho||\mathcal{G}(\rho)\right) \tag{3.20}$$

is a G-asymmetry monotone. This monotone has been previously introduced in [22] and its monotonicity was proven using a different argument.

It turns out that this function has a very simple interpretation:

Proposition 13 *Let* $\Gamma_{unif}(\rho) \equiv S\left(\rho||\mathcal{G}(\rho)\right)$ *then*

1.
$$\Gamma_{unif}(\rho) = S(\mathcal{G}(\rho)) - S(\rho) \tag{3.21}$$

2.
$$\Gamma_{unif}(\rho) = \min_{\sigma \in G\text{-}inv} S(\rho||\sigma) \tag{3.22}$$

where the minimization is over all G-invariant states.

It turns out that this type of result can be generalized to all unital, idempotent channels [6]. [5]

Proof. To prove item 1 we first note that

$$\begin{aligned}
\Gamma_{\text{unif}}(\rho) &= S\left(\rho||\mathcal{G}(\rho)\right) \\
&= \text{tr}\left(\rho \log \rho\right) - \text{tr}\left(\rho \log \mathcal{G}(\rho)\right) \\
&= \text{tr}\left(\rho \log \rho\right) - \text{tr}\left(\mathcal{G}(\rho) \log \mathcal{G}(\rho)\right) \\
&= S(\mathcal{G}(\rho)) - S(\rho)
\end{aligned}$$

where to get the third equality we have used the fact that $\mathcal{G}(\rho)$ is G-invariant (commutes with all $\{U(g) : g \in G\}$) and so for any arbitrary $g \in G$ $\text{tr}\left(\rho \log \mathcal{G}(\rho)\right) = \text{tr}\left(\mathcal{U}_g(\rho) \log \mathcal{G}(\rho)\right)$.

[5] Let $\mathcal{E}$ be a unital, idempotent channel (i.e. $\mathcal{E} \circ \mathcal{E} = \mathcal{E}$). Then i) $S\left(\rho||\mathcal{E}(\rho)\right) = S\left(\mathcal{E}(\rho)\right) - S(\rho)$ and ii) $S\left(\rho||\mathcal{E}(\rho)\right) = \min_{\sigma \in \text{Image}(\mathcal{E})} S(\rho||\sigma)$ where the minimization is over all states in the image of $\mathcal{E}$. The key idea is that i) if $\mathcal{E}$ is idempotent then any state in the image of $\mathcal{E}$ is also a fixed point of $\mathcal{E}$ and so the set of fixed points of the channel are the same as the image of the channel, ii) if $\mathcal{E}$ is a unital channel then its fixed points form an algebra (the algebra of commutants of its Kraus operators). This also implies that iii) the fixed points of $\mathcal{E}$ and $\mathcal{E}^\dagger$ are the same.

To prove item 2, we first use the Klein inequality: $S(\rho_1||\rho_2) \geq 0$ and $S(\rho_1||\rho_2) = 0$ iff $\rho_2 = \rho_1$. This implies that for any pair of states ρ_1 and ρ_2 it holds that

$$\mathrm{tr}\left(\rho_1 \log \rho_2\right) \leq \mathrm{tr}\left(\rho_1 \log \rho_1\right) \tag{3.23}$$

and equality holds iff $\rho_2 = \rho_1$. So for any fixed ρ_1

$$\max_{\rho_2} \mathrm{tr}\left(\rho_1 \log \rho_2\right) = \mathrm{tr}\left(\rho_1 \log \rho_1\right) \tag{3.24}$$

Now to find

$$\min_{\sigma \in \text{G-inv}} S(\rho||\sigma) = \min_{\sigma \in \text{G-inv}} \left[\mathrm{tr}\left(\rho \log \rho\right) - \mathrm{tr}\left(\rho \log \sigma\right)\right]$$

we first note that the minimum happens for the same G-invariant σ which maximizes $\mathrm{tr}\left(\rho \log \sigma\right)$. Then one can easily see that

$$\begin{aligned}
\max_{\sigma \in \text{G-inv}} \mathrm{tr}\left(\rho \log \sigma\right) &= \max_{\sigma} \mathrm{tr}\left(\rho \log \mathcal{G}(\sigma)\right) \\
&= \max_{\sigma} \mathrm{tr}\left(\mathcal{G}(\rho) \log \sigma\right) \\
&= \mathrm{tr}\left(\mathcal{G}(\rho) \log \mathcal{G}(\rho)\right) \\
&= \mathrm{tr}\left(\rho \log \mathcal{G}(\rho)\right)
\end{aligned}$$

where to get the third equality we have used Eq.(3.24). Note that this argument also implies that the G-invariant state σ which minimizes $S(\rho||\sigma)$ is $\mathcal{G}(\rho)$. ■

The second item in the above proposition suggests that $\Gamma_{\text{unif}}(\rho)$ can be interpreted as the minimum relative entropy distance between the state ρ and the set of G-invariant states (Note that strictly speaking the relative entropy does not define a metric because in general $S(\rho||\sigma) \neq S(\sigma||\rho)$). Also, it implies that the closest state in the set of G-invariant states to state ρ is $\mathcal{G}(\rho)$. So $\Gamma_{\text{unif}}(\rho)$ as a measure of asymmetry quantifies the minimum distance of state ρ to the set of symmetric states.

The first item in the above proposition together with Eq.(3.15) implies that, $\Gamma_{\text{unif}}(\rho)$ can also be interpreted as $\gamma\{p_{\text{unif}}(g), \mathcal{U}_g(\rho)\}$, i.e. the Holevo quantity for the ensemble $\{p_{\text{unif}}(g), \mathcal{U}_g(\rho)\}$ where $p_{\text{unif}}(g)$ is the uniform distribution over group G. Indeed, as we will see in the following, another way to prove the monotonicty of $\Gamma_{\text{unif}}(\rho)$ under G-covariant operations is to use the monotonicity of the Holevo quantity. First, note that for any distribution $p(g)$ and any channel $\mathcal{E}$ it holds that

$$\gamma\{p(g), \mathcal{E}\left(\mathcal{U}_g(\rho)\right)\} \leq \gamma\{p(g), \mathcal{U}_g(\rho)\} \tag{3.25}$$

Now for G-covariant quantum channels $\mathcal{E}$, this implies that

$$\gamma\{p(g),\mathcal{U}_g \circ \mathcal{E}(\rho)\} \leq \gamma\{p(g),\mathcal{U}_g(\rho)\} \tag{3.26}$$

For probability distribution $p(g)$ define

$$\Gamma_p(\rho) \equiv \gamma\{p(g),\mathcal{U}_g(\rho)\} \tag{3.27}$$

This definition together with Eq.(3.26) implies that if there exists a G-covariant channel $\mathcal{E}$ which maps ρ to σ then

$$\Gamma_p(\sigma) \leq \Gamma_p(\rho) \tag{3.28}$$

and so Γ_p is a monotone.

3.5 Application: Entropy generation in symmetric open systems

It turns out that the monotonicty of Holevo asymmetry has a nice physical interpretation: Using Eq.(3.1) one can rewrite Eq.(3.28) as

$$S(\sigma) - S(\rho) \geq S(\mathcal{G}_p(\sigma)) - S(\mathcal{G}_p(\rho)) \tag{3.29}$$

Now the left hand side of this inequality is the entropy generation in an open system dynamics. Then the inequality states that the fact that the open system dynamics has a symmetry described by group G by itself implies a non-trivial lower bound on the entropy generation.

Let us reconsider the example of a spin-half particle initially aligned in the +z direction, $\rho = |\uparrow\rangle\langle\uparrow|$, interacting with an unplorized environment. Assume that, after interacting with the spin-half system the state of the specific subsystem of the environment we are interested in is described by σ. Now we use the above inequality for $p(g)$ the uniform probability distribution over the symmetry group (which in this problem is SO(3)). Then we can easily show that if σ has a large angular momentum in some direction then $S(\mathcal{G}_p(\sigma))$ will be large (logarithmic in the angular momentum) while $S(\mathcal{G}_p(\rho))$ is constant and equal to one. So, the right hand side will be large and the inequality implies that $S(\sigma)$, the entropy of the final state, should be large. In other words, although it is possible to amplify the polarization, the output will necessarily be noisy. This is a simple demonstration of a much more general fact about quantum amplifiers and is basically happening because an amplifier should not increase the information content of the input signal. So although it can amplify the signal, it should add some noise to it such that the distinguishability of signals at the output is less than or equal to the distinguishability of states at the input.

3.6 Application: Conservation laws not captured by Noether's theorem

The symmetry of a closed system dynamics can have many interesting consequences. Perhaps the most prominent and powerful example of the consequences of symmetry is the existence of conservation laws for closed systems. The inference from dynamical symmetries to constants of the motion has its origin in the work of Lagrange in classical mechanics. But these days, it is conventional to use the term *Noether's theorem* to refer to the generic result, and we follow this convention here. The result extends to quantum theory, where symmetries of the time evolution imply the existence of a set of observables such that the expectation value of each (and all powers thereof) are conserved.

On the other hand, as we have seen in proposition 11, in the closed system dynamics with a symmetry G, any G-asymmetry monotone is a constant of motion. In words this means that the amount of G-asymmetry in a closed system with symmetry G is a conserved quantity. For G-asymmetry monotones which are constructed from information monotones this has a simple interpretation: In a closed system dynamics with rotational symmetry, for instance, the amount of information a system has about direction is a conserved quantity. In contrast, if the system is undergoing open dynamics this information could leak to the environment and so the information content of system about direction could decrease. Conversely, if the dynamics is closed but it breaks the symmetry this information content can increase, e.g. a state which does not break the rotational symmetry can evolve to a state which breaks the rotational symmetry and so the final state can have more information about direction.

An interesting question here is whether using these new constants of motion, i.e. asymmetry monotones, we can find constraints beyond the standard conservation laws implied by Noether's theorem. It might be the case that these standard conservation laws capture all the consequences of symmetry such that any other conserved quantity or more generally any other constraint imposed on the dynamics by symmetry cannot give equations independent of the equations implied by these standard conservation laws. In this section we study this problem. Interestingly it turns out that the answer will be different for the cases of pure states and mixed states.

First we consider all the equations implied by Noether's theorem. This theorem implies that for any (differentiable) symmetry of a closed system dynamics there is a conservation law. More precisely, any generator L of the Lie group G is conserved. Note that the conservation of an observable not only means that its expectation value is conserved but also the expectation value of any function of the observable is also conserved. In other

words, if under a unitary G-covariant dynamics, state ρ evolves to state σ, then all the implications of Noether's theorem can be summarized as:

$$\forall L, k: \quad \mathrm{tr}(\rho L^k) = \mathrm{tr}(\sigma L^k) \tag{3.30}$$

where L is an arbitrary generator of G. (Note that the number of independent constraints we can get for each L is at most $d-1$ where d is the dimension of the Hilbert space.) In the case of connected Lie groups, the above set of equations are equivalent to

$$\forall g \in G: \quad \mathrm{tr}\left(\rho U(g)\right) = \mathrm{tr}\left(\sigma U(g)\right) \tag{3.31}$$

Thus far we have discussed only Lie groups. For finite groups there are no generators and so there is no analogous of Eq.(3.30). However, if $\rho \xrightarrow{G-cov} \sigma$ for a finite group G then Eq.(3.31) still holds. This one way in which Eq.(3.31) is a better statement of the consequences of symmetry than Eq.(3.30).

For any state ρ we can think of $\mathrm{tr}\left(\rho U(g)\right)$ as a function from group G to complex numbers. We call this function the *characteristic function* of state ρ. In chapter 6 we study more on the properties of characteristic functions.

In the following we answer this question that whether Eq.(3.31) capture all the consequences of symmetry in a closed system dynamics or not. It turns out that the answer depends on whether the state is pure or not.

3.6.1 Pure states

Consider the situation wherein one knows that the state is pure. Then, the assumption of closed system dynamics will ensure that it remains pure. Now, as we prove in chapter 6 all the asymmetry properties of a pure state relative to the symmetry G are determined by its characteristic function. Indeed, one can prove that

Lemma 14 *There exists a unitary V which is G-invariant, i.e.$\forall g \in G : [V, U(g)] = 0$, such that $V|\psi\rangle = |\phi\rangle$ iff*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle. \tag{3.32}$$

This means that if Eq.(3.32) holds for all $g \in G$ then there exists a closed system dynamics which has the symmetry G under which the state $|\psi\rangle$ can evolve to state $|\phi\rangle$. In the other words, if the only thing we know about the closed system dynamics is that it has symmetry G then for a given initial state ψ any state ϕ which satisfies Eq(3.32) is a possible final state, i.e. it is not forbidden by symmetry. This means that for pure states, Noether's theorem, i.e. Eq. (3.31), includes all the possible implications of the symmetry of dynamics.

3.6.2 Mixed states

It turns out that Noether's theorem does not capture all the consequences of symmetry for mixed states. In this section we first present a simple example which shows this fact and then prove that conservation of any non-trivial (and continuous, in the case of Lie groups) asymmetry monotone yields a constraint which is independent of all constraints implied by the Noether's theorem, i.e. for some states this constraint could be independent of Eq.(3.31).

Before presenting the example we recall that even in the absence of any symmetry restriction, a mixed state ρ can not generally evolve to another mixed state σ by a unitary time evolution. The necessary and sufficient condition for existence of such a unitary is that two states have the same eigenvalues, or equivalently,

$$\forall k: \quad \mathrm{tr}(\rho^k) = \mathrm{tr}(\sigma^k) \tag{3.33}$$

where the number of independent equations in the d dimensional Hilbert space is $d-1$. So even in the absence of symmetry for any initial state ρ of a closed system dynamics there is a restriction on the possible final states: Any final state σ should satisfy Eq.(3.33). This means that to find the constraints on the dynamics which are solely due to the symmetry, we should restrict our attention to those pairs of initial and final states which satisfy these equations.

Now one might expect that if (i) these conditions hold and (ii) all the conditions implied by the Noether's theorem hold then there exists a G-invariant unitary time evolution which transforms ρ to σ. In that case Noether's theorem would capture all the consequences of symmetry. However we will see in the following example that this is not the case: Consider a spin-half system which also has some other independent degree of freedom which is invariant under rotation, say electrical charge. Assume $|\uparrow, q_1\rangle$ and $|\downarrow, q_2\rangle$ are, respectively, the states with spin in +z with charge q_1 and -z direction with charge q_2. Similarly assume $|\rightarrow, q_1\rangle$ and $|\leftarrow, q_2\rangle$ are, respectively, the states with spin in +x with charge q_1 and -x direction with charge q_2. Let

$$\rho = \frac{1}{2}(|\uparrow, q_1\rangle\langle\uparrow, q_1| + |\downarrow, q_2\rangle\langle\downarrow, q_2|) \tag{3.34}$$

and

$$\sigma = \frac{1}{2}(|\rightarrow, q_1\rangle\langle\rightarrow, q_1| + |\leftarrow, q_2\rangle\langle\leftarrow, q_2|). \tag{3.35}$$

Then we can easily check that for these two states the following statements are true: i) There exists a unitary which transforms ρ to σ and so all Eqs. (3.33) hold. For example a

$\pi/2$ rotation around y axis transforms ρ to σ. This implies that in the absence of symmetry the transition from ρ to σ is possible. ii) All constraints implied by Noether's theorem (i.e. condition (3.31)) hold. [6] iii) Yet the transformation of ρ to σ is impossible by a rotationally invariant unitary.

This last point can be easily seen by noting that the state ρ is invariant under all rotations around $\hat{z}$ but it is not invariant under all rotations around $\hat{x}$. On the other hand, the state σ is invariant under all rotations around $\hat{x}$ but it is not invariant under all rotations around $\hat{z}$. So clearly the two states are breaking the rotational symmetry in totally different ways and so they cannot be transformed to each other by a dynamics which does not break rotational symmetry (not even in an open system dynamics).

In this specific simple example the impossibility of the transition between two states could be shown by the above simple argument. But it is instructive to see how this fact can also be shown using an asymmetry monotone which we have already introduced, i.e. the Holevo asymmetry monotone. Assume p_z (p_x) is the uniform distribution over all rotations around $\hat{z}$ ($\hat{x}$). Consider the monotones Γ_{p_x} and Γ_{p_z} defined in Eq.(3.1). Then, it is straightforward to check that

$$\Gamma_{p_z}(\rho) = 0, \quad \Gamma_{p_z}(\sigma) = 1$$

and

$$\Gamma_{p_x}(\rho) = 1, \quad \Gamma_{p_x}(\sigma) = 0$$

So these two monotones are clearly not equal for the two states ρ and σ and this forbids the transition. Furthermore, one can also conclude that there is not even an open system dynamics with rotational symmetry which transforms ρ to σ or vice versa.

This example shows that i) Noether's theorem cannot capture all the consequences of symmetry in the case of closed system dynamics and mixed states and ii) using asymmetry monotones one can put more constraints on which final states are accessible by symmetric dynamics staring from ρ. In other words, the conservation of asymmetry monotones can give constraints which are independent of the constraints imposed by the standard conservation laws. In the following we prove that this is true for any *non-trivial* monotone, where by non-trivial monotones we mean those monotones which are not constant over all states. We prove that the conservation of any non-trivial asymmetry monotone can give equations which are independent of equations implied by Noether's theorem.

[6] This is true because angular momentum operators are non-trivial only on the two dimensional subsystem associated to the spin-half degree of freedom, and for both states ρ and σ the reduced state of this subsystem is the totally mixed state. So the expectation value of any function of angular momentum is the same for these two states.

Theorem 15 *Let G be an arbitrary finite or compact Lie group. Then the equations implied by the conservation of any non-trivial G-asymmetry monotone (which is also continuous in the case of Lie groups) are independent of the conservation laws implied by Noether's theorem (i.e. Eq.(3.31)).*

To prove this we use lemma 16 (see below) which roughly speaking says that if we only know the function $\mathrm{tr}(\sigma U(g))$ but we do not know the exact state σ we cannot determine the value of any non-trivial asymmetry monotone for the state σ. This means that even if we know that Eq.(3.31) holds for a pair of states ρ and σ, then for any given non-trivial asymmetry monotone we cannot conclude that its value is equal for the two states ρ and σ. So the fact that this value is equal for the two states gives a new independent equation. This completes the proof of the theorem. In the following we present the formal statement of the lemma and prove it.

Lemma 16 *Let f be a G-asymmetry monotone which can be expressed as a function of the characteristic function of the state, i.e., $f(\rho) = \mathcal{F}[tr(\rho U(g))]$ for some functional $\mathcal{F} : \mathbb{C}(G) \to \mathbb{R}$. Furthermore, in the case of compact Lie groups assume f is continuous. Then the monotone f is a constant function, i.e. $f(\rho)$ is independent of ρ.*

Proof. (lemma 16)

We first present the proof for the case of finite groups and then we explain how the result can be generalized to the case of compact Lie groups as well.

Suppose $\mathcal{H}$ is the Hilbert space of a physical system on which the symmetry G is represented by the left regular representation of group G, i.e. $\mathcal{H}$ has an orthonormal basis denoted by $\{|g\rangle : \ g \in G\}$ such that

$$\forall g, h \in G : \ U(g)|h\rangle = |gh\rangle \tag{3.36}$$

where $g \to U(g)$ is the representation of the symmetry G on this space. Then, it turns out that on this space we can define another representation of G, called the *right regular representation* denoted by $g \to V_R(g)$, such that

$$\forall g, h \in G : V_R(g)|h\rangle = |hg^{-1}\rangle \tag{3.37}$$

Then one can easily see that these two representations of G on $\mathcal{H}$ commute, i.e.

$$\forall g, h \in G : \ [V_R(h), U(g)] = 0 \tag{3.38}$$

Let $h \in G$ be an arbitrary group element and $e \in G$ be the identity element of group. Then one can easily see that

$$\begin{aligned}
\mathrm{tr}\left(U(g)\mathcal{G}(|h\rangle\langle h|)\right) &= \mathrm{tr}\left(U(g)\mathcal{G}\left(U(h)|e\rangle\langle e|U^\dagger(h)\right)\right) \\
&= \mathrm{tr}\left(U(g)\mathcal{G}(|e\rangle\langle e|)\right) \\
&= \frac{1}{|G|}\sum_{s\in G}\mathrm{tr}\left(U(g)U(s)|e\rangle\langle e|U^\dagger(s)\right) \\
&= \frac{1}{|G|}\sum_{s\in G}\mathrm{tr}\left(U(g)V_R(s^{-1})|e\rangle\langle e|V_R^\dagger(s^{-1})\right) \\
&= \mathrm{tr}\left(U(g)|e\rangle\langle e|\right)
\end{aligned}$$

where to get the second equality we have used the fact $\forall h \in G:\ \mathcal{G}(X) = \mathcal{G}(U(h)XU^\dagger(h))$ and to get the last equality we have used the fact that two representations commute, i.e. Eq.(3.38). So the characteristic function of state $|h\rangle$ is equal to the characteristic function of the state $\mathcal{G}(|e\rangle\langle e|)$. This means that for any monotone f whose value for a given state depends only on the characteristic function of that state it holds that

$$f\left(|e\rangle\langle e|\right) = f\left(\mathcal{G}(|e\rangle\langle e|)\right) \tag{3.39}$$

But, as we have seen before, for any G-asymmetry monotone the value of monotone is the same for all G-invariant states and furthermore this value is the minimum value of that function over all states. So the above equation implies that

$$f\left(|e\rangle\langle e|\right) = \min_\sigma f\left(\sigma\right) \tag{3.40}$$

Now consider an arbitrary state ρ in a space with arbitrary projective unitary representation of symmetry G denoted by $g \to T(g)$. Then, one can easily show that there exists G-covariant channels which map state $|e\rangle$ to state ρ. One such quantum channel is described by the map

$$\mathcal{E}_\rho(X) \equiv \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}\left(|g\rangle\langle g|X\right)T(g)\rho T^\dagger(g) \tag{3.41}$$

But the fact that $\mathcal{E}_\rho$ is G-covariant together with the fact that f is a G-asymmetry monotone implies that for any state ρ it holds that

$$f\left(\rho\right) = f\left(\mathcal{E}_\rho(|e\rangle\langle e|)\right) \le f\left(|e\rangle\langle e|\right) \tag{3.42}$$

This together with Eq.(3.40) imply that for an arbitrary state ρ in a space with arbitrary projective unitary representation of symmetry G it holds that

$$f(\rho) = \min_{\sigma} f(\sigma) \tag{3.43}$$

and so the monotone f should be constant over all states. This completes the proof of lemma for the case of finite groups.

In the following, we prove that making the extra assumption that the asymmetry monotone is also continuous, this result can be extended to the case of compact Lie groups. Note that in this case the regular representation of the group is not finite dimensional. But, as it is highlighted in [30] and later in [1] there still exists a sequence of finite dimensional spaces $\mathcal{H}_d$, where d is the maximum dimension of irreps showing up in $\mathcal{H}_d$, with an over-complete basis $\{|g\rangle : g \in G\}$ such that

$$\forall g, h \in G : \; U(g)|h\rangle = |gh\rangle \tag{3.44}$$

where $g \to U(g)$ is the representation of the symmetry G on this space. [7]

Furthermore, as it is discussed in [30] and [1], by allowing larger and larger dimension d of irreps showing up in the Hilbert spaces $\mathcal{H}_d$ it is possible to make the inner products $\langle g_2|g_1\rangle$ arbitrary close to zero for any pairs of group elements $g_1 \neq g_2$. In this limit, the state $|e\rangle$ has the *maximal asymmetry* in the sense that for any given state ρ in a finite dimensional space with arbitrary representation of G there exists a G-covariant channel $\mathcal{E}_\rho$ such that

$$\lim_{d\to\infty} \mathcal{E}_\rho(|e\rangle\langle e|) \to \rho \tag{3.45}$$

The G-covariant channel $\mathcal{E}_\rho$ can be defined in the similar way it was defined for the case of finite groups, i.e.

$$\mathcal{E}_\rho(X) \equiv \int dg \; \mathrm{tr}\left(|g\rangle\langle g|X\right) T(g)\rho T^\dagger(g) \tag{3.46}$$

where $g \to T(g)$ is the representation of G on the Hilbert space which ρ belongs to.

[7] Let $\mathcal{H}_d = \bigoplus_{\mu:d_\mu\leq d} \mathcal{M}_\mu \otimes \mathcal{N}_\mu$ where the summation is over all irreps of G whose dimension d_μ is less than or equal to d, and $\mathcal{M}_\mu$ is the subsystem on which the symmetry G acts like its irrep μ and $\mathcal{N}_\mu$ is the multiplicity subsystem with dimension equal to d_μ. Define $|e\rangle = c\sum_\mu \sqrt{d_\mu}\sum_{i=1}^{d_\mu} |\mu, i\rangle \otimes |\tilde{i}\rangle$ $(*)$ where c is a normalization factor, $\{|\mu, i\rangle : i = 1 \cdots d_\mu\}$ is an orthonormal basis for subsystem $\mathcal{M}_\mu$ and $\{|\tilde{i}\rangle : i = 1 \cdots d_\mu\}$ is an orthonormal basis for $\mathcal{N}_\mu$. The properties assumed for $\{|g\rangle = U(g)|e\rangle : \; g \in G\}$ used in the proof hold if this set of states is generated from a fiducial state of the form of $|e\rangle$ defined in Eq. $(*)$.

Now, similar to the case of finite groups we can also define another representation of G on $\mathcal{H}_d$ denoted by $g \to V_R(g)$ such that

$$\forall g, h \in G : V_R(g)|h\rangle = |hg^{-1}\rangle \tag{3.47}$$

Then one can easily see that these two representations of G on $\mathcal{H}$ commute, i.e.

$$\forall g, h \in G : \ [V_R(h), U(g)] = 0 \tag{3.48}$$

Therefore, using the same argument we used for finite groups we can prove that for any $h \in G$ it holds that $\mathrm{tr}\left(|h\rangle\langle h|U(g)\right) = \mathrm{tr}\left(\mathcal{G}(|e\rangle\langle e|)U(g)\right)$ where e is the identity element of group G. Therefore, for any monotone f whose value for a given state depends only on the characteristic function of that state it holds that

$$f\left(|e\rangle\langle e|\right) = \min_{\rho} f\left(\rho\right) \tag{3.49}$$

Furthermore, since f is a G-asymmetry monotone and since $\mathcal{E}_\rho$ is G-covariant then

$$f\left(\mathcal{E}_\rho(|e\rangle\langle e|)\right) \leq f(|e\rangle\langle e|) \tag{3.50}$$

The above two equations imply that

$$f\left(\mathcal{E}_\rho(|e\rangle\langle e|)\right) = \min_{\rho} f\left(\rho\right) \tag{3.51}$$

On the other hand, assuming f is continuous Eq. (3.45) implies that

$$\lim_{d\to\infty} f\left(\mathcal{E}_\rho(|e\rangle\langle e|)\right) \to f(\rho) \tag{3.52}$$

This together with Eq. (3.51) prove that for any arbitrary state ρ in a finite dimensional space with arbitrary representation of the symmetry G it holds that $f(\rho) = \min_\sigma f\left(\sigma\right)$. Therefore, we conclude that in the case of compact Lie groups any continuous G-asymmetry monotone which only depends on the characteristic function of state is a constant function. This completes the proof of lemma 16. ■

3.7 Wigner-Yanase-Dyson skew information as an asymmetry monotone

In section 3.4 we introduced a recipe to construct a new asymmetry monotone from information monotones an appled it to the case of relative entropy. In this section we apply this idea for the case of *relative Renyi entropy*. Interestingly, it turns out that the asymmetry monotone we find in this way is in fact a function which has been previously known and studied under the title of *Wigner-Yanase-Dyson skew information*. We start this section by a short review of this topic.

3.7.1 Wigner-Yanase-Dyson skew information

For any observable L, Wigner and Yanase define the skew information of state ρ as

$$\begin{aligned} I(\rho, L) &\equiv -\frac{1}{2}\mathrm{tr}\left([\rho^{1/2}, L]^2\right) \\ &= \mathrm{tr}(\rho L^2) - \mathrm{tr}\left(\rho^{1/2} L \rho^{1/2} L\right) \end{aligned} \tag{3.53}$$

where the bracket here denotes the commutator [31]. It is usually assumed that L is an observable whose eigenvalues are integer or half-integer.[8]

A generalization of Wigner-Yanase skew information is proposed by Dyson as

$$\begin{aligned} I_s(\rho, L) &\equiv -\frac{1}{2}\mathrm{tr}\left([\rho^s, L][\rho^{1-s}, L]\right) \\ &= \mathrm{tr}(\rho L^2) - \mathrm{tr}\left(\rho^s L \rho^{1-s} L\right) \end{aligned} \tag{3.54}$$

for arbitrary $0 < s < 1$ [31]. This is usually called Wigner-Yanase-Dyson skew information. Note that for pure states and for all $0 < s < 1$,

$$I_s(|\psi\rangle\langle\psi|, L) = \mathrm{Var}_L(\rho), \tag{3.55}$$

where

$$\mathrm{Var}_L(\rho) \equiv \langle\psi|L^2|\psi\rangle - \langle\psi|L|\psi\rangle^2 \tag{3.56}$$

is the variance of the observable L for state ρ.

Wigner and Yanase introduce $I(\rho, L)$ as a measure of information about the state of a system which is described by the density operator ρ and, equivalently, they introduce $-I(\rho, L)$ as an entropy measure. They consider the situation where the observable L is an additive conserved quantity such as charge or components of linear or angular momenta. In this situation measuring the observables which do not commute with L is much more complicated than measuring observable which commute with L. Then, they argue that under this assumption the negative of von Neumann entropy, i.e. $-S(\rho) = \mathrm{tr}(\rho \log \rho)$, can no longer specify our knowledge about the state of system. Instead, they claim that in this situation $I(\rho, L)$ is the right measure of information in the sense that it specifies "*the amount of information which an ensemble described by a state vector or a statistical matrix contains with respect to the not easily measured quantities*" [31]. Here by "not easily measured quantities" they mean observables which do not commute with L.

[8] Note that this implies $\theta \to \exp i\theta L$ is a projective representation of group U(1).

To support this claim they show several nice properties of $I(\rho, L)$ such as the additivity

$$I\left(\rho_A \otimes \rho_B, L_A \otimes I + I \otimes L_B\right) = I\left(\rho_A, L_A\right) + I\left(\rho_B, L_B\right) \tag{3.57}$$

and the convexity

$$I(p\rho + (1-p)\sigma, L) \leq pI(\rho, L) + (1-p)I(\sigma, L) \tag{3.58}$$

for arbitrary $0 \leq p \leq 1$. Furthermore, they observe that under a closed system unitary dynamics which commutes with observable L the skew information remains constant. It is worth mentioning that all these properties of the function $I(\cdot, L)$ can be extended to the function $I_s(\cdot, L)$ for $0 < s < 1$. In particular, the convexity of $I_s(\cdot, L)$ for $0 < s < 1$ is a famous result of Lieb [33]. He also discovered an important connection between the convexity of this function and the strong sub-additivity of von Neumann entropy (See also [35, 36]).

Alternatively, $I(\rho, L)$ is sometimes interpreted as a measure of non-commutativity of the state ρ and the observable L (See e.g. [34, 32, 37]). But, in this point of view $I(\rho, L)$ does not have any operational meaning and it is hard to find a physical interpretation for all the nice properties of this function. Also, it is not clear why to quantify the non-commutativity of ρ and L we should look at this specific function and not a simpler function which is symmetric with respect to ρ and L such as $-\mathrm{tr}([\rho, L]^2)$.

In the following, we offer a new interpretation of the function $I_s(\cdot, L)$ for arbitrary $0 < s < 1$. We show that this function is in fact an asymmetry monotone relative to the group generated by L, i.e. the group of unitaries $\{e^{i\theta L}\}$. In other words, $I(\rho, L)$ quantifies how much this symmetry is broken by state ρ.

3.7.2 Asymmetry monotone from the relative Renyi entropy

The *Relative Renyi entropy* of order s of two states ρ_1 and ρ_2 is defined as $\log D_s(\rho_1, \rho_2)$ where

$$D_s(\rho_1, \rho_2) \equiv \mathrm{tr}(\rho_1^s \rho_2^{1-s}) \tag{3.59}$$

For $s \in (0, 1)$ and for any arbitrary completely positive trace-preserving channel $\mathcal{E}$ it holds that [44]

$$\forall \rho_1, \rho_2 : \; D_s(\rho_1, \rho_2) \leq D_s\left(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)\right) \quad s \in (0, 1) \tag{3.60}$$

In other words, for $s \in (0, 1)$ the function $-D_s(\rho_1, \rho_2)$ is an information monotone (note the negative sign.). On the other hand, for $-1 < s < 0$

$$\forall \rho_1, \rho_2 : \; D_s\left(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)\right) \leq D_s(\rho_1, \rho_2) \quad s \in (-1, 0) \tag{3.61}$$

for arbitrary channel $\mathcal{E}$ and so the function $D_s(\rho_1, \rho_2)$ is an information monotone (See [44]).

Note that in the case of $s \in (0,1)$ and for any pair of pure states ψ_1 and ψ_2 it holds that

$$-D_s(\psi_1, \psi_2) = -|\langle\psi_1|\psi_2\rangle|^2 \tag{3.62}$$

In the following we use the information monotone $-D_s$ for $s \in (0,1)$ to construct an asymmetry monotone. Assume for an observable L_1 and a state ρ in $\mathcal{B}(\mathcal{H}_1)$ and an observable L_2 and a state σ in $\mathcal{B}(\mathcal{H}_2)$ there exists a quantum channel $\mathcal{E}$ from $\mathcal{B}(\mathcal{H}_1)$ to $\mathcal{B}(\mathcal{H}_2)$ which is covariant, i.e.

$$\forall\theta: \quad \mathcal{E}\left(e^{i\theta L_1}(\cdot)e^{-i\theta L_1}\right) = e^{i\theta L_2}\mathcal{E}\left(\cdot\right)e^{-i\theta L_2} \tag{3.63}$$

and furthermore maps ρ to σ, i.e.

$$\mathcal{E}(\rho) = \sigma \tag{3.64}$$

Consider

$$D_s\left(\rho, e^{i\theta L_1}\rho e^{-i\theta L_1}\right) = \mathrm{tr}\left(\rho^s[e^{i\theta L_1}\rho e^{-i\theta L_1}]^{1-s}\right) = \mathrm{tr}\left(\rho^s e^{i\theta L}\rho^{1-s}e^{-i\theta L}\right)$$

Then for small θ where $e^{i\theta L_1} \simeq I + i\theta L_1 - (\theta L_1)^2/2 + \mathcal{O}(\theta^3)$ we get

$$D_s\left(\rho, e^{i\theta L_1}\rho e^{-i\theta L_1}\right) \simeq 1 - \theta^2\left[\mathrm{tr}(\rho L_1^2) - \mathrm{tr}(\rho^s L_1 \rho^{(1-s)} L_1)\right] + \mathcal{O}(\theta^3) \tag{3.65}$$

Now Eqs. (3.63,3.64) together with the monotonicity of D_s under information processing, i.e. Eq. (3.61), imply that

$$D_s\left(\rho, e^{i\theta L_1}\rho e^{-i\theta L_1}\right) \leq D_s\left(\sigma, e^{i\theta L_2}\sigma e^{-i\theta L_2}\right) \tag{3.66}$$

Then, by virtue of Eq. (3.65) we conclude that

$$\mathrm{tr}(\sigma L_2^2) - \mathrm{tr}(\sigma^s L_2 \sigma^{(1-s)} L_2) \leq \mathrm{tr}(\rho L_1^2) - \mathrm{tr}(\rho^s L_1 \rho^{(1-s)} L_1) \tag{3.67}$$

In other words

$$\forall s \in (0,1): \quad I_s(\sigma, L_2) \leq I_s(\rho, L_1) \tag{3.68}$$

So we conclude that Wigner-Yanase-Dyson skew information is in fact an asymmetry monotone.[9] Note that L can be a generator of a compact Lie group G. This means that if $\rho \xrightarrow{\text{G-cov}} \sigma$ then for any generator L of G it holds that $I_s(\sigma, L) \leq I_s(\rho, L)$.

[9] It has been previously shown in [37] that Wigner-Yanase skew information, i.e. $I_s(\cdot, L)$ for the special case of $s = 1/2$, can be derived in a similar fashion from Fisher Information.

As we mentioned before this asymmetry monotone is additive, i.e. for arbitrary $0 < s < 1$ it holds that

$$I_s\left(\rho_A \otimes \rho_B, L_A \otimes I + I \otimes L_B\right) = I_s\left(\rho_A, L_A\right) + I_s\left(\rho_B, L_B\right). \tag{3.69}$$

Also, using the same idea we used in section 3.3, it is straightforward to show that if $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$ then

$$\sum_i p_i \; I_s(\sigma_i, L) \leq I_s(\rho, L) \tag{3.70}$$

where L is an arbitrary generator of the compact Lie group G.

3.7.3 Uncertainty relations for skew information

There has been several works on the possible generalizations of the uncertainty relations in terms of skew information (See e.g. [37, 38, 39, 40, 42]). These investigations are mainly motivated by the fact that for all $0 < s < 1$

$$I_s(\rho, L) \leq \mathrm{Var}_L(\rho) \tag{3.71}$$

and in the special case of pure states this holds as an equality. So, one might expect a generalization of the uncertainty relations as

$$I(\rho, L_1) I(\rho, L_2) \geq \frac{1}{4} \left|\mathrm{tr}\left(\rho[L_1, L_2]\right)\right| \tag{3.72}$$

Note that in the case of pure states this inequality is equivalent to the standard uncertainty relation. In fact, [40, 42] claim to prove this inequality. But, as later was noticed in [41, 38, 43] this proof is not correct and the above inequality does not hold in general.

Indeed, adopting the point of view that $I_s(\rho, L_1)$ and $I_s(\rho, L_2)$ are asymmetry monotones it is clear why the above inequality cannot hold: The left hand-side is an asymmetry monotone for the symmetry group generated by L_1 and L_2 while the right hand side is not. For example, consider the case of SO(3) and assume L_1 to be the angular momentum in the $\hat{z}$ direction and L_2 to be the angular momentum in the $\hat{x}$ direction. Then $[L_1, L_2]$ will be proportional to the angular momentum in the $\hat{y}$ direction. Now since the left-hand side of the above inequality is an asymmetry monotone for the group of SO(3), then it cannot be increased under rationally covariant time evolutions. In other words, for any rotationally covariant channel $\mathcal{E}$

$$I_s(\mathcal{E}(\rho), L_1) I_s(\mathcal{E}(\rho), L_2) \leq I_s(\rho, L_1) I_s(\rho, L_2)$$

On the other hand, as we have seen before the expectation value of angular momentum is not an asymmetry monotone and it can be arbitrarily amplified. In particular, if $\text{tr}(\rho L_{\hat{z}})$ is nonzero then there exists a rotationally covariant channel $\mathcal{E}$ such that $|\text{tr}(\mathcal{E}(\rho)L_{\hat{z}})|$ is arbitrary larger than $|(\rho L_{\hat{z}})|$. So this means that $1/4\,|\text{tr}\,(\mathcal{E}(\rho)[L_1, L_2])|$ cannot be a lower bound for $I_s(\mathcal{E}(\rho), L_1)I_s(\mathcal{E}(\rho), L_2)$ and so the inequality 3.72 cannot hold in general.

Based on this intuition we know that one way to fix this wrong inequality is to change the left-hand side in a way that it can increase under symmetric channels. One example of such inequalities is

$$I(\rho, L_1)\text{Var}_{L_2}(\rho) \geq \frac{|\text{tr}(\rho[L_1, L_2])|}{8} \tag{3.73}$$

which is proven at the end of this section. Note that if ρ is a pure state then this inequality is exactly in the form of uncertainty relation with an extra factor of 2 in the right-hand side's denominator.

One way to interpret this inequality is to think of it as a lower bound on the amount of asymmetry relative to the U(1) group generated by L_1, i.e. the group formed by the unitaries $\{e^{i\theta L_1}\}$. Then, the inequality implies that

$$I(\rho, L_1) \geq \frac{|\text{tr}(\rho[L_1, L_2])|}{8\text{Var}_{L_2}(\rho)}$$

Now consider the example of SO(3) and assume L_1 to be the angular momentum in the $\hat{z}$ direction and L_2 to be the angular momentum in the $\hat{x}$ direction. Then $[L_1, L_2]$ will be proportional to the angular momentum in the $\hat{y}$ direction. So the above inequality implies that for any representation of SO(3) if the expectation value of angular momentum in the $\hat{y}$ direction is large but the variance of angular momentum in the $\hat{x}$ direction is small, then the state will have a large asymmetry relative to rotations around the z. In the following we prove the inequality (3.73).

Proof of the inequality (3.73):

We assume ρ has full support. Otherwise, if ρ does not have full support we define the state $\rho_\epsilon \equiv (1-\epsilon)\rho + \epsilon I/d$ where ϵ is a small positive number and I/d is the totally mixed state. This state will have full support. So we can continue the proof using this state and then at the end take the limit of $\epsilon \to 0$.

Consider the inner product defined by

$$\langle A, B\rangle_\rho \equiv \text{tr}(\rho A^\dagger B) \tag{3.74}$$

Then the Schwartz inequality implies that

$$\langle A, A\rangle_\rho \langle B, B\rangle_\rho \geq |\langle A, B\rangle_\rho|^2 \tag{3.75}$$

Let L_1 and L_2 be two arbitrary generators of the Lie group G. Now we use the above inequality for the operators

$$A = L_1 - \sqrt{\rho} L_1 \sqrt{\rho^{-1}} \tag{3.76}$$

and

$$B = L_2 - \mathrm{tr}\left(\rho L_2\right) I \tag{3.77}$$

Then it turns out that

$$\langle A, A\rangle_\rho = 2\left[\mathrm{tr}(\rho L_1^2) - \mathrm{tr}(\sqrt{\rho} L_1 \sqrt{\rho} L_1)\right], \tag{3.78}$$

$$\langle B, B\rangle_\rho = \mathrm{tr}(\rho L_2^2) - \mathrm{tr}(\rho L_2)^2 \tag{3.79}$$

and

$$\langle A, B\rangle_\rho = \mathrm{tr}(\rho L_1 L_2) - \mathrm{tr}(\sqrt{\rho} L_1 \sqrt{\rho} L_2) \tag{3.80}$$

Now one can easily see that

$$|\langle A, B\rangle_\rho|^2 \geq |\mathrm{Im}\left[\langle A, B\rangle_\rho\right]|^2 = \left|\frac{\langle A, B\rangle_\rho - \langle A, B\rangle_\rho^*}{2}\right|^2 = \frac{|\mathrm{tr}\left(\rho[L_1, L_2]\right)|^2}{4}$$

where by $\mathrm{Im}\left[\langle A, B\rangle_\rho\right]$ we mean the imaginary part of $\langle A, B\rangle_\rho$.

Putting all of these in the Schwartz inequality Eq.(3.75), we find that

$$I(\rho, L_1)\mathrm{Var}_{L_2}(\rho) \geq \frac{1}{8}\mathrm{tr}\left(\rho[L_1, L_2]\right)^2 \tag{3.81}$$

which completes the proof.

3.8 More examples of asymmetry monotones

In this section, we present more examples of asymmetry monotones. In particular, we use the trace distance as an information monotone to construct a new asymmetry monotone.

3.8.1 Asymmetry monotones constructed from the trace distance

The trace norm is defined by

$$\|X\| \equiv \mathrm{tr}\left(\sqrt{XX^\dagger}\right). \tag{3.82}$$

It turns out that the trace norm is non-increasing under positive, trace-preserving maps, i.e. for any positive (and not necessarily completely positive) trace-preserving map $\mathcal{E}$ it holds that

$$\|\mathcal{E}(X)\| \leq \|X\| \tag{3.83}$$

This implies that for any pairs of state ρ_1 and ρ_2 their trace distance, defined by $\|\rho_1 - \rho_2\|$, is non-increasing under positive trace-preserving maps, i.e.

$$\|\mathcal{E}(\rho_1) - \mathcal{E}(\rho_2)\| \leq \|\rho_1 - \rho_2\|. \tag{3.84}$$

So the trace distance of two states is an information monotone. A theorem proven by Helstrom provides a simple operational interpretation of the trace distance of two states: $\|\rho_1 - \rho_2\|$ determines the maximum probability of successfully distinguishing ρ_1 and ρ_2 when we are given a quantum system either in state ρ_1 or state ρ_2 with equal probability. Then the maximum probability of success is equal to

$$\frac{1}{2} + \frac{\|\rho_1 - \rho_2\|}{4}$$

Now using the same ideas we have used in section 3.4 to define the Holevo asymmetry monotone we can use the trace distance to define a new family of asymmetry monotones. In particular, in the case of Lie groups one can find an interesting monotone by considering the trace distance between states ρ and $\mathcal{U}_g(\rho)$ for a group element g which is infinitesimally close to the identity element: Suppose $U(g) = e^{i\theta L}$ where L is a generator of the Lie group. Then at the limit where $\theta \to 0$ it holds that

$$\|\rho - \mathcal{U}_g(\rho)\| \simeq \theta \|[\rho, L]\| + \mathcal{O}(\theta^2) \tag{3.85}$$

Now, the monotonicity of the trace distance implies that if $\rho \xrightarrow{\text{G-cov}} \sigma$ then

$$\|[\sigma, L]\| \leq \|[\rho, L]\|. \tag{3.86}$$

So we conclude that for any generator L of the Lie group the function

$$F_L(\cdot) \equiv \|[\cdot, L]\| \tag{3.87}$$

is a G-asymmetry monotone. It is straightforward to check the following properties:

1. For any G-invariant state the value of this monotone is zero.

2. For a pure state $|\psi\rangle$, $F_L(|\psi\rangle\langle\psi|)$ is proportional to the square root of the variance of L for state ψ as
$$F_L(|\psi\rangle\langle\psi|) = 2\sqrt{\mathrm{Var}_L(\psi)} \tag{3.88}$$

3. Using the same idea we used in section 3.3 we can prove that if $\rho \xrightarrow{\text{G-cov}} \{p_i, \sigma_i\}$ then
$$\sum_i p_i \; F_L(\sigma_i) \leq F_L(\rho) \tag{3.89}$$

In chapter 5 we introduce more examples of asymmetry monotones which can be constructed based on the trace distance.

3.8.2 Generating new monotones from known monotones

Given any asymmetry monotone one can construct new asymmetry monotones. Clearly any non-decreasing monotonic function of an asymmetry monotone is another asymmetry monotone. Also, using the convention that asymmetry monotones are non-negative, the product of two asymmetry monotones are also asymmetry monotones. As a less trivial example, if $F(\cdot)$ is an asymmetry monotone then for any fixed state ρ, $F\left(\,\cdot\,\otimes\rho\right)$ is also an asymmetry monotone.

This way of generating new monotones from given monotones clearly works in any other resource theory as well. But in the following we focus on some ideas for building new monotones from old monotones which are specific to the resource theory of asymmetry.

First, if $H \subset G$ is a subgroup of G, then the representation of G on a Hilbert space naturally induces a representation of H. Then any quantum channel which is covariant with respect to this representation of G is also covariant with respect to the induced representation of H. This implies that any H-asymmetry monotone on this space is also a G-asymmetry monotone. So, in particular the study of U(1)-asymmetry monotones will be useful because any compact Lie group has subgroups isomorphic to U(1).

Second, note that if F is a G-asymmetry monotone then for all group elements $g \in G$, $\tilde{F}(\cdot) \equiv F\left(U(g)\cdot U^\dagger(g)\right)$ is also an asymmetry monotone. More generally, for any arbitrary probability distribution $p(g)$ over group G,
$$\tilde{F}(\cdot) \equiv F\left(\mathcal{G}_p(\cdot)\right)$$
is also a G-asymmetry monotone.

Example 17 *We have seen that for any arbitrary probability distribution $q(g)$ over group G the function*

$$\Gamma_q(\cdot) \equiv S\left(\mathcal{G}_q(\cdot)\right) - S(\cdot) \tag{3.90}$$

is a G-asymmetry monotone. The above observation implies that for any arbitrary probability distributions $p(g)$ and $q(g)$ over group G the function $\Gamma_q\left(\mathcal{G}_p(\cdot)\right)$ is also a monotone. Consider the special case where $q(g)$ is uniform. Then, this implies that

$$\overline{\Gamma}_p(\rho) \equiv \Gamma_q(\cdot) = S(\mathcal{G}(\rho)) - S(\mathcal{G}_p(\rho)) \tag{3.91}$$

is also a monotone. It follows that for any given probability distribution $p(g)$ over group G we can decompose the monotone $\Gamma_{unif}(\cdot) = S(\mathcal{G}(\cdot)) - S(\cdot)$ as the sum of two monotones Γ_p and $\bar{\Gamma}_p$ defined above, i.e.

$$\Gamma_{unif} = \overline{\Gamma}_p + \Gamma_p. \tag{3.92}$$

Chapter 4

Different Representations of symmetric channels

In this chapter we review two known representations of G-covariant channels i.e. Kraus representation and Stinespring dilation of G-covariant channels. We also introduce a new representation which basically describes a G-covariant channel by specifying how it acts on an *irreducible tensor operator basis*.

In the next chapter we use this new representation to study asymmetry of quantum states. We will also use the Stinespring dilation of G-covariant channels to study asymmetry of pure quantum states in chapter 6.

We start this chapter by a short review of irreducible tensor operators. See e.g. [11] and [47] for more information on this subject.

4.1 Review of irreducible tensor operators

Let $\mathcal{B}(\mathcal{H})$ be the space of all bounded operators acting on the Hilbert space $\mathcal{H}$. For any unitary $V \in \mathcal{B}(\mathcal{H})$ the super-operator $V(\cdot)V^\dagger$ preserves the Hilbert-Schmidt inner product on $\mathcal{B}(\mathcal{H})$, defined as $\langle A, B\rangle \equiv \mathrm{tr}(A^\dagger B)$ for arbitrary $A, B \in \mathcal{B}(\mathcal{H})$. So the super-operator $V(\cdot)V^\dagger$ can be thought as a unitary acting on the space $\mathcal{B}(\mathcal{H})$.

Suppose $g \to U(g)$ is a projective unitary representation of a finite or compact Lie group G on the Hilbert space $\mathcal{H}$. Then $g \to \mathcal{U}(g)$ is a unitary representation of G on $\mathcal{B}(\mathcal{H})$, where $\mathcal{U}_g[\cdot] \equiv U(g)(\cdot)U^\dagger(g)$. Note that this representation is always non-projective, i.e.

$$\forall g_1, g_2 \in G: \quad \mathcal{U}_{g_2} \circ \mathcal{U}_{g_1} = \mathcal{U}_{g_2 g_1} \tag{4.1}$$

Let $\{T_m^{(\mu,\alpha)}\}$ be a basis of $\mathcal{B}(\mathcal{H})$ in which the representation $g \to \mathcal{U}(g)$ decomposes to the irreps of G such that

$$\mathcal{U}_g[T_m^{(\mu,\alpha)}] = \sum_{m'} u_{m'm}^{(\mu)}(g)\ T_{m'}^{(\mu,\alpha)} \tag{4.2}$$

where

$$u_{m'm}^{(\mu)}(g) \equiv \langle \mu, m'|U^{(\mu)}(g)|\mu, m\rangle \tag{4.3}$$

are the matrix elements of $U^{(\mu)}(g)$, the unitary (non-projective) irreducible representation of G labeled by μ. We choose this basis to be normalized such that

$$\mathrm{tr}(T_m^{(\mu,\alpha)\dagger} T_{m'}^{(\mu',\alpha')}) = \delta_{\mu,\mu'}\delta_{\alpha,\alpha'}\delta_{m,m'} \tag{4.4}$$

Here, α can be thought as a multiplicity index. We call the basis $\{T_m^{(\mu,\alpha)}\}$ the *irreducible tensor operator basis*. Also, the elements of the set $\{T_m^{(\mu,\alpha)}\}$ for a fixed μ and α are called *components* of the irreducible tensor $T^{(\mu,\alpha)}$. We call the irrep label μ the *rank* of the tensor operator $T_m^{(\mu,\alpha)}$.

Example 18 ***U(1)***

Let $e^{i\theta} \to U(\theta)$ be an arbitrary (non-projective) unitary representation of group $U(1)$ and

$$U(\theta) = \sum_{n=n_{min},\alpha}^{n_{max}} e^{in\theta}|n,\alpha\rangle\langle n,\alpha| \tag{4.5}$$

be its decomposition to irreps. Then, one can easily see that a basis of irreducible tensor operators is defined by

$$\{T^{(k,\tilde{\alpha})} = |n+k,\alpha\rangle\langle n,\alpha'| : |k| \le n_{max} - n_{min}\}$$

where $\tilde{\alpha} \equiv (\alpha, \alpha', n)$ is the multiplicity label.

Consider the Hermitian conjugate of both sides of Eq.(4.2), i.e.

$$\left(\mathcal{U}_g[T_m^{(\mu,\alpha)}]\right)^\dagger = \mathcal{U}_g[T_m^{(\mu,\alpha)\dagger}] = \sum_{m'} \bar{u}_{m'm}^{(\mu)}(g)\ T_{m'}^{(\mu,\alpha)\dagger} \tag{4.6}$$

where $\bar{u}_{m'm}^{(\mu)}(g)$ denotes the complex conjugate of $u_{m'm}^{(\mu)}(g)$. This implies that for any component $T_m^{(\mu,\alpha)}$ of a tensor operator of rank μ, its Hermitian conjugate, i.e. $T_m^{(\mu,\alpha)\dagger}$ is in the subspace spanned by rank $\bar{\mu}$ irreducible tensor operators where $\bar{\mu}$ denotes the irrep

equivalent to the complex conjugate of irrep μ. In particular, in the case of SO(3) (or equivalently SU(2)) where the complex conjugate of any irrep μ is equivalent to the irrep μ, the Hermitian conjugate of a component of an irreducible tensor operator with rank μ is in the subspace spanned by the irreducible tensor operators with rank μ.

To find an irreducible tensor operator basis in $\mathcal{B}(\mathcal{H})$ it is helpful to use the Liouville representation of operators in which an operator will be represented by a vector formed by stacking all the rows of its matrix representation (in some specific basis defining the representation) in a column vector [53]. This is equivalent to the Choi isomorphism between operators on $\mathcal{H}$ and vectors on $\mathcal{H} \otimes \mathcal{H}$.

Then the Liouville (or Choi) representation of the super-operator $\mathcal{U}_g$ will be $U(g) \otimes \bar{U}(g)$ where $\bar{U}(g)$ denotes the complex conjugate of $U(g)$ in the basis that defines the representation. So the ranks of all tensor operators which show up in the space $\mathcal{B}(\mathcal{H})$ corresponds to the set of all irreps of G which show up in the representation $g \to U(g) \otimes \bar{U}(g)$. Furthermore, to decompose a particular operator in $\mathcal{B}(\mathcal{H})$ to irreducible tensor operators we can write the Liuoville representation of that operator and find out how it decomposes into the irreducible basis of G defined by the representation $g \to U(g) \otimes \bar{U}(g)$.

One can construct higher ranks of irreducible tensor operators by decomposing the product of irreducible tensor operators with lower ranks. Let $\{T_m^{(\mu_1)}\}$ be the components of a rank μ_1 tensor operator and $\{R_m^{(\mu_2)}\}$ be the components of a rank μ_2 tensor operator. Finally, let $C^{\mu_3,m_3,\alpha}_{\mu_1,m_1;\mu_2,m_2}$ be the Clebsch-Gordon coefficients (see e.g. [47]). Then the set of operators $\{S_m^{(\mu_3,\beta)}\}$ defined by

$$S_m^{(\mu_3,\alpha)} = \sum_{m_1,m_2,\mu_1,\mu_2} C^{\mu_3,m_3,\alpha}_{\mu_1,m_1;\mu_2,m_2} T_{m_1}^{(\mu_1)} R_{m_2}^{(\mu_2)} \tag{4.7}$$

are components of a rank μ_3 irreducible tensor operator.

Finally, we present the Wigner-Eckart theorem which gives a useful tool to find the irreducible tensor operator basis (See e.g. [11]):

Theorem 19 *(**Wigner-Eckart**) Let G be a finite group or a compact Lie group. Let $T_{m_1}^{(\mu_1,\alpha)}$ be an element of a tensor operator. Then*

$$\langle \mu_3, m_3 | T_{m_1}^{(\mu_1,\alpha)} | \mu_2, m_2 \rangle = \sum_{\beta} \left(C^{\mu_3,m_3,\beta}_{\mu_1,m_1;\mu_2,m_2} \right)^* \left(\mu_3 | T^{(\mu_1,\alpha)} | \mu_2 \right)_\beta$$

where β is a multiplicity index that counts the number of the μ_3 irrep can be formed by composing irreps μ_1 and μ_2, $C^{\mu_3,m_3,\beta}_{\mu_1,m_1;\mu_2,m_2}$ are the Clebsch-Gordon coefficients for this composition and $\left(\mu_3 | T^{(\mu_1,\alpha)} | \mu_1\right)_\beta$ is a number which is independent of m_1, m_2, m_3.

Note that the left hand side of the equality can be interpreted as the matrix elements of the unitary acting on $\mathcal{B}(\mathcal{H})$ which transforms the orthonormal basis $\{|\mu_3, m_3\rangle\langle\mu_2, m_2|\}$ to the orthonormal basis $\{T^{(\mu_1,\alpha)}_{m_1}\}$.

4.1.1 Example: SO(3)

In the case of SO(3), the complex conjugate of any representation is unitarily equivalent to the original representation: Suppose $\bar{U}(g)$ is the complex conjugate of $U(g)$ in the basis in which L_z is diagonal and all the matrix elements of L_x are real numbers. Then

$$\forall g \in \mathrm{SO}(3) \quad \bar{U}(g) = e^{-i\pi L_y} U(g) e^{-i\pi L_y} \tag{4.8}$$

Let $g \to U(g)$ be an arbitrary projective unitary representation of SO(3) on $\mathcal{H}$. The above discussion implies that one way to find the ranks of tensor operators and their multiplicities for the basis $\{T^{(\mu,\alpha)}_m\}$ which spans $\mathcal{B}(\mathcal{H})$ is to find the irreps and their multiplicities which show up in the representation

$$g \to U(g) \otimes U(g)$$

An important special case, which we use later, is when $\mathcal{H}$ carries a spin-j irrep of SO(3). Then the above observation implies that $\mathcal{B}(\mathcal{H})$ is spanned by

$$\{T^{(\mu)}_m : (\mu, m) : 0 \le \mu \le 2j, -\mu \le m \le \mu\}$$

and there is no multiplicity. In other words, the maximum rank of the irreducible tensor operators on this space is $2j$.

Note that the operators $\{T^{(\mu)}_m\}$ are uniquely defined only when we fix the basis we use to represent the matrix elements $u^{(\mu)}_{m'm}(g)$ in Eq.(4.2). In the case SO(3) we always use the basis in which the matrix representation of L_z is diagonal and the matrix elements of L_x are all real numbers.

Then, it follows that in this basis

$$\begin{aligned}
&\mu = 0 : && T^{(\mu=0)} = c_0 \mathbb{I} \\
&\mu = 1 : && T^{(\mu=1)}_{m=0} = c_1 L_z, \quad T^{(\mu=1)}_{m=1} = c_1 \frac{1}{\sqrt{2}} L_+, \quad T^{(\mu=1)}_{m=-1} = c_1 \frac{-1}{\sqrt{2}} L_-
\end{aligned}$$

where $\mathbb{I}$ is the identity operator on $\mathcal{H}$, $L_\pm \equiv L_x \pm i L_y$ and c_0, c_1 are normalization factors [47].

One can generate all higher rank tensor operators on this space, by considering the products of $T^{(\mu=1)}_{m_1} T^{(\mu=1)}_{m_2} \cdots$ and decomposing them to irreducible tensor operators using Eq.(4.7). Following this method one can show that the rank-2 irreducible tensor operators are

$$\mu = 2: \quad T^{(\mu=2)}_{m=\pm 2} = c_2 \frac{1}{2} L^2_{\pm}, \quad T^{(\mu=2)}_{m=\pm 1} = c_2 \frac{\pm 1}{2} (L_{\pm} L_z + L_z L_{\pm}), \quad T^{(\mu=2)}_{m=0} = c_2 \frac{1}{\sqrt{6}} \left(3L_z^2 - L^2\right)$$

where $L^2 = L_x^2 + L_y^2 + L_z^2$ is the total angular momentum and c_2 is a normalization factor (see e.g. [47]).

4.2 A representation of G-covariant super-operators

In this section we introduce a representation of G-covariant super-operators which will be useful in the next chapter.

Recall that a super-operator $\mathcal{E}$ is G-covariant if it commutes with the super-operator representation of the group G, i.e.

$$\forall g \in G: \quad \mathcal{E} \circ \mathcal{U}_g = \mathcal{U}_g \circ \mathcal{E} \tag{4.9}$$

Then Schur's lemma imply that $\mathcal{E}$ should be block diagonal in any basis of the operator space $\mathcal{B}(\mathcal{H})$ which decomposes the representation $g \to \mathcal{U}_g$ into the irreps of G. But this is the definition of an irreducible tensor operator basis and therefore G-covariant channels are block diagonal in the irreducible tensor operator bases. The following lemma states this result.

Lemma 20 *Let $g \to U_{in}(g)$ and $g \to U_{out}(g)$ be projective unitary representations of group G on the Hilbert spaces $\mathcal{H}_{in}$ and $\mathcal{H}_{out}$. Let $\{T^{(\mu,\alpha)}_m\}$ and $\{S^{(\mu,\beta)}_m\}$ be the corresponding normalized irreducible tensor operator bases for $\mathcal{B}(\mathcal{H}_{in})$ and $\mathcal{B}(\mathcal{H}_{out})$. Consider a linear super-operator $\mathcal{E}: \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ which is G-covariant, i.e. $\forall g \in G: \ \mathcal{E}\left(U_{in}(g) \cdot U^{\dagger}_{in}(g)\right) = U_{out}(g) \mathcal{E}(\cdot) U^{\dagger}_{out}(g)$. Then*

$$\mathcal{E}(X) = \sum_{\mu,m,\alpha} tr\left(T^{(\mu,\alpha)\dagger}_m X\right) \left[\sum_{\beta} c^{(\mu)}_{\beta\alpha} \ S^{(\mu,\beta)}_m\right] \tag{4.10}$$

where $c^{(\mu)}_{\beta\alpha} \equiv tr\left(S^{(\mu,\beta)\dagger}_m \mathcal{E}(T^{(\mu,\alpha)}_m)\right)$ (which turns out to be independent of m).

Proof.

Since $\{S_m^{(\mu,\alpha)}\}$ is a basis for $\mathcal{B}(\mathcal{H}_{out})$ then for any map $\mathcal{E}$

$$\mathcal{E}(T_m^{(\mu,\alpha)}) = \sum_{\mu',m',\beta} c_{(\mu,\mu';m,m';\alpha,\beta)} S_{m'}^{(\mu',\beta)} \tag{4.11}$$

for some coefficients $c(\mu,\mu';m,m';\alpha,\beta)$. Now we apply the super-operator $\mathcal{U}_g$ to both sides of the above equation. Applying $\mathcal{U}_g$ on the left hand side and using G-covariance of $\mathcal{E}$ we get

$$\mathcal{U}_g(\mathcal{E}(T_m^{(\mu,\alpha)})) = \mathcal{E}(\mathcal{U}_g(T_m^{(\mu,\alpha)})) = \sum_{m''} u_{m''m}^{(\mu)}(g)\ \mathcal{E}(T_{m''}^{(\mu,\alpha)}) \tag{4.12}$$

On the other hand, applying $\mathcal{U}_g$ to the right-hand side of Eq.(4.11) we get

$$\mathcal{U}_g(\sum_{\mu',m',\beta} c_{(\mu,\mu';m,m';\alpha,\beta)} S_{m'}^{(\mu',\beta)}) = \sum_{\mu',m',\beta} c_{(\mu,\mu';m,m';\alpha,\beta)} \sum_{m''} u_{m''m'}^{(\mu')}(g) S_{m''}^{(\mu',\beta)}$$

Equating the right hand sides of the above two equations and using the orthogonality of the functions $\{u_{mm''}^{(\mu)}(g)\}$ we find that $c_{(\mu,\mu';m,m';\alpha,\beta)}$ can be written as

$$c_{(\mu,\mu';m,m';\alpha,\beta)} = \delta_{mm'}\delta_{\mu\mu'} c_{\beta\alpha}^{(\mu)} \tag{4.13}$$

So we conclude that

$$\mathcal{E}(T_m^{(\mu,\alpha)}) = \sum_{\beta} c_{\beta\alpha}^{(\mu)} S_m^{(\mu,\beta)} \tag{4.14}$$

Note that the orthonormality of the basis $\{S_m^{(\mu,\alpha)}\}$ implies

$$c_{\beta\alpha}^{(\mu)} = \mathrm{tr}\left(S_m^{(\mu,\beta)\dagger}\mathcal{E}(T_m^{(\mu,\alpha)})\right) \tag{4.15}$$

which holds for all m. Finally, we notice that the orthonormality of the basis $\{T_m^{(\mu,\alpha)}\}$ together with linearity of $\mathcal{E}$ implies

$$\mathcal{E}(X) = \sum_{\mu,m,\alpha} \mathrm{tr}\left(T_m^{(\mu,\alpha)\dagger} X\right) \mathcal{E}(T_m^{(\mu,\alpha)}) \tag{4.16}$$

These last three equations together prove the lemma. ■

Lemma 20 implies that any linear G-covariant super-operator can be uniquely specified by specifying the set of matrices $\{c^{(\mu)}\}$ for the set of all μ which show up as ranks of irreducible tensor operator basis in both input and output spaces. In the next chapter we use this representation of G-covariant super-operators to study asymmetry properties of quantum states. It can also have applications in other fields such as tomography of G-covariant channels or equivalently tomography of the symmetrized version of a channel (See [45, 46]).

Example 21 *Consider a rotationally covariant super-operator from $\mathcal{B}(\mathcal{H}_{j_1})$ to $\mathcal{B}(\mathcal{H}_{j_2})$ where the input and output spaces $\mathcal{H}_{j_1}$ and $\mathcal{H}_{j_2}$ are spin-j_1 and spin-j_2 irreps of SO(3) respectively.*

Then, from section 4.1.1 we know that the tensor operators for both input and output spaces do not have multiplicity and their rank varies between $\mu_1^{min} = 0$ and $\mu_1^{max} = 2j_1$ in the input space and between $\mu_2^{min} = 0$ and $\mu_2^{max} = 2j_2$ in the output space. So lemma 20 implies that an arbitrary rotationally covariant super-operator from $\mathcal{B}(\mathcal{H}_{j_1})$ to $\mathcal{B}(\mathcal{H}_{j_2})$ can be described by coefficients $c^{(\mu)}$ where μ varies between $\mu^{(min)} = 0$ and $\mu^{(max)} = \min\{\mu_1^{max}, \mu_2^{max}\}$. Now if this super-operator is a channel, i.e. it is trace-preserving and completely positive then we can put more constraints on the coefficients $c^{(\mu)}$. First, we use the fact that any completely positive super-operator maps Hermitian operators to Hermitian operators. This implies that all the coefficients $\{c^{(\mu)}\}$ should be real. On the other hand, the fact that a quantum channel is trace-preserving fixes one coefficient, i.e. $c^{(\mu=0)}$. So any SO(3) covariant channel on these spaces can be described by

$$2\min\{j_1, j_2\}$$

real numbers. The special case of this result for $j_1 = j_2$ has been observed previously in [53].

In particular, if the input space is a spin-half system, the channel can be described by only one real parameter. Note that in the absence of symmetry the number of parameters one needs to specify in order to specify the channel acting on a these spaces scales as $j_1^2 j_2^2$.

Let $\{T_m^{(\mu)}\}$ and $\{S_m^{(\mu)}\}$ be the irreducible tensor operator basis for $\mathcal{B}(\mathcal{H}_{j_1})$ and $\mathcal{B}(\mathcal{H}_{j_2})$ and $\{c^{(\mu)} : \mu = 1 \cdots 2\min\{j_1, j_2\}\}$ be the coefficients describing the rotationally invariant super-operator $\mathcal{E}$ from $\mathcal{B}(\mathcal{H}_{j_1})$ to $\mathcal{B}(\mathcal{H}_{j_2})$. It follows from lemma 20 that if $\mathcal{E}(\rho) = \sigma$ then

$$tr\left(\sigma S_m^{(\mu)\dagger}\right) = c^{(\mu)} tr\left(\rho T_m^{(\mu)\dagger}\right) \tag{4.17}$$

Finally, recall that the trace norm is non-increasing under positive and trace-preserving super-operators. This implies that if the super-operator $\mathcal{E}$ is positive and trace-preserving then $\forall(\mu, m) : \|\mathcal{E}(T_m^{(\mu)})\| \leq \|T_m^{(\mu)}\|$ which by virtue of lemma 20 implies

$$\forall(\mu, m) : \left|c^{(\mu)}\right| \leq \frac{\|T_m^{(\mu)}\|}{\|S_m^{(\mu)}\|} \tag{4.18}$$

In particular, if the input and output spaces are the same, i.e. $j_1 = j_2$, then

$$\forall(\mu, m) : \left|c^{(\mu)}\right| \leq 1 \tag{4.19}$$

Consider the case where the output space of the G-covariant super-operator $\mathcal{E}_1$ matches the input space of $\mathcal{E}_2$ such that the composition $\mathcal{E}_2 \circ \mathcal{E}_1$ is well-defined. If $\mathcal{E}_1$ is described by the set of matrices $\{c^{(\mu)}\}$ and $\mathcal{E}_2$ is described by the set of matrices $\{d^{(\mu)}\}$ then $\mathcal{E}_2 \circ \mathcal{E}_1$ is described by the set of matrices $\{d^{(\mu)}c^{(\mu)}\}$. This implies that in cases such as the example above, where all tensor operators are multiplicity free, then all G-covariant super-operators commute with each other. Furthermore, this observation implies that a master equation which describes a G-covariant dynamics can be decomposed to a set of uncoupled differential equations for each of these matrices.

Example 22 *Suppose a spin-j system has a rotationally invariant open system dynamics. As we have seen in the above, any such dynamics at any time t can be specified by $2j$ real coefficients $c^{(\mu)}(t)$, describing a semi-group of superoperators $\{\mathcal{E}_t\}$. Furthermore, assume this dynamics is Markovian, i.e. the state at $t + \Delta$ can be expressed as a function of the state at time t, for arbitrary t and $0 \leq \Delta$. Because the $c^{(\mu)}$'s are multiplicative, this implies that*

$$\frac{d\ c^{(\mu)(t)}}{dt} = f^{(\mu)}(t)c^{(\mu)}(t) \tag{4.20}$$

for some real function $f^{(\mu)}(t)$. Therefore, one can conclude that

$$c^{(\mu)}(t) = e^{-\int_0^t ds f^{(\mu)}(s)} \tag{4.21}$$

where we have used the fact that at $t = 0$ the map is the identity map. Note that to get this result we have only used linearity, rotational symmetry and Markovianity of the map. The fact that the dynamics should be completely positive can put stronger conditions on the functions $f^{(j)}(t)$.

4.3 Kraus Representation of G-covariant channels

Any quantum channel (i.e. completely positive-trace preserving super-operator) $\mathcal{E}$ admits a Kraus representation, [17, 18, 19] i.e. theres exists operators $\{K_\lambda\}$ such that

$$\mathcal{E}(\cdot) = \sum_\lambda K_\lambda(\cdot)K_\lambda^\dagger \tag{4.22}$$

where the Kraus operators satisfy the normalization condition

$$\sum_\lambda K_\lambda^\dagger K_\lambda = \mathbb{I} \tag{4.23}$$

The Kraus operators $\{K_\mu\}$ can be chosen to be linearly independent. Let $\{K_\lambda\}$ be $\{K'_\nu\}$ two sets of operator and assume the operators in each set satisfy the above normalization condition and also are linearly independent. Then these two sets of Kraus's operators describe the same quantum channel if and only if there exists a unitary matrix V which transforms one set to the other such that

$$K'_\nu = \sum_\mu V_{\lambda\nu} K_\lambda \tag{4.24}$$

It is shown in [16] that if $\mathcal{E}$ is a G-covariant channel then its Kraus operators can be chosen to be elements of irreducible tensor operators as described in the following lemma

Lemma 23 *A G-covariant quantum channel admits a Kraus decomposition with Kraus operators $\{K_m^{(\mu,\alpha)}\}$, where μ denotes the (non-projective) unitary irreps of G, m labels elements of a basis for this irrep, and α is a multiplicity index, satisfying*

$$\mathcal{U}_g\left(K_m^{(\mu,\alpha)}\right) = \sum_{m'} u^{(\mu)}_{m'm}(g) K_{m'}^{(\mu,\alpha)} \quad \forall g \in G \tag{4.25}$$

In the other words, for each pair of (μ,α) the set $\{K_m^{(\mu,\alpha)}\}$ is an irreducible tensor operator.

Proof. Let the set of linearly independent operators $\{K_\lambda\}$ be a Kraus decomposition of the G-covariant map $\mathcal{E}$ such that

$$\mathcal{E}(\cdot) = \sum_\mu K_\mu(\cdot)K_\mu^\dagger \tag{4.26}$$

Since $\mathcal{E}$ is G-covariant then $\forall g \in G:\ \mathcal{U}_g \circ \mathcal{E} \circ \mathcal{U}_{g^{-1}} = \mathcal{E}$. This implies that for any arbitrary group element $g \in G$ the set $\{\mathcal{U}_g(K_\lambda)\}$ is also a valid a Kraus representation of $\mathcal{E}$. But Kraus representations of the same channel are all related by unitaries [17] and so

$$\mathcal{U}_g(K_\lambda) = \sum_\lambda V_{\lambda'\lambda}(g) K_{\lambda'} \tag{4.27}$$

for some unitary matrix $V(g)$ with matrix elements $V_{\lambda'\lambda}(g)$. The linear independence of $\{K_\lambda\}$ implies that for any g there is a unique unitary $V(g)$ which satisfies the above equation. It follows that $g \to V(g)$ is a (non-projective) unitary representation of group G. Now using the unitary freedom in choosing the basis $\{K_\mu\}$ we can choose a basis in which the representation $g \to V(g)$ of group is block-diagonal in the unitary irreps of G. We denote this basis by $\{K_m^{(\mu,\alpha)}\}$ where μ is the irrep label, α is the multiplicity label. This completes the proof. ■

Example 24 *Consider a system with spin-j representation of SO(3). Then as we have seen in the section 4.1.1, the irreducible tensor operators on this space has rank from 0 to $2j$ and there is no multiplicity. So the most general rotationally-covariant channel on this space can be written as*

$$\mathcal{E} = \sum_{\mu=0}^{2j} q_\mu \ \mathcal{E}^{(\mu)} \tag{4.28}$$

where for each μ, $\mathcal{E}^{(\mu)}$ is a fixed completely positive map whose Kraus operators include only rank μ irreducible tensor operators, i.e.

$$\mathcal{E}^{(\mu)}(\cdot) \equiv \sum_m T_m^{(\mu)}(\cdot)T_m^{(\mu)\dagger} \tag{4.29}$$

and q_μ are some non-negative real numbers. The fact that $\mathcal{E}$ should be trace-preserving put one extra condition on the coefficients $\{q_j\}$. So, it follows that the most general rotationally-covariant channel acting on a spin-j system is specified by at most $2j$ coefficients. This is in total agreement with the result of example 21 and the result of [53].

4.4 Stinespring dilation of G-covariant channels

As we have mentioned in chapter 1, if we couple the object system with an environment using a Hamiltonian which has the symmetry G and if the environment is initially uncorrelated with the system and prepared in a state that is G-invariant then the total effect of this time evolution on the object system is described by a G-covariant quantum operation. Intuitively this is clear, because there is nothing in such a dynamics that can break the symmetry.

As it turns out, *every* G-covariant quantum operation can in fact be realized in this way, i.e. by first coupling the system to an uncorrelated environment in a G-invariant state via a G-invariant unitary and secondly discarding the environment. This is a consequence of a version of Stinespring's dilation theorem applied to G-covariant operations [48]. This result provides an operational prescription for realizing every such operation. Here, we present the formal statement of the result and provide a new proof which works based on the lemma 23.

Theorem 25 *Let $g \to U(g)$ be the projective unitary representation of the symmetry G on the Hilbert space $\mathcal{H}$ and $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a G-covariant channel. Then, there exists*

a symmetric dilation *of* $\mathcal{E}$ *in the following sense: There exists a finite dimensional Hilbert space* $\mathcal{H}_{env}$ *with a (non-projective) unitary representation of* G *given by* $g \to U_{env}(g)$ *and a* G*-invariant pure state* $|\eta\rangle$ *in this space and a* G*-invariant unitary* V *acting on* $\mathcal{H} \otimes \mathcal{H}_{env}$ *such that*

$$\mathcal{E}(\rho) = tr_{env}\left(V\rho \otimes |\eta\rangle\langle\eta| V^\dagger\right) \tag{4.30}$$

Proof.

According to the lemma 23, $\mathcal{E}$ admits a Kraus decomposition with Kraus operators $\{K_m^{(\mu,\alpha)}\}$, where μ denotes irreps, m labels elements of a basis for the irrep, and α labels multiplicities, satisfying

$$U(g) K_m^{(\mu,\alpha)} U^\dagger(g) = \sum_{m'} u^{(\mu)}_{m'm}(g) K_{m'}^{(\mu,\alpha)} \quad \forall g \in G \tag{4.31}$$

where $U^{(\mu)}$ is an irreducible (non-projective) unitary representation of G. Then map $\mathcal{E}$ can be written as

$$\mathcal{E}(\rho) = \sum_{\mu,\alpha} \sum_{m} K_m^{(\mu,\alpha)} \ \rho \ K_m^{(\mu,\alpha)\dagger} \tag{4.32}$$

Define

$$\mathcal{H}_{\text{env}} \equiv \mathcal{H}_{\text{inv}} \bigoplus_{(\mu,\alpha)\in \text{decom}(\mathcal{E})} \mathcal{H}^{(\mu,\alpha)} \tag{4.33}$$

where $\mathcal{H}_{\text{inv}}$ is a one-dimensional subspace on which the symmetry G has the trivial representation and each $\mathcal{H}^{(\mu,\alpha)}$ admits a representation of G corresponding to the (non-projective) unitary irrep μ of G and where the summation is over all irreps μ and multiplicities α which show up in the decomposition 4.32 of $\mathcal{E}$. Let $\{|\overline{\mu, m, \alpha}\rangle \in \mathcal{H}^{(\mu,\alpha)}\}$ be an orthonormal basis for $\mathcal{H}^{(\mu,\alpha)}$ and the vector $|\eta\rangle$ be a normalized vector in the one-dimensional subspace $\mathcal{H}_{\text{inv}}$.

Let $g \to U_{\text{env}}(g)$ be the (non-projective) unitary representation of G on $\mathcal{H}_{\text{env}}$ defined by

$$\forall g \in G: \ U_{\text{env}}(g) \equiv |\eta\rangle\langle\eta| \bigoplus_{(\mu,\alpha)\in \text{decom}(\mathcal{E})} \left(\sum_{m_2 m_1} \overline{u}^{(\mu)}_{m_2 m_1}(g) \ |\overline{\mu, m_2, \alpha}\rangle\langle\overline{\mu, m_1, \alpha}| \right)$$

where $\overline{u}^{(\mu)}_{m_2 m_1}(g)$ is the complex conjugate of $u^{(\mu)}_{m_2 m_1}(g)$.

Define

$$S \equiv \sum_{\mu,m,\alpha} K_m^{(\mu,\alpha)} \otimes |\overline{\mu, m, \alpha}\rangle\langle\eta| \tag{4.34}$$

It follows that S is a G-invariant isometry from the subspace $\mathcal{H}\otimes\mathcal{H}_{\rm inv}$ to the total Hilbert space, i.e. $\mathcal{H}\otimes\mathcal{H}_{\rm env}$: The fact that S is an isometry is an immediate consequence of the normalization of Kraus operators

$$\sum_{\mu,\alpha,m} K_m^{(\mu,\alpha)\dagger} K_m^{(\mu,\alpha)} = \mathbb{I}_{\mathcal{H}} \tag{4.35}$$

where $\mathbb{I}_{\mathcal{H}}$ is the identity on $\mathcal{H}$. This implies that $S^\dagger S = \mathbb{I}_{\mathcal{H}}\otimes|\eta\rangle\langle\eta|$. To see that S is G-invariant we consider

$$U(g)\otimes U_{\rm env}(g)\ S\ U^\dagger(g)\otimes U_{\rm env}^\dagger(g) = \sum_{\mu,m,\alpha}\sum_{m'}\sum_{m''}\left[u^{(\mu)}_{m'm}(g)\overline{u}^{(\mu)}_{m''m}(g)\right] K_{m'}^{(\mu,\alpha)}\otimes|\overline{\mu,m'',\alpha}\rangle\langle\eta|$$

where we have used the fact that $|\eta\rangle$ is invariant under $U_{\rm env}(g)$. But from the unitarity of the matrix $u^{(\mu)}$ it follows that $\sum_m u^{(\mu)}_{m'm}(g)\overline{u}^{(\mu)}_{m''m}(g) = \delta_{m',m''}$ and therefore

$$\forall g\in G:\quad U(g)\otimes U_{\rm env}(g)\ S\ U^\dagger(g)\otimes U_{\rm env}^\dagger(g) = \sum_{\mu,m',\alpha} K_{m'}^{(\mu,\alpha)}\otimes|\overline{\mu,m',\alpha}\rangle\langle\eta| = S \tag{4.36}$$

and so S is a G-invariant isometry. Now, as we have shown in lemma 91 in the appendix A.1.2, the G-invariant isometry S can be extended to a G-invariant unitary V such that $V\Pi = S\Pi$ where Π is the projector to $S^\dagger S = \mathbb{I}_{\mathcal{H}}\otimes|\eta\rangle\langle\eta|$. Finally, using the definition of S, Eq.(4.34), it is straightforward to check that V satisfies Eq.(4.30). This completes the proof of theorem. ■

Chapter 5

Modes of asymmetry: Fourier analysis for the study of linear covariant maps

The two properties of linearity and symmetry of an operation together imposes many non-trivial constraints on the way that operations map a given state to another. It turns out that under these assumptions one can decompose the input and output spaces to different *modes*, such that any given mode at the input can generate only that particular mode at the output. This is why, for example, Fourier analysis turns out to be extremely useful to study Linear-Time-Invariant systems: the symmetry of time invariance and linearity together imply that in these systems a signal with the frequency ω at the input can only generate a signal with the same frequency ω at the output (See Fig. 5.1).

In this chapter we study a similar notion in the context of G-covariant linear super-operators. Indeed, the fact that the input and output spaces of any G-covariant super-operator can be decomposed to different independent modes which do not mix under the G-covariant super-operator is already shown in lemma 20. In the present chapter we explore the consequences of this lemma.

This provides us with a powerful tool for the study of asymmetry. In particular, this framework is especially useful for the study of quantum reference frames, that is, understanding asymmetric quantum states of finite-dimensional systems as physical resources. For example, these tools allow one to determine which aspects of the quantum reference frame state are relevant for the degree of success that can be achieved in a reference frame alignment protocol and more generally in covariant quantum estimation problems. Simi-

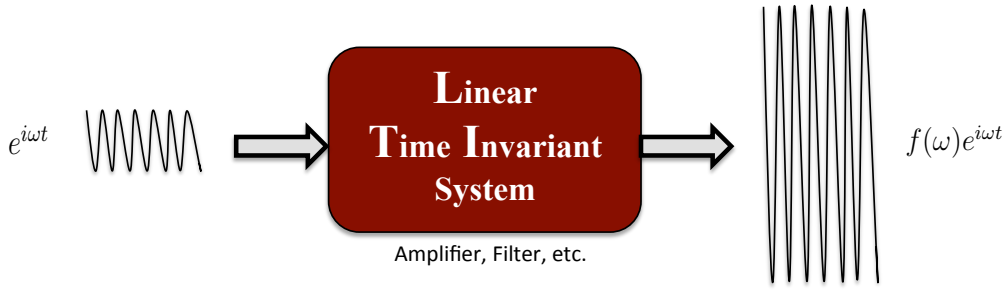

Figure 5.1: Any linear time invariant system transforms an input signal in frequency ω to an output signal in the same frequency. In other words, linearity together with time invariance implies that the system cannot change the frequency of the input. It follows that any linear time invariant system can be uniquely specified by a complex function $f(\omega)$. This explains why Fourier analysis is extremely useful for the study of these systems.

larly, they allow one to determine which aspects of the quantum reference frame state are relevant for being able to simulate asymmetric dynamics or asymmetric measurements.

Previous work has sometimes identified, for certain tasks, which properties of the state of a quantum reference frame are relevant for performing that task, but these insights were achieved in an ad hoc manner (See e.g. [50] and [53]). The framework presented in this chapter provides a systematic way of determining what aspects of the quantum state are relevant for any given physical task.

We start by looking to the specific example of U(1)-symmetry with (non-projective) unitary representation on space and explain the main ideas based on this example. Then we present a generalization to an arbitrary finite or compact Lie group with arbitrary projective representation.

5.1 Modes of asymmetry for the group U(1)

Let $e^{i\theta} \to U(\theta)$ be an arbitrary unitary representation of the group $U(1)$. Let $\{|n,\alpha\rangle\}$ be an orthonormal basis in which the representation $e^{i\theta} \to U(\theta)$ is decomposed into irreducible representations as

$$U(\theta) = \sum_{n,\alpha} e^{in\theta} |n,\alpha\rangle\langle n,\alpha| \tag{5.1}$$

where the integer n specifies the irrep of $U(1)$ and α is the multiplicity index.

Let $\mathcal{B}(\mathcal{H})$ be the space of linear operators on $\mathcal{H}$, which is clearly spanned by $\{|n,\alpha\rangle\langle m,\beta|\}$. Consider the subspace in $\mathcal{B}(\mathcal{H})$ spanned by operators $\{\forall n,\alpha,\beta:\ |n+k,\alpha\rangle\langle n,\beta|\}$. We denote this subspace by $\mathcal{B}^{(k)}$. We call any operator in this subspace a *mode k operator*.

Suppose $A^{(k)}$ is a mode k operator, i.e., it lives in $\mathcal{B}^{(k)}$. We may then write it as

$$A^{(k)} = \sum_{n,\alpha,\beta} |n+k,\alpha\rangle\langle n,\beta|\ \mathrm{tr}(A|n,\beta\rangle\langle n+k,\alpha|). \tag{5.2}$$

It also follows that $U(\theta)A^{(k)}U^\dagger(\theta) = e^{ik\theta}A^{(k)}$. On the other hand, if an operator A satisfies this equality for all θ then by virtue of the linear independence of functions $\{e^{ik\theta}\}$ we can conclude that A necessarily lives in the subspace $\mathcal{B}^{(k)}$. Therefore, we have

$$A^{(k)} \in \mathcal{B}^{(k)} \quad \Longleftrightarrow \quad \forall\theta:\ U(\theta)A^{(k)}U^\dagger(\theta) = e^{ik\theta}A^{(k)} \tag{5.3}$$

Let $A = \sum_k A^{(k)}\ :\ \ A^{(k)} \in \mathcal{B}^{(k)}$ be the decomposition of an arbitrary operator A into its components in the different modes. Note that for all $k \neq 0$ we have $\mathrm{tr}(A^{(k)}) = 0$. Furthermore

$$U(\theta)AU^\dagger(\theta) = \sum_k e^{ik\theta}A^{(k)}. \tag{5.4}$$

So to decompose a given operator A to its modes we can use the following relation

$$\forall k:\quad A^{(k)} = \frac{1}{2\pi}\int d\theta\ e^{-ik\theta}\ U(\theta)AU^\dagger(\theta) \tag{5.5}$$

Note that for any Hermitian operator A it holds that ${A^{(k)}}^\dagger = A^{(-k)}$.

Suppose $\mathcal{E}$ is a U(1)-covariant super-operator, i.e.

$$\forall\theta:\quad \mathcal{E}\left(U(\theta)(\cdot)U^\dagger(\theta)\right) = U(\theta)\mathcal{E}\left(\cdot\right)U^\dagger(\theta)$$

Then, if both sides of this equation act on an arbitrary operator in $A^{(k)} \in \mathcal{B}^{(k)}$ we get

$$e^{ik\theta}\mathcal{E}(A^{(k)}) = U(\theta)\mathcal{E}(A^{(k)})U^\dagger(\theta) \tag{5.6}$$

Then Eq.(5.3) implies that $\mathcal{E}(A^{(k)})$ also lives in $\mathcal{B}^{(k)}$. [1]

Note that this result did not require $\mathcal{E}$ to be a completely positive map nor to be trace-preserving, but it certainly applies in these cases. Recall that the term *quantum operation* refers to a completely-positive trace-nonincreasing superoperator, and *quantum channel*

[1] This also follows from lemma 20.

to refer to the deterministic operations. So we can infer that U(1)-covariant quantum operations cannot change the mode of a state; they just map an operator in one mode to another operator in the same mode. In particular, if a U(1)-covariant channel $\mathcal{E}$ maps state ρ to σ then

$$\mathcal{E}(\rho^{(k)}) = \sigma^{(k)} \tag{5.7}$$

where

$$\rho = \sum_k \rho^{(k)} : \rho^{(k)} \in \mathcal{B}^{(k)}, \quad \text{and} \quad \sigma = \sum_k \sigma^{(k)} : \sigma^{(k)} \in \mathcal{B}^{(k)}$$

are the mode decompositions of ρ and σ.

This suggests that we can interpret different k as different modes of asymmetry: they cannot be interconverted to each other under U(1)-covariant quantum channels. In particular, if the initial state does not have a particular mode, then the final state of a U(1)-covariant dynamics also does not have that mode. (Of course, a mode can be eliminated if the associated component is mapped to zero by the dynamics.) Furthermore, a state ρ is U(1)-invariant if and only if it contains only mode $k = 0$.

Let Modes(ρ) be the set of all integer k's for which the state ρ has a nonzero component in mode k (This will always include $k = 0$). So using this notation the above observation can be summarized as the following

Proposition 26 *Assume a state ρ can be transformed to another state σ under a U(1)-covariant operation (deterministic or stochastic). Then*

$$\textit{Modes}(\sigma) \subseteq \textit{Modes}(\rho) \tag{5.8}$$

This proposition can be thought as a refined version of this simple fact that if the initial state of a U(1)-covariant operation is invariant under a U(1)-subgroup then the final state will also be invariant under that U(1)-subgroup. To see this first recall that under the action of the symmetry group, state ρ transforms as

$$U(\theta)\rho U^\dagger(\theta) = \sum_k e^{ik\theta}\rho^{(k)} \tag{5.9}$$

Now suppose a state ρ is invariant under the unitary $U(\frac{2\pi}{l})$ for some integer l such that $U(\frac{2\pi}{l})\rho U^\dagger(\frac{2\pi}{l}) = \rho$. Using Eq. (5.9) and noting that the set $\{\rho^{(k)}\}$ are all linearly independent, we can conclude that for all modes k which are not equal to an integer time l, $\rho^{(k)}$ must be equal to zero. On the other hand, if for all k's which are equal to some integer times l, $\rho^{(k)} = 0$ then the state is invariant under $U(\frac{2\pi}{l})$. So, we conclude that Modes(ρ) uniquely specifies the symmetries of ρ, i.e. all U(1)-subgroups which leaves ρ invariant.

Example 27 *Consider a pure state* $|\psi\rangle = \sum_{n,\alpha} \psi_{n,\alpha}|n,\alpha\rangle$. *Let* $\Delta(\psi)$ *be the difference between the highest and lowest* n *for which* $\sum_\alpha |\psi_{n,\alpha}|^2$ *is nonzero. Then clearly,* $\Delta(\psi) = \max\{Modes(\psi)\}$. *Now proposition 26 implies that if there exists a U(1)-covariant channel which transforms a pure state* $|\psi\rangle$ *to another pure state* $|\phi\rangle$ *with a nonzero probability then* $Modes(\phi) \subseteq Modes(\psi)$. *This implies that* $\max\{Modes(\phi)\} \leq \max\{Modes(\psi)\}$ *and therefore* $\Delta(\phi) \leq \Delta(\psi)$. *This result has been obtained in [16] using a totally different argument*[2]. *So the above proposition capture this result as a particular case.*

We finish this section by a list of useful facts about modes of asymmetry:

1) Modes of asymmetry of a joint system: Suppose ρ_1 and ρ_2 are two states with the mode decompositions

$$\rho_1 = \sum_k \rho_1^{(k)} : \rho_1^{(k)} \in \mathcal{B}^{(k)}, \quad \text{and} \quad \rho_2 = \sum_l \rho_2^{(l)} : \rho_2^{(k)} \in \mathcal{B}^{(k)}$$

We denote the mode decomposition of $\rho_1 \otimes \rho_2$ as $\rho_1 \otimes \rho_2 = \sum_j (\rho_1 \otimes \rho_2)^{(j)}$. Then we can easily see that

$$(\rho_1 \otimes \rho_2)^{(j)} = \sum_k \rho_1^{(k)} \otimes \rho_2^{(j-k)} \tag{5.10}$$

2) Mode decomposition for a weighted twirling operation: Let $p(\theta)$ be an arbitrary probability distribution and

$$\sigma \equiv \int d\theta \; p(\theta) \; U(\theta)\rho U^\dagger(\theta) \tag{5.11}$$

Let

$$\rho = \sum_k \rho^{(k)} : \rho^{(k)} \in \mathcal{B}^{(k)}, \quad \text{and} \quad \sigma = \sum_k \sigma^{(k)} : \sigma^{(k)} \in \mathcal{B}^{(k)}$$

be the mode decomposition of ρ and σ. Then

$$\sigma^{(k)} = p_{-k}\rho^{(k)} \tag{5.12}$$

where $p_k = \int d\theta \; p(\theta)e^{-i\theta k}$ is the kth component of the Fourier transform of $p(\theta)$.

[2] In [16] the the authors first use lemma 23 to find a characterization of the Kraus operators of U(1)-covariant channels and then they find which pure state transformations are possible under quantum channels with this type of Kraus operators.

5.1.1 Asymmetry monotones for different modes

In this section we consider the problem of *quantifying* the amount of asymmetry in each different mode. In other words, we find asymmetry monotones which only measure the degree of asymmetry associated with some specific mode of asymmetry.

One family of such monotones can be built based on the trace-norm. Recall that for an arbitrary operator X the trace-norm of X is $\|X\| \equiv \mathrm{tr}(\sqrt{X^\dagger X})$. As we have seen in chapter 3 this norm is non-increasing under quantum channels (trace preserving, completely positive linear super-operators). So for any arbitrary quantum channel $\mathcal{E}$ we have

$$\|\mathcal{E}(X)\| \leq \|X\|.$$

In the previous section we have seen that if $\mathcal{E}$ is a U(1)-covariant channel which maps state ρ to σ (with the mode decomposition $\rho = \sum_k \rho^{(k)} : \rho^{(k)} \in \mathcal{B}^{(k)}$, and $\sigma = \sum_k \sigma^{(k)} : \sigma^{(k)} \in \mathcal{B}^{(k)}$) then $\forall k : \ \mathcal{E}(\rho^{(k)}) = \sigma^{(k)}$. Now the monotonicity of the trace-norm implies

$$\forall k : \ \|\sigma^{(k)}\| \leq \|\rho^{(k)}\|$$

So we can think of $\|\rho^{(k)}\|$ as a measure of the amount of asymmetry of the state ρ in the mode k. Note that for arbitrary state ρ, its $k = 0$ component, i.e. $\rho^{(0)}$ is a valid quantum state and so $\|\rho^{(0)}\| = 1$ for all ρ.

Now suppose a given state ρ can be transformed to another state σ under a U(1)-covariant channel with probability p. If this is possible then there exists a U(1)-covariant channel which maps state ρ to

$$\tilde{\sigma} \equiv p\ \sigma \otimes |\mathrm{succ}\rangle\langle\mathrm{succ}| + (1-p)\frac{I}{d} \otimes |\mathrm{fail}\rangle\langle\mathrm{fail}|$$

where $|\mathrm{succ}\rangle, |\mathrm{fail}\rangle$ are two orthonormal states which are invariant under the symmetry transformations and $\frac{I}{d}$ is the completely mixed state in the space where σ belongs to and is clearly invariant under all symmetry transformations. Now the fact that this channel is U(1)-covariant implies that for all k: $|\tilde{\sigma}^{(k)}| \leq |\rho^{(k)}|$. However, because states $|\mathrm{succ}\rangle, |\mathrm{fail}\rangle$ and $\frac{I}{d}$ are invariant under the symmetry transformations this implies that for all $k \neq 0$ it holds that

$$\|\tilde{\sigma}^{(k)}\| = \left\| \frac{1}{2\pi} \int d\theta e^{-i\theta k} U(\theta) \tilde{\sigma} U^\dagger(\theta) \right\| = p\|\sigma^{(k)}\| \leq \|\rho^{(k)}\|$$

So to summarize, we have shown that

Proposition 28 *Suppose there is a U(1)-covariant channel which maps a state ρ to state σ with probability p. Then it holds that*

$$\forall k: \quad p|\rho^{(k)}| \leq |\sigma^{(k)}| \tag{5.13}$$

This proposition can be thought as a quantitative version of proposition 26.

In the following we calculate $\|\rho^{(k)}\|$ for arbitrary state ρ in the case where the representation is multiplicity free and so $U(\theta) = \sum_n e^{i\theta n}|n\rangle\langle n|$. (Note that all the previous results work for any representation of $U(1)$ no matter if the representation has multiplicity or not.) Consider an arbitrary density operator $\rho = \sum_{n,m} \rho_{n,m}|n\rangle\langle m|$. Then

$$\rho^{(k)} = \sum_n \rho_{n+k,n}|n+k\rangle\langle n|$$

Therefore

$$|\rho^{(k)}| = \mathrm{tr}\left(\sqrt{\rho^{(k)}\rho^{(k)\dagger}}\right) = \sum_n |\rho_{n+k,k}| \tag{5.14}$$

In particular, if the state is pure i.e. $\rho = |\psi\rangle\langle\psi|$ where $|\psi\rangle = \sum_n \psi_n|n\rangle$ then

$$|\rho^{(k)}| = \sum_n |\psi_{n+k}||\psi_n| \leq 1 \tag{5.15}$$

where the bound follows from Cauchy-Schwartz inequality.

Example 29 *Consider the sequence of states*

$$\left\{ |\psi_N\rangle \equiv \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle : N \in \mathbb{N} \right\} \tag{5.16}$$

One can easily see that for any given state $|\phi\rangle$ there is a U(1)-covariant channel $\mathcal{E}_N$ which transforms $|\psi_N\rangle$ to a state arbitrary close to $|\phi\rangle$ in the limit of large N, $\mathcal{E}_N$ is given by

$$\mathcal{E}_N(\rho) = \int d\theta \; U(\theta)|\phi\rangle\langle\psi_N|U^\dagger(\theta) \; \rho \; U(\theta)|\psi_N\rangle\langle\phi|U^\dagger(\theta). \tag{5.17}$$

So in a sense, at the limit of large N, the state $|\psi_N\rangle$ has the maximal asymmetry. Now one can easily see that

$$\left\||\psi_N\rangle\langle\psi_N|^{(k)}\right\| = \sum_n |\psi_{n+k}||\psi_n| = 1 - \frac{|k|}{N} \quad |k| \leq N$$
$$= 0 \qquad \textit{otherwise.}$$

So for all modes k for which $|k| \ll N$, the state $|\psi_N\rangle$ has almost the maximal value of asymmetry for mode k with respect to this monotone.

5.1.2 Effect of misalignment of reference frames

To be able to measure a quantity with high precision one fundamental requirement is to have precise reference frames, such as a high precision clock. Any uncertainty of reference frames can limit the precision of the measurements that one can perform.

In this section, we consider the problem of misalignment of reference frames for some phase. So we assume the system under consideration carries a non-trivial representation of the group U(1) given by $e^{i\theta} \rightarrow U(\theta)$. The U(1) group may have different physical interpretations: It may describe a rotation around some axis or a phase shift between states with different numbers of photons.

We assume there is an ideal perfect reference frame possessed by Alice and there is a noisy reference frame possessed by Bob. For example, Bob can be on a satellite and so has access to a clock with low accuracy while Alice is on earth and has access to a high precision atomic clock.

Assume, they know that Bob's reference frame is misaligned relative to Alice reference frame by phase θ with probability $p(\theta)$. This means that a state which is described by ρ relative to Alice's reference frame, with probability $p(\theta)$ will be described by $U(\theta)\rho U^{\dagger}(\theta)$ relative to Bob's reference frame. So the statistics of Bob's measurement is consistent with the statistics he gets from the state

$$\widetilde{\rho} \equiv \int d\theta \; p(\theta) \; U(\theta)\rho U^{\dagger}(\theta) \tag{5.18}$$

if he had perfect reference frame. This explains how the lack of a perfect reference frame can limit Bob's ability to get information about the state ρ.

The state $\tilde{\rho}$ can be rewritten in terms of the mode decomposition of ρ as

$$\widetilde{\rho} = \sum_{k} p_{-k}\rho^{(k)} \tag{5.19}$$

where $\rho^{(k)}$ is the kth component of the mode decomposition of ρ and

$$p_k = \int d\theta \; p(\theta) e^{-i\theta k} \tag{5.20}$$

is the kth component of the Fourier transform of $p(\theta)$.

So to understand how the uncertainty about the phase reference can affect Bob, it is helpful to consider the Fourier transform of the probability distribution $p(\theta)$. For example,

if the Hilbert space of the system under consideration carries a finite number of irreps of U(1), then there will be a finite set of modes in which an arbitrary state can have nonzero components. Then any quantity which quantifies the effect of misalignment described by the probability distribution $p(\theta)$ should only depend on the Fourier component of the probability distribution $p(\theta)$ in those particular modes. In other words, to compare different probability distributions we only need to consider the components of their Fourier transform in these modes.

Example

Consider the representation of U(1) given by $e^{i\theta} \to U(\theta)$ where

$$U(\theta) = \sum_{n=n_{\min}}^{n_{\max}} e^{i\theta n} |n\rangle\langle n|$$

Assume the phase difference between Alice and Bob's local reference frames is θ with probability $p(\theta)$. Now, to quantify the effect of this misalignment on the description of an arbitrary state of this system we only need to consider p_k the Fourier component of $p(\theta)$ for $0 \leq k \leq n_{\max} - n_{\min}$. For example, suppose Bob wants to estimate the phase ϕ of the state

$$\frac{1}{\sqrt{2}} \left(|n = 0\rangle + e^{i\phi} |n = l\rangle \right) \tag{5.21}$$

The information about this phase lives only in the modes $l, -l$. So the only property of the probability distribution $p(\theta)$ which is relevant for this estimation problem is its l'th Fourier component. In particular, if the l component of the Fourier transform of $p(\theta)$ is zero, then Bob cannot get any information about the phase ϕ. This can happen even if the two phase references are highly correlated. For example if

$$p(\theta) = \frac{1}{2}\delta(\theta) + \frac{1}{4}\delta(\theta - \pi/l) + \frac{1}{4}\delta(\theta + \pi/l)$$

then $p(\theta)$ has no component in the mode l and therefore Bob cannot get any information about the phase ϕ. This simple observation shows that a measure of the alignment of two reference frames should be chosen based on the specific operation for which we use the reference frames.

In many practical situations we can assume that the probability distribution $p(\theta)$ is almost Gaussian. In particular, if Bob's knowledge of θ is obtained by averaging over many independent estimations then $p(\theta)$ is Gaussian. Let $\delta\theta$ be the standard deviation

of θ. Then, for Gaussian distributions we know that for all modes with $|k| \ll 1/\delta\theta$, $|p_k| \approx 1$ and therefore for these modes the distribution is effectively a delta function over θ. So in the case of the above example where Bob is interested to estimate the phase of $1/\sqrt{2}\left(|n=0\rangle + e^{i\phi}|n=l\rangle\right)$, if $\delta\theta \ll 1/l$ then the imperfectness of Bob's local frame does not put any limitation on his performance for measuring the phase ϕ.

Alignment by quantum reference frames

If Alice wishes to ensure that Bob's reference frame is aligned with her own, she can send him a *quantum reference frame*, i.e. a quantum system which carries information about her reference frame. For example, Alice can send Bob many copies of the state described by $1/\sqrt{2}(|0\rangle + |1\rangle)$ relative to her reference frame and also tell him the description of this state relative to her reference frame. Then Bob can use these quantum systems to obtain information about the relative phase between his reference frame and Alice's.

Assume Alice and Bob's prior knowledge about the phase difference between their local phase references is described by the probability distribution $p(\theta)$. Consider an arbitrary state described by ρ relative to Alice's reference frame. As we have seen before the imperfectness of Bob's reference frame prevents him from getting a precise description of ρ. Now assume Alice sends Bob a quantum reference frame in the state τ and assume the representation of phase shifts on this system is given by $e^{i\theta} \to V(\theta)$.

To find more precise information about ρ Bob can first use the quantum reference frame τ to align his reference frame with Alice's and then perform some measurement on ρ. But, this procedure does not describe the most general thing Bob can do. The most general process is to perform a joint measurement on the state ρ and the quantum reference frame τ. In this case the information Bob can obtain about the unknown state ρ is the information he can extract from the state

$$\int d\theta \; p(\theta) \left(V(\theta) \otimes U(\theta)\right) \tau \otimes \rho \left(V^\dagger(\theta) \otimes U^\dagger(\theta)\right) \tag{5.22}$$

But this state is equal to

$$\sum_{k_1,k_2} p_{-k_1} \tau^{(-k_2)} \otimes \rho^{(k_1+k_2)}, \tag{5.23}$$

where $\tau = \sum_k \tau^{(k)}$ is the mode decomposition of τ and p_k is the kth component of the Fourier transform of $p(\theta)$. This shows precisely how the information Bob can get from different modes of ρ is determined by different modes of the quantum reference frame and Fourier components of the probability distribution $p(\theta)$.

Example

Suppose Alice and Bob's local reference frames are initially uncorrelated and therefore the prior distribution $p(\theta)$ is uniform.

Assume Bob wants to find information about the phase ϕ of the state

$$\frac{1}{\sqrt{2}}\left(|n=0\rangle + e^{i\phi}|n=2\rangle\right) \tag{5.24}$$

Note that here the information is encoded in the modes 2 and -2. So to enable Bob to encode this information Alice should send him a quantum reference frame which has modes 2 and -2. In particular, the reference frame should not be invariant under $U(\pi)$, because if $U(\pi)\tau U^\dagger(\pi) = \tau$ then the state τ will not have any component in mode 2. But, lack of this symmetry does not imply that the quantum reference frame has mode 2. For example, assume Alice sends Bob the quantum reference frame

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{5.25}$$

This state is not invariant under any subgroup of U(1). But it still does not have any component in the mode $k = 2$ and so it does not help Bob to obtain information about the phase ϕ of the state 5.24. Furthermore, the quantum reference frame might have arbitrarily high asymmetry and still not help Bob. For instance, the state

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|4k\rangle, \tag{5.26}$$

in the limit that $N \to \infty$ has infinite asymmetry by some measures, but because it has no component in the mode $k = 2$ mode, it is not useful for determining the phase ϕ of the state 5.24.

5.2 Modes of asymmetry for an arbitrary group

In this section we generalize the notion of modes of asymmetry which was previously defined for the special case of group U(1) to the case of finite groups and compact Lie groups.

Consider the subspace spanned by $\{T_m^{(\mu,\alpha)} : \forall\alpha\}$ for a fixed m and μ. Then lemma 20 implies that any G-covariant super-operator maps an operator in this subspace to another operator in this subspace. This suggests the following definition of modes of asymmetry

Definition 30 *The (μ, m) mode component of an operator X, denoted $X^{(\mu,m)}$, is defined by*

$$X^{(\mu,m)} \equiv \sum_{\alpha} T_m^{(\mu,\alpha)} tr\left(T_m^{(\mu,\alpha)\dagger} X\right) \tag{5.27}$$

We call the decomposition $X = \sum_{\mu,m} X^{(\mu,m)}$ the mode decomposition *of operator X.*

Note that in the above definition we have assumed the basis $\{T_m^{(\mu,\alpha)}\}$ is an orthonormal basis, i.e.

$$\text{tr}\left(T_m^{(\mu,\alpha)} T_{m'}^{(\mu',\alpha')\dagger}\right) = \delta_{m,m'}\delta_{\mu,\mu'}\delta_{\alpha,\alpha'}.$$

Lemma 20 has a simple interpretation in terms of mode decompositions of operators: A G-covariant super-operator $\mathcal{E}$ maps an operator in a particular mode of asymmetry to an operator in the same mode of asymmetry, i.e. if $Y = \mathcal{E}(X)$ then

$$\forall \mu, m: \quad Y^{(\mu,m)} = \mathcal{E}(X^{(\mu,m)}) \tag{5.28}$$

So we can think of different pairs of (μ, m) as different independent modes which cannot be mixed under a G-covariant linear super-operator. In particular, if an input X has no component in a particular mode then the corresponding output Y also cannot have any component in that mode.

The above definition is independent of the choice of the tensor operators basis, $\{T_m^{(\mu,\alpha)}\}$. In the following lemma, we present another way to define modes of asymmetry which is explicitly basis independent.

Let $\{g \to u^{(\mu)}(g)\}$ be the (non-projective) set of all unitary irreps of finite or compact Lie group G and $\{u^{(\mu)}_{mm'}(g)\}$ be the matrix elements of these unitary irreps. Recall that these matrix elements satisfy the orthonormality relations, i.e.

$$\int dg\ \bar{u}^{(\mu)}_{m_1 m_2}(g) u^{(\nu)}_{m_3 m_4}(g) = \frac{1}{d_\mu}\delta_{\mu,\nu}\delta_{m_1,m_3}\delta_{m_2,m_4} \tag{5.29}$$

Then one can easily see that

Lemma 31 *Let $X = \sum_{\mu,m} X^{(\mu,m)}$ be the mode decomposition of operator X. Then*

$$X^{(\mu,m)} = d_\mu \int dg\ \bar{u}^{(\mu)}_{mm}(g)\ \mathcal{U}_g(X) \tag{5.30}$$

where d_μ is the dimension of the irrep μ, dg is the uniform measure over the group G and the bar represents complex conjugation.

Proof. Consider the equation

$$\mathcal{U}_g(T_m^{(\mu,\alpha)}) = \sum_{m'} u_{m'm}^{(\mu)} T_{m'}^{(\mu,\alpha)}$$

We multiply both sides by $\bar{u}_{nn}^{(\nu)}(g)$ and integrate over G. Now we use the orthonormality relations Eq.(5.29). This implies that

$$\forall \alpha : \quad d_\mu \int dg\ \bar{u}_{nn}^{(\mu)}(g)\ \mathcal{U}_g(T_m^{(\mu,\alpha)}) = \delta_{m,n}\delta_{\mu,\nu} T_m^{(\mu,\alpha)} \tag{5.31}$$

The lemma follows from this equality together with the definition of mode decompositions given by Eq.(5.27). ■

This lemma gives us an alternative method to find the mode decomposition of a given operator.

It is worth emphasizing on an important difference between the mode decomposition for the case of non-Abelian groups and the mode decomposition for the case of Abelian groups such as U(1). This difference is about the action of group on operators in different modes. Since

$$\mathcal{U}_g[T_m^{(\mu,\alpha)}] = \sum_{m'} u_{m'm}^{(\mu)}(g) T_{m'}^{(\mu,\alpha)} \tag{5.32}$$

it follows that modes (μ, m) and (μ', m') for which $\mu \neq \mu'$ do not mix together under the action of the group, but modes for which $\mu = \mu'$ and $m \neq m'$ can mix together under this action. This can happen because in general a symmetry transformation $\mathcal{U}_g$ is not a G-covariant operation, unless the group G is Abelian. In this case, modes are just specified by an irrep label μ.

5.3 Asymmetry monotones for different modes

As we saw in the specific case of the group U(1), one can quantify, for a given state, the amount of asymmetry in each mode by looking to the trace-one norm of the component of the state in that particular mode. In other words, for each mode (μ, m) the function defined by

$$F_{\mu,m}(X) \equiv \|X^{(\mu,m)}\| \tag{5.33}$$

is an asymmetry monotone. Then, the natural generalization of proposition 28 is

Proposition 32 *Suppose there is a G-covariant channel which maps a state ρ to state σ with probability p. Then for all modes (μ, m) it holds that*

$$\forall(\mu,m): \quad p\,\|\sigma^{(\mu,m)}\| \leq \|\rho^{(\mu,m)}\| \tag{5.34}$$

Using definition 30 we can rewrite this bound as

$$\forall(\mu,m): \; p\sum_{\alpha}\mathrm{tr}\left(\sqrt{T_m^{(\mu,\alpha)}T_m^{(\mu,\alpha)\dagger}}\right)\left|\mathrm{tr}\left(T_m^{(\mu,\alpha)}\sigma\right)\right| \;\leq\; \sum_{\alpha}\mathrm{tr}\left(\sqrt{T_m^{(\mu,\alpha)}T_m^{(\mu,\alpha)\dagger}}\right)\left|\mathrm{tr}\left(T_m^{(\mu,\alpha)}\rho\right)\right|$$

5.3.1 Example: spin-j system

Consider the case of spin-j representation of SO(3). Then, as we have seen before, all the modes are multiplicity-free and so

$$\forall(\mu,m): \; F_{\mu,m}(\rho) \equiv \|\rho^{(\mu,m)}\| = \mathrm{tr}\left(\sqrt{T_m^{(\mu)}T_m^{(\mu)\dagger}}\right)\left|\mathrm{tr}\left(T_m^{(\mu)}\rho\right)\right| \tag{5.35}$$

Now, if a state ρ of the spin-j system evolves under a rotationally invariant dynamics to a state σ of the spin-j system with the probability p then for all modes (μ, m) it holds that

$$p\left|\mathrm{tr}\left(T_m^{(\mu)}\sigma\right)\right| \leq \left|\mathrm{tr}\left(T_m^{(\mu)}\rho\right)\right| \tag{5.36}$$

So, for example, in the case of mode $(\mu = 1, m = 0)$, where $T_0^{(1)} = cL_z$ for some constant c we find

$$p\left|\mathrm{tr}\left(L_z\sigma\right)\right| \leq \left|\mathrm{tr}\left(L_z\rho\right)\right|$$

Note that, here the direction z is chosen arbitrarily and so for any direction $\hat{n}$ it holds that

$$p\left|\mathrm{tr}\left(L_{\hat{n}}\sigma\right)\right| \leq \left|\mathrm{tr}\left(L_{\hat{n}}\rho\right)\right| \tag{5.37}$$

This results looks very intuitive. If a spin-j undergoes a deterministic or stochastic rotationally covariant dynamics the *absolute value* of the expectation value of angular momentum can not increase. Note that the sign of this expectation value can change, i.e. a state whose angular momentum is negative in the $\hat{z}$ direction can evolve to a state whose angular momentum is positive in this direction.

Recall that previously we have seen that in a rotationally covariant open dynamics, the absolute value of angular momentum can increase. This may look in contradiction with the above result. Nevertheless there is no contradiction because in the above problem we have

assumed that the initial and final spaces are both spin-j systems. One can easily show that the absolute value of angular momentum can increase if the final space is allowed to have a higher spin. In the following we will find a bound which applies to these cases where the initial and final spaces have different spins. Before this we present another consequence of Eq.(5.36) for the case where both input and output spaces have the same spin-j.

Although in a rotationally-covariant dynamics of a spin-j system the absolute value of angular momentum cannot increase, nevertheless the expectation value of higher orders of angular momentum can increase. However, using Eq.(5.36) we can find non-increasing functions which involve the expectation value of higher orders of angular momentum. For instance, consider the case of $(\mu = 2, m = 0)$. Then, as we have seen in section 4.1.1, in the case of spin-j representation of SO(3)

$$T^{(\mu=2,m=0)} = c(3L_z^2 - L^2)$$

where c is a normalization factor. Then Eq.(5.36) implies that

$$p\left|\mathrm{tr}(\sigma L_z^2) - \frac{j(j+1)}{3}\right| \leq \left|\mathrm{tr}(\rho L_z^2) - \frac{j(j+1)}{3}\right| \tag{5.38}$$

where we have used the fact that for all spin-j systems the expectation value of L^2 is $j(j+1)$. Note that the $\hat{z}$ direction is chosen arbitrarily. So, for arbitrary direction $\hat{n}$, $|\mathrm{tr}(\rho L_z^2) - j(j+1)/3|$ is non-increasing under rotationally covariant dynamics, though $\mathrm{tr}(\rho L_{\hat{n}}^2)$ can increase under this type of dynamics.

Now we find a bound on the change of absolute value of the expectation value of angular momentum when the input and output spaces have different spins.

To achieve this goal we calculate $\|\rho^{(\mu,m)}\|$ for the mode $(\mu = 1, m = 0)$ in the case of arbitrary spin-j system. Using the fact that $T^{(\mu=1,m=0)} = cL_z$ for some constant c we find

$$F_{\mu=1,m=0} \equiv \|\rho^{(1,0)}\| = \frac{\mathrm{tr}\left(\sqrt{L_z^2}\right)}{\mathrm{tr}\left(L_z^2\right)}\left|\mathrm{tr}\left(L_z\rho\right)\right| = \frac{3\mathrm{tr}\left(\sqrt{L_z^2}\right)}{\mathrm{tr}\left(L^2\right)}\left|\mathrm{tr}\left(L_z\rho\right)\right| \tag{5.39}$$

where we have used the normalization condition, i.e. $|c|^2\mathrm{tr}\left(L_z^2\right) = 1$. One can easily see that $\mathrm{tr}\left(L^2\right) = j(j+1)(2j+1)$ and

$$\begin{aligned} \mathrm{tr}\left(\sqrt{L_z^2}\right) &= j(j+1) && \text{integer } j \\ &= (j+1/2)^2 && \text{half integer } j \end{aligned}$$

So

$$\begin{aligned} \|\rho^{(1,0)}\| &= 3/2\frac{|\mathrm{tr}\,(L_z\rho)|}{j+1/2} && \text{integer } j \\ &= 3/2\frac{|\mathrm{tr}\,(L_z\rho)|\,(j+1/2)}{j(j+1)} && \text{half integer } j \end{aligned}$$

So $\|\rho^{(1,0)}\|$ is less than or equal $3/2$ and at the limit of j going to infinity it tends to $3/2$.

Now we can find an analogue of the bound of eq. (5.37) for the case where the input and output systems have spins j and j' respectively. If, for example, both j and j' are integer then

$$p\frac{|\mathrm{tr}\,(L_{\hat{n}}\sigma)|}{j'+1/2} \leq \frac{|\mathrm{tr}\,(L_{\hat{n}}\rho)|}{j+1/2} \tag{5.40}$$

In proposition 41 we provide an operational interpretation of the quantity $\frac{|\mathrm{tr}(L_z\rho)|}{j+1/2}$ in terms of the ability of the state ρ to act as a quantum reference frame to distinguish two orthogonal states of a spin-half system $|j=1/2, m=\pm 1/2\rangle$.

5.4 Applications in estimation theory

In this section we show that the mode decomposition of a state can provide us with a new insight into covariant quantum estimation problems. A large family of interesting state estimation problems can be understood as estimating an unknown element g of a group G, where g is chosen according to some prior $p(g)$, and where we are given a copy of the state $U(g)\rho U^\dagger(g)$ for some known state ρ and some known representation of G, $g \to U(g)$.

Any given strategy for estimating the unknown parameter can be described by a POVM $\{M_{g'} : g' \in G\}$. Born's rule implies that the probability of obtaining the outcome g' given that the real value of parameter is g is

$$p\,(g'|g) = \mathrm{tr}\left(M_{g'}U(g)\rho U^\dagger(g)\right) \tag{5.41}$$

There are different choices of figure of merit for a particular strategy. A popular family of figures of merits can be described in terms of the average of *cost functions*. Let $c : G\times G \to \mathbb{R}$ be a cost function for this estimation problem, i.e. it quantifies the cost of estimating the group element to be g' while the true group element is g. Then the average of the cost

function,

$$C(\rho, \{M_{g'}\}) \equiv \int dg\ p(g) \int dg' p\,(g'|g)\, c(g, g')$$
$$= \int dg\ p(g) \int dg'\ \mathrm{tr}\left(M_{g'} U(g) \rho U^\dagger(g)\right) c(g, g'), \tag{5.42}$$

quantifies the performance of the particular strategy $\{M_{g'}\}$ (see e.g. [21]).

For any state ρ the relevant property of the state which determines this average cost is uniquely determined by the operator

$$\int dg\ p(g) c(g, g')\ U(g) \rho U^\dagger(g)$$

This suggests that the mode decomposition of state ρ can be useful to get some insight about the relevant properties of the state which determines the average cost $C(\rho, \{M_{g'}\})$. To see this point, we consider the Fourier transform of the function $p(g)c(g, g')$: Assume g' is a fixed parameter. Then expand the function $p(g)c(g, g')$ as

$$p(g)c(g, g') = \sum_{\mu,m,m'} f_{\mu,m,m'}(g') u^{(\mu)}_{m'm}(g) \tag{5.43}$$

where $u^{(\mu)}_{m'm}(g)$ are the matrix elements of the (non-projective) unitary irreps of G. Then, using the fact that

$$d_\mu \int\ dg\ u^{(\mu)}_{m'm}(g) U(g) \rho U^\dagger(g) = \sum_\alpha T^{(\mu,\alpha)\dagger}_{m'} \mathrm{tr}\left(T^{(\mu,\alpha)}_m \rho^{(\mu,m)}\right)$$

it is straightforward to show that

$$\int dg\ p(g) c(g, g')\ U(g) \rho U^\dagger(g)$$

is uniquely determined by the components of ρ in those modes (μ, m) for which $f_{\mu,m,m'}(g')$ is nonzero for some g'. In other words, if for two states ρ and σ it holds that $\rho^{(\mu,m)} = \sigma^{(\mu,m)}$ for all modes (μ, m) for which $\exists g' \in G, \exists m' :\ f_{\mu,m,m'}(g') \neq 0$ then for any strategy $\{M_{g'}\}$, $C(\rho, \{M_{g'}\}) = C(\sigma, \{M_{g'}\})$. In words, this means that the performance of a given state ρ is only specified by its components in those modes (μ, m) for which $f_{\mu,m,m'}(g')$ is nonzero for some m' and g'.

5.4.1 Example: Average fidelity of estimation of a random direction

Suppose Alice has randomly chosen a direction in space and wants to send it to Bob using a quantum system. Assume Bob has no prior knowledge about this chosen direction. Suppose Alice and Bob are trying to maximize the average fidelity $\hat{n} \cdot \hat{n}'$ between the direction Alice has sent $\hat{n}$ and the direction Bob has estimated $\hat{n}'$.

This estimation problem can be phrased in the above framework in terms of estimating an element of SO(3) where the probability distribution over SO(3) is uniform (See [21] for more discussion on this problem). Let $\hat{z}$ be the direction which Alice has chosen when she sends state ρ to Bob. In this case, $\Omega\hat{z}$ is the direction Alice has chosen when she sends $U(\Omega)\rho U^\dagger(\Omega)$. Then, it is natural to assume that ρ is invariant under rotations around z. Then, the cost function corresponding to the fidelity can be chosen to be

$$c(\Omega, \Omega') \equiv -\langle \Omega'\hat{z}|\Omega\hat{z}\rangle$$

where Ω is the rotation chosen by Alice, Ω' is Bob's estimation (see [21]). Now we use the fact that the defining representation of SO(3) corresponds to its unitary irrep with angular momentum $j = 1$. In particular, if $\hat{r}' = \Omega\hat{r}$ for some $\Omega \in \mathrm{SO}(3)$ then

$$\begin{pmatrix} (r'_x + ir'_y)/\sqrt{2} \\ r'_z \\ (r'_x - ir'_y)/\sqrt{2} \end{pmatrix} = U^{(j=1)}(\Omega) \begin{pmatrix} (r_x + ir_y)/\sqrt{2} \\ r_z \\ (r_x - ir_y)/\sqrt{2} \end{pmatrix} \tag{5.44}$$

where $U^{(j=1)}(\Omega)$ is the irrep of SO(3) with angular momentum $j = 1$ in the basis in which L_z is diagonal and all the matrix elements of L_x are real. So, the Fourier transform of the fidelity function has the form

$$\langle \Omega'\hat{z}|\Omega\hat{z}\rangle = \sum_{m'} r_{m'}(\Omega') u^{(\mu=1)}_{m',m=0}(\Omega).$$

for some functions $r_{m'}(\Omega')$ where $m' \in \{-1, 0, +1\}$. This together with the fact that $P(\Omega)$ is uniform implies that in the Fourier expansion of $p(\Omega)c(\Omega, \Omega')$,

$$p(\Omega)c(\Omega, \Omega') = \sum_{\mu,m,m'} f_{\mu,m,m'}(\Omega') u^{(\mu)}_{mm'}(\Omega),$$

the only nonzero components are $f_{\mu=1,m=0,m'}$ for $m' \in \{-1, 0, +1\}$. This implies that the integral

$$\int d\Omega \; p(\Omega)c(\Omega, \Omega') \; U(\Omega)\rho U^\dagger(\Omega)$$

is uniquely specified by, $\rho^{(\mu=1,m=0)}$, i.e. mode $(\mu = 1, m = 0)$ of state ρ.

If, for instance, the system under consideration is a spin-j system, then the $(\mu = 1, m = 0)$ mode component of state ρ is uniquely specified by the angular momentum of ρ in the $\hat{z}$ direction. Therefore, the average cost $C(\rho, \{M_{\Omega'}\})$ only depends on the choice of measurement $\{M_{\Omega'} : \Omega' \in SO(3)\}$ and the angular momentum of state in the $\hat{z}$ direction. (Recall that the direction $\hat{z}$ is defined to be the direction which Alice has chosen to send to Bob when she sends him the state ρ).

In other words, if Bob does not have any prior information about the direction, then relative to the average fidelity measure any two states of a spin-j system which have the same angular momentum in the $\hat{z}$ direction yield the same performance for any measurement $\{M_{\Omega'} : \Omega' \in SO(3)\}$. This observation is consistent with the result of Holevo in [21] which, using different argument, shows that if the state ρ is invariant under rotations around $\hat{z}$ then the average fidelity for the *optimal* measurement is $\mathrm{tr}(\rho L_z)/(j+1)$.

Note that there are many states of a spin-j system which break rotational symmetry and so can transfer information about direction, but nevertheless have expectation of angular momentum L_z equal to zero. For example, in the case of integer j consider the state

$$\frac{1}{3}|j, 2k\rangle\langle j, 2k| + \frac{2}{3}|j, -k\rangle\langle j, -k|$$

for an integer $k \leq j/2$. The above result implies that with respect to the figure of merit defined by the average fidelity such states are indistinguishable from a totally symmetric state which does not transfer any information about direction.

5.5 Simulating quantum operations by quantum reference frames

Consider the situation where we are restricted to those Hamiltonians which all have a particular symmetry. Then it is still possible to *simulate* a dynamics which breaks this symmetry if we have access to a state which breaks the symmetry, i.e. a source of asymmetry. As we have defined before, this symmetry breaking state is called a quantum reference frame. Now by coupling this quantum reference frame to a system via a symmetric dynamics, we can effectively generate a non-symmetric dynamics or measurement on this system. In this section we are interested to find the set of non-symmetric dynamics and measurements which can be simulated using a given a quantum reference frame.

As a simple example, consider the case where we are restricted to the rotationally-invariant Hamiltonians. Then by coupling a quantum system to a large magnet with magnetic field in the $\hat{z}$ direction via a rotationally invariant Hamiltonian, we can effectively simulate a rotation around the $\hat{z}$ axis on that quantum system (Note that a rotation is not rotationally invariant and so cannot be performed without having access to a system which breaks the rotational symmetry). In this case, we can model the magnet by a large coherent spin-j in $\hat{z}$ direction, i.e. a spin-j system in the state $|j, m = j\rangle$. Then, by coupling the quantum system to this quantum reference frame one can realize a quantum channel on the system such that this channel at the limit where j goes to infinity approaches a perfect (unitary) rotation. In fact, one can show that using a spin-j in the coherent state in $\hat{z}$ direction, at the limit of large j any arbitrary dynamics which is invariant under rotation around $\hat{z}$ can be simulated on the system ([5]).[3]

Note that having access to this quantum reference frame we still cannot simulate a rotation around $\hat{x}$ or any other dynamics which is not invariant under rotation around $\hat{z}$. More generally, using a quantum reference frame only those time evolutions and measurements can be simulated which have all the symmetries of the quantum reference frame. In this section we generalize this simple observation by finding a relation between the modes of asymmetry of the quantum reference frame and the modes of asymmetry of a time evolution or measurement that can be simulated using this quantum reference frame.

5.5.1 Modes of asymmetry of quantum operations

The notion of modes of asymmetry naturally extends to the super-operators. Let $g \to U(g)$ be the projective unitary representation of G on the Hilbert space $\mathcal{H}$. Also, let $\mathcal{U}_g(\cdot) \equiv U(g)(\cdot)U^\dagger(g)$. Then $g \to \mathcal{U}_g$ is a (non-projective) unitary representation of G on $\mathcal{B}(\mathcal{H})$. Similarly, we can define a representation of G on the space of all linear super-operators: Consider the linear space of all super-operators from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$. Then a natural representation of G on this space is given by the following map

$$\forall g \in G: \qquad \mathfrak{U}_g[\mathcal{E}] \equiv \mathcal{U}_g^{\text{out}} \circ \mathcal{E} \circ \mathcal{U}_{g^{-1}}^{\text{in}} \tag{5.45}$$

for arbitrary $\mathcal{E} : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$, where $g \to \mathcal{U}_g^{\text{in}}$ and $g \to \mathcal{U}_g^{\text{out}}$ are the representations of the symmetry on $\mathcal{B}(\mathcal{H}_{\text{in}})$ and $\mathcal{B}(\mathcal{H}_{\text{out}})$ respectively. This representation has a natural physical interpretation: Suppose the representation $g \to U(g)$ describes a change of reference

[3] Furthermore, it is shown in this paper that if in addition to this quantum reference frame we have also access to a similar quantum reference frame in a coherent state in $\hat{x}$ direction then we can simulate any arbitrary dynamics on the system.

frame, such that a state which is described by $|\psi\rangle$ in the old reference frame is described by $U(g)|\psi\rangle$ in the new reference frame. Then, an observable or a density operator which is described by an operator A relative to the old reference frame will be described by $\mathcal{U}_g[A]$ relative to the new reference frame. Similarly, a super-operator which is described by $\mathcal{E}$ relative to the old reference frame will be described by $\mathfrak{U}_g[\mathcal{E}]$ relative to the new reference frame.

Now, following the same logic we used to define modes of asymmetry of operators based on the representation $g \to \mathcal{U}_g$ of group G on the space of operators, we can define the notion of modes of asymmetry of super-operators based on the representation $g \to \mathfrak{U}_g$ of group G on the space of super-operators. One way to do this is by defining the analogues of the irreducible tensor operators for super-operators. But, we can also define modes of asymmetry for super-operators using the analogue of lemma 31:

Definition 33 *The mode (μ, m) of the super-operator $\mathcal{E}$, denoted by $\mathcal{E}^{(\mu,m)}$ is defined by*

$$\mathcal{E}^{(\mu,m)} = d_\mu \int dg\ \bar{u}^{(\mu)}_{mm}(g)\ \mathfrak{U}_g\left[\mathcal{E}\right] \tag{5.46}$$

where d_μ is the dimension of the irrep μ. We call the decomposition $\mathcal{E} = \sum_{\mu,m} \mathcal{E}^{(\mu,m)}$ the mode decomposition *of the super-operator $\mathcal{E}$ and $\mathcal{E}^{(\mu,m)}$ the (μ, m) modal component of $\mathcal{E}$.*

Note that this definition implies that a *G-covariant* super-operator only has nonzero component in the mode which correspond to the trivial representation of the group, denoted by $\mu = 0$.

Let $g \to U(g)$ be the representation of symmetry on the Hilbert space $\mathcal{H}$. As we have seen before, we can find the set of all modes of asymmetry that an operator $X \in \mathcal{B}(\mathcal{H})$ can possibly have, by decomposing the representation $g \to U(g) \otimes \bar{U}(g)$. Similarly, we can find all modes of asymmetry that a super-operator $\mathcal{E} : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$ can possibly have, by decomposing the representation

$$g \to U_{\text{out}}(g) \otimes \bar{U}_{\text{out}}(g) \otimes U_{\text{in}}(g) \otimes \bar{U}_{\text{in}}(g)$$

to irreps of G where $g \to U_{\text{in}}(g)$ and $g \to U_{\text{out}}(g)$ are the representations of symmetry on $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ respectively.

Example 34 *Consider the group of rotations in $\mathbb{R}^3$, i.e. G=SO(3), and assume the input Hilbert space carries a j_1 irrep and the output Hilbert space carries a j_2 irrep. Then any super-operator from $\mathcal{B}(\mathcal{H}_{in})$ to $\mathcal{B}(\mathcal{H}_{out})$ can have modes (μ, m) with $\mu \leq 2(j_1 + j_2)$. In*

particular, if the input and output spaces of a super-operator are both spin-half systems (i.e. $j_1 = j_2 = 1/2$), then the super-operator can only have modes $(\mu = 0), (\mu = 1, m = -1, 0, 1)$ and $(\mu = 2, m = -2, -1, 0, 1, 2)$. On the other hand, if the input space $\mathcal{H}_{in}$ is a spin-half irrep of SO(3) and the output space is invariant under rotation (i.e. $j_1 = 1/2$ and $j_2 = 0$) then the super-operator can only have modes $(\mu = 0), (\mu = 1, m = -1, 0, 1)$. These kinds of super-operators can describe, for example, measurements on a spin-half system where the post-measurement state is always rotationally invariant.

In this example, we found all modes of asymmetry that a measurement performed on a spin-half system can possibly have. In the following we study the notion of modes of asymmetry of measurements more closely.

Modes of asymmetry of measurements

In the study of the modes of asymmetry of measurements we focus on the aspect of a measurement that is relevant for making inferences about the input, that is, its informative aspect, and neglect the aspect that is relevant for making predictions about future measurements on the system, that is, its state-updating aspect.

Let $\{M_\lambda\}$ be the POVM describing an arbitrary measurement. Define the channel

$$\mathcal{M}(X) \equiv \sum_\lambda \mathrm{tr}(XM_\lambda)|\lambda\rangle\langle\lambda| \tag{5.47}$$

where $\{|\lambda\rangle\}$'s are all orthogonal and G-invariant states. Then, any measurement whose statistics is described by the POVM $\{M_\lambda\}$ can be realized by first applying the channel $\mathcal{M}(\cdot)$ to the state and then measuring the output system in $\{|\lambda\rangle\}$ basis. But, this latter measurement is G-covariant and so one does not need a quantum reference frame to realize it. So to study the informative aspect of a measurement with POVM $\{M_\lambda\}$ from the point of view asymmetry and find the asymmetry resources required to implement this measurement, we can equivalently study the corresponding channel $\mathcal{M}$ and find the asymmetry resources required to implement $\mathcal{M}$.

Then, one can easily show that

Lemma 35 *$\mathcal{M}^{(\mu,m)}$, the (μ, m) modal component of $\mathcal{M}$, is equal to*

$$\mathcal{M}^{(\mu,m)}(X) = \sum_\lambda tr(XM_\lambda^{(\mu,m)})|\lambda\rangle\langle\lambda| \tag{5.48}$$

where $M_\lambda^{(\mu,m)}$ is the (μ, m) modal component of the operator M_λ.

Proof. First note that by definition 33

$$\mathcal{M}^{(\mu,m)}(X) \equiv d_\mu \int dg\ \bar{u}^{(\mu)}_{mm}(g)\ \mathcal{U}^{\text{out}}_g \circ \mathcal{M} \circ \mathcal{U}^{\text{in}}_{g^{-1}}(X) \tag{5.49}$$

Here, the representation of symmetry on the output system is trivial and so

$$\begin{aligned}
\mathcal{M}^{(\mu,m)}(X) &= d_\mu \int dg\ \bar{u}^{(\mu)}_{mm}(g)\ \mathcal{U}^{\text{out}}_g \circ \mathcal{M} \circ \mathcal{U}^{\text{in}}_{g^{-1}}(X) \\
&= d_\mu \sum_\lambda |\lambda\rangle\langle\lambda| \int dg\ \bar{u}^{(\mu)}_{mm}(g) \text{tr}(\mathcal{U}^{\text{in}}_{g^{-1}}(X) M_\lambda) \\
&= d_\mu \sum_\lambda |\lambda\rangle\langle\lambda| \int dg\ \bar{u}^{(\mu)}_{mm}(g) \text{tr}\left(X \mathcal{U}^{\text{in}}_g(M_\lambda)\right) \\
&= \sum_\lambda \text{tr}(X M^{(\mu,m)}_\lambda) |\lambda\rangle\langle\lambda|
\end{aligned}$$

■

Later, in this chapter we use this observation to infer the asymmetry resources which are required to implement a given measurement.

5.5.2 From modes of quantum reference frames to modes of quantum operations

As described above, under the assumption that all symmetric dynamics are free we can use a quantum quantum reference frame, which breaks the symmetry, as a *resource* of asymmetry which enables us to *simulate* dynamics which break the symmetry.

Definition 36 *Let $\mathcal{H}_{sys}$ and $\mathcal{H}_{RF}$ be Hilbert spaces with projective unitary representations $g \to U_{sys}(g)$ and $g \to U_{RF}(g)$ of group G. We say that a channel $\mathcal{E} : \mathcal{B}(\mathcal{H}_{sys}) \to \mathcal{B}(\mathcal{H}_{sys})$ can be simulated using the resource state ρ_{RF} if there exists a channel $\tilde{\mathcal{E}} : \mathcal{B}(\mathcal{H}_{sys} \otimes \mathcal{H}_{RF}) \to \mathcal{B}(\mathcal{H}_{sys} \otimes \mathcal{H}_{RF})$ which is G-covariant, i.e.*

$$\forall g \in G : \quad \tilde{\mathcal{E}} \circ (\mathcal{U}^{sys}_g \otimes \mathcal{U}^{RF}_g) = (\mathcal{U}^{sys}_g \otimes \mathcal{U}^{RF}_g) \circ \tilde{\mathcal{E}}$$

such that

$$\mathcal{E}(X) = tr_{RF}\left(\tilde{\mathcal{E}}(X \otimes \rho_{RF})\right). \tag{5.50}$$

Now one can easily prove the following result.

Lemma 37 *Suppose the channel $\mathcal{E}$ can be simulated using a quantum reference frame in the state ρ and a G-covariant channel $\tilde{\mathcal{E}}$ such that $\mathcal{E}(X) = tr_{RF}\left(\tilde{\mathcal{E}}(X \otimes \rho)\right)$. Then*

$$\mathcal{E}^{(\mu,m)}(X) = tr_{RF}\left(\tilde{\mathcal{E}}(X \otimes \rho^{(\mu,m)})\right) \tag{5.51}$$

Proof. First, note that

$$\begin{aligned}\mathfrak{U}_g[\mathcal{E}](X) &= \mathcal{U}_g \circ \mathcal{E} \circ \mathcal{U}_{g^{-1}}(X) \\ &= \mathcal{U}_g \circ \mathrm{tr}_{RF}\left(\tilde{\mathcal{E}}(\mathcal{U}_{g^{-1}}(X) \otimes \rho)\right)\end{aligned}$$

But because $\tilde{\mathcal{E}}$ is G-covariant, we have

$$\mathfrak{U}_g[\mathcal{E}](X) = \mathrm{tr}_{RF}\left(\tilde{\mathcal{E}}(X \otimes \mathcal{U}_g(\rho))\right)$$

By multiplying both sides by $\bar{u}^{(\mu)}_{mm}(g)$ and taking the integral over G, we can prove the lemma. ■

In the previous section, we defined Modes(ρ) to be the set of all modes in which state ρ has nonzero components. Similarly, we define Modes($\mathcal{E}$) to be the set of all modes in which a channel $\mathcal{E}$ has nonzero components. Then the above lemma implies that

Proposition 38 *If a quantum reference frame ρ can simulate a quantum channel $\mathcal{E}$ then*

$$\textit{Modes}(\mathcal{E}) \subseteq \textit{Modes}(\rho) \tag{5.52}$$

So if a quantum reference frame does not have a particular mode of asymmetry, it cannot simulate a time evolution or measurement which has that mode of asymmetry. Also, the lemma implies that to specify whether a given quantum reference frame ρ can simulate a quantum channel $\mathcal{E}$ or not we only need to know the components of ρ in modes contained in Modes($\mathcal{E}$). So, as we will see in an example, although the Hilbert space of the quantum reference frame might be arbitrary large, the number of parameters required to specify its performance for some specific simulation can be very small.

Furthermore, for any given finite dimensional Hilbert space $\mathcal{H}_{\mathrm{sys}}$, there are a finite set of modes in which a channel acting on $\mathcal{B}(\mathcal{H}_{\mathrm{sys}})$ can have nonzero components. So for a given quantum reference frame ρ_{RF} on an arbitrarily large Hilbert space and having amplitude over arbitrarily many representations of the group, the properties of the quantum reference frame which are relevant for simulating arbitrary channels acting on $\mathcal{B}(\mathcal{H}_{\mathrm{sys}})$ can be specified merely by specifying the components of ρ_{RF} in that finite set of modes.

Example: Reference frames of unbounded size may still lack modes

In the case of G=SO(3), consider the family of quantum reference frames defined by

$$|\psi_N\rangle \equiv \frac{1}{\sqrt{N}} \sum_{k=1}^{N} |j = N^2 + 2k, m = N^2 + k\rangle$$

One can easily show that, at the limit of large N these states are very sensitive to rotations around $\hat{z}$ and also rotations around any axis in the $x-y$ plane. In other words, for any small such rotation, $|\psi_N\rangle$ is almost orthogonal to the rotated version of $|\psi_N\rangle$. So, one may think that at the limit of large N this quantum reference frame completely breaks the symmetry and so it can be used to simulate any arbitrary measurement on a spin-half system. But, this is not the case. Indeed, it turns out that though at the limit of large N these states are very sensitive to rotations around $\hat{z}$ and so breaks this symmetry, yet they cannot simulate any measurement on a spin-half system which is not invariant under rotations around $\hat{z}$. To see this first note that if the POVM elements of a measurement on a spin-half system are not invariant under rotations around $\hat{z}$ then they have nonzero components in the modes $(\mu = 1, m = \pm 1)$. Then, lemma 35 implies that the channel describing that measurement will have modes $(\mu = 1, m = \pm 1)$. Now proposition 38 implies that to be able to simulate any such measurement a quantum reference frame needs to have a non-zero component in the modes $(\mu = 1, m = \pm 1)$. So, to summarize to be able to simulate a measurement on a spin-half system whose POVM elements are not invariant under rotations around $\hat{z}$, a quantum reference frame needs to have nonzero components in modes $(\mu = 1, m = \pm 1)$. Now using the Wigner-Eckart theorem one can easily show that none of the states in the above family have a nonzero-component in the modes $(\mu = 1, m = \pm 1)$[4].

The conclusion is that there are measurements that break rotational symmetry that cannot be simulated by this family of quantum reference frames.

[4]Consider the terms in the decomposition

$$|\psi_N\rangle\langle\psi_N| = \frac{1}{N} \sum_{k,k'=1}^{N} \left|j = N^2 + 2k, m = N^2 + k\right\rangle\left\langle j' = N^2 + 2k', m' = N^2 + k'\right|$$

Any term in this decomposition with $k = k'$ is invariant under rotations around $\hat{z}$ and so it only has components in modes $(\mu, m = 0)$. On the other hand, terms with $k \neq k'$ has no componenets in the neither of the modes $(\mu = 1, m = -1, 0, +1)$. This can be seen, for instance, using the Wigner-Eckart theorem

5.6 Example: Spin-j systems as a quantum reference frame

The problem of using a spin-j system as a quantum reference frame to simulate dynamics or measurements which are not invariant under rotations has been studied in several papers (See e.g. [49, 50, 51, 52, 53, 5]). In this section we focus on this problem and show that the mode decomposition of states provide an extremely powerful insight into this problem. In particular, we show that using this approach some of the previously known results which have been achieved in an ad hoc manner can be reproduced and generalized in a systematic way.

5.6.1 Simulating measurements and channels on a spin-half system

We start by the problem of simulating measurements on a spin-half system. Here, the assumption is that we are restricted to use rotationally invariant unitaries, ancillary systems in rotationally invariant states and measurements whose POVM elements are all rotationally invariant. Under this restriction, we are given a spin-j system in an arbitrary state ρ as a quantum reference frame and our goal is to simulate a non-invariant measurement on a spin-half system. Here, we focus on the informative aspect of the measurement, i.e. we do not care how the state of system is updated after the simulated measurement.

For an arbitrary measurement on a spin-half system consider the channel which describes the informative aspects of this measurement, as defined in Eq. (5.47). Then, consider the set of all modes $\{(\mu, m)\}$ in which these channels can have nonzero components. We can conclude from lemma 35 that this set is equal to $\{(\mu = 0), (\mu = 1, m = -1, 0, +1)\}$ (This is also shown in example 34.).

Then, it follows from proposition 37 that the only relevant properties of ρ the state of the quantum reference frame which determine its performance for simulating a measurement on a spin-half system are uniquely specified by the components of state ρ in the modes $\{(\mu = 0), (\mu = 1, m = -1, 0, +1)\}$, i.e. $\rho^{(\mu=0)}, \rho^{(\mu=1,m=-1,0,1)}$. Furthermore, since the irreducible tensor operator basis on a spin-j system are multiplicity-free then each of the components $\rho^{(\mu=0)}, \rho^{(\mu=1,m=-1,0,1)}$ is determined with only one parameter, namely, the Hilbert Schmidt inner product of state ρ in the corresponding component of the irreducible tensor operator basis, i.e.

$$T^{(\mu=0)} = c_0 \mathbb{I}, \quad T^{(\mu=1)}_{m=0} = c_1 L_z, \quad \text{and} \quad T^{(\mu=1)}_{m=\pm 1} = \pm \frac{c_1}{\sqrt{2}} L_{\pm}$$

where c_0 and c_1 are normalization factors. It follows that the components of state ρ in the modes $\{(\mu = 0), (\mu = 1, m = -1, 0, +1)\}$, is uniquely specified by the vector of expectation value of angular momentum for state ρ, i.e. $(\langle L_x \rangle, \langle L_y \rangle, \langle L_z \rangle)$.

So we conclude that

Proposition 39 *The performance of a spin-j system as a quantum reference frame for simulating (informative aspects of) measurements on a spin-half system is uniquely specified by three real parameters, i.e. the vector of expectation values of angular momentum for the state of quantum reference frame.*

This result has been previously obtained in [50] using a totally different and rather ad hoc argument. But, using our approach we can easily generalize it to the case of measurements on the systems which have arbitrary representation of SO(3) (as opposed to the spin-half representation). Before presenting this generalization we investigate some implications of proposition 39.

An interesting consequence of proposition 39 is the following: Suppose the vector of expectation values of angular momentum of state ρ of the spin-j system is in the $\hat{n}$ direction. Clearly, in general the state ρ is not invariant under rotations around $\hat{n}$. Now consider the symmetrized version of state ρ, i.e. the state

$$\rho_{\text{sym}} \equiv \frac{1}{2\pi} \int d\theta \; e^{-i\theta \vec{L}.\hat{n}} \rho \; e^{i\theta \vec{L}.\hat{n}}$$

which is invariant under rotation around $\hat{n}$. One can easily see that this state has the same vector of expectation values of angular momentum as the original state ρ. Therefore, any measurement on the spin-half system which can be simulated using ρ can also be simulated using ρ_{sym} and vice versa. But, since ρ_{sym} is invariant under rotations around $\hat{n}$, it can only simulate those measurements whose POVM elements are invariant under rotations around $\hat{n}$. This argument implies that

Corollary 40 *Using a spin-j system as a quantum reference frame for direction, one can only simulate those measurements on a spin-half system whose POVM elements are invariant under rotations around the direction of the vector of the expectation values of angular momentums of the state of quantum reference frame.*

So, even at the limit of large j, a single spin-j system cannot act as a perfect reference frame for direction. For example, in general the state $|\psi\rangle = |j, j\rangle_{\hat{n}} + |j, j\rangle_{\hat{n}'}$ has no symmetries,

but the POVM effects that it can simulate are necessarily invariant under rotations about $\langle\psi|\vec{L}|\psi\rangle$.

As an example of simulating measurements on a spin-half system consider the following problem: Suppose one uses a spin-j system in the state ρ as a quantum reference frame to measure the angular momentum of a spin-half system in the $\hat{z}$ direction or equivalently to measure the observable σ_z. But it can be shown that this measurement cannot be simulated perfectly with a quantum reference frame with bounded size. Now the question is using the spin-j system in the state ρ as a quantum reference frame, how well one can simulate this measurement. In other words, what is the highest precision obtainable using this quantum reference frame to simulate a σ_z measurement? We evaluate the precision of the realized measurement using the following figure of merit: The highest probability of successfully distinguishing an unknown eigenstate of σ_z when we are given each of the two eigenstates with equal probability.

Then in the appendix A.2 we prove the following

Proposition 41 *Suppose we are restricted to the rotationally invariant measurements but we have access to the state ρ of a spin-j system as a quantum reference frame. Then the maximum probability of successfully distinguishing the two eigenstates of σ_z for a spin-half system, that is, $|j = 1/2, m = 1/2\rangle$ and $|j = 1/2, m = -1/2\rangle$, when one of these is chosen uniformly at random is given by*

$$p_{succ}(\rho) = \frac{1}{2}\left[1 + \frac{|tr(\rho L_z)|}{j + 1/2}\right] \tag{5.53}$$

So, as we expected from proposition 39, this probability only depends on the expectation value of the vector of angular momentum. Note that, as one may expect intuitively, at the limit where j goes to infinity the coherent state $|j, j\rangle$ can be used as a quantum reference frame to simulate the measurement of σ_z perfectly.

Finally, it is worth mentioning that if the Hilbert space of the quantum reference frame under consideration carries different irreps of SO(3) or if it has more than one copy of an irrep then the vector of angular momentum of the reference frame state alone is not sufficient to specify the measurements it can simulate on a spin-half system. For example, suppose the quantum reference frame is formed from a spin-j system and a qubit whose states are invariant under rotation. This means that the total Hilbert space of the quantum reference frame has two copies of irrep j of SO(3). Suppose the quantum reference frame is in the state

$$\frac{1}{\sqrt{2}}\left(|j, m = j, \lambda = 1\rangle + |j, m = -j, \lambda = 2\rangle\right)$$

where λ labels different orthogonal states of the qubit. Then, one can easily show that at the limit of large j this reference frame can simulate any arbitrary measurement which is invariant under rotation around $\hat{z}$. But, the expectation value of angular momentum for this state is zero in all directions. So, for a general representation of SO(3) these expectation values cannot characterize the ability of state for simulating measurements on a spin-half system.

Proposition 39 can be easily generalized to the problem of simulating arbitrary dynamics on a spin-half system.[5]

Recall from example 34 that the modes of asymmetry of any channel acting on a spin-half system is in the set $\{(\mu = 0), (\mu = 1, m = -1, 0, 1), (\mu = 2, m = -2, -1, 0, 1, 2)\}$. So, proposition 37 implies that to specify the ability of a particular state ρ of the spin-j system for simulating an arbitrary dynamics on a spin-half system we merely need to specify these modes of asymmetry of ρ. Again from the result of section 4.1.1 we can see that the component of arbitrary state ρ in these modes is uniquely specified by the following eight real parameters

$$\begin{aligned} &\mu = 1 \text{ modes}: \ \langle L_x \rangle, \langle L_y \rangle, \langle L_z \rangle \\ &\mu = 2 \text{ modes}: \ \langle L_x^2 \rangle, \langle L_y^2 \rangle, \ \langle L_x L_y + L_y L_x \rangle, \ \langle L_x L_z + L_z L_x \rangle, \ \ \langle L_y L_z + L_z L_y \rangle \end{aligned} \tag{5.54}$$

So to summarize we have shown that

Proposition 42 *The performance of a spin-j system in state ρ as a quantum reference frame for simulating channels on a spin-half system is uniquely specified by the eight real parameters given by Eq.(5.54).*

In the next section we present generalizations of propositions 39 and 42.

5.6.2 Generalization to arbitrary systems

Using the same technique we used to prove propositions 39 and 42 we can prove the following generalization

Theorem 43 *The performance of a given state of a spin-j system as a quantum reference frame for simulating an arbitrary measurement (or channel) on a given system with Hilbert*

[5] This also includes the problem of simulating measurements where the update rule of measurement should also be simulated as well as its informative aspect.

space $\mathcal{H}$ is uniquely specified by $(2l+1)^2-1$ (or $(4l+1)^2-1$ in the case of channels) real parameters of that state where l is the largest angular momentum which shows up in the decomposition of the Hilbert space $\mathcal{H}$ into irrep of SO(3). These parameters of the state of quantum reference frame corresponds to the expectation values of all the non-trivial irreducible tensor operators with rank less than or equal to $2l$ ($4l$ in the case of channels) for that state.

The proof is presented at the end of this section. Note that in general an arbitrary state ρ of spin-j system is specified by $(2j+1)^2-1$ real parameters. But the above result implies that the number of parameters of state of quantum reference frame which we need to consider to specify the performance of the quantum reference frame does not grow with the size of quantum reference frame.

An important special case is where the state ρ of quantum reference frame is invariant under rotations around some axis $\hat{n}$. This special case has been previousy considered for example in [53]. Then it follows from theorem 43 that

Corollary 44 *In theorem 43 if the state ρ of quantum reference frame is invariant under rotations around direction $\hat{n}$ then its performance to simulate a measurement can be uniquely specified by $2l$ (or $4l$ in the case of channels) real parameters corresponding to the moments $\{tr\left(\rho L_{\hat{n}}^k\right) : 1 \leq k \leq 2l\}$ (or $\{tr\left(\rho L_{\hat{n}}^k\right) : 1 \leq k \leq 4l\}$ in the case of channels) where $L_{\hat{n}}$ is the angular momentum operator in $\hat{n}$ direction.*

Note that to specify an arbitrary state ρ of spin-j system which is invariant under rotations around direction $\hat{n}$ one needs $2j$ real parameters. An instance of these parameters are $\{\mathrm{tr}\left(\rho L_{\hat{n}}^k\right) : 1 \leq k \leq 2j\}$. This particular characterization of states is used in [53] to specify how the quality of a quantum reference frame *degrades* after using it to simulate a channel or measurement.

In particular, they use this characterization to study the problem of simulating channels on a spin-half system and simulating measurements on a spin-one system. But from the result of corollary 43 we know that to specify the performance of the quantum reference frame in both of these cases we only need to specify two real parameters, i.e. $\mathrm{tr}\left(\rho L_{\hat{n}}\right)$ and $\mathrm{tr}\left(\rho L_{\hat{n}}^2\right)$. As we will see next, this can highly simplify the study of the problem of the *degradation* of quantum reference frames.

5.6.3 Degradation of quantum reference frames

Using a quantum reference frame to simulate a symmetry-breaking measurement or channel will inevitably *degrade* it. This *degradation* of quantum reference frames can be understood

as a manifestation of the fact that obtaining information about a quantum system will necessarily disturb it.

For example, in the case of rotational symmetry, consider a quantum reference frame which specifies an unknown direction in space. Now we can use this quantum reference frame to simulate a rotation around this unknown direction on an object system. But by comparing the initial and final state of the object system we can obtain some information about the unknown direction. So, using a quantum system as a quantum reference frame for simulating a rotation can be thought as performing a measurement on the quantum reference frame and since in this process, we in principle can obtain some information about the unknown direction specified by quantum reference frame, its state will necessarily be disturbed in this process.

Different aspects of the degradation of quantum reference frames have been studied in several papers (See e.g. [49, 50, 51, 52, 53, 54, 55] and the references in [1]). A central question studied in these papers is how after k times using a quantum reference frame for simulating a measurement or a channel the quality of this simulation drops as a function of k.

A natural assumption to study the degradation of quantum reference frames, which has been made for example in [51, 52, 53], is that the average of the state of the object system on which we simulate a measurement or a channel is symmetric. In other words, each time which we use the quantum reference frame to simulate an operation on the object system, the state of the object system is chosen randomly in a way that the average state does not break the symmetry. So, for example, in the case of rotational symmetry, which we study in this section, the average state of the object system should be rotationally invariant.

Then it follows that under this assumption the degradation of the quantum reference frame will be described by a rationally covariant channel. In other words, ρ_k the state of quantum reference frame after k times using it to simulate a fixed measurement or channel, will be

$$\rho_k = \mathcal{E}_{\mathrm{Deg}}(\rho_{k-1}) \tag{5.55}$$

where $\mathcal{E}_{\mathrm{Deg}}$ is a G-covariant channel. This implies that under this assumption about the distribution of the states of the object system, different modes of asymmetry of quantum reference frame degrade independently, i.e.

$$\forall(\mu, m): \quad \rho_k^{(\mu,m)} = \mathcal{E}_{\mathrm{Deg}}(\rho_{k-1}^{(\mu,m)}) \tag{5.56}$$

This simple observation can highly simplify the study of degradation of quantum reference frames.

Consider the case of spin-j quantum reference frames for direction. First, note that this observation together with theorem 43 implies that the quality of simulation of a channel or measurement on an object system after using the quantum reference frame for arbitrary number of times only depends on a fixed number of parameters of the initial state of the quantum reference frame and this number is independent of the size of quantum reference frame.

Furthermore, from example 21 we know that since the channel $\mathcal{E}$ which describes the degradation of quantum reference frame is rotationally covariant it holds that

$$\forall(\mu,m): \quad \rho_k^{(\mu,m)} = c^{(\mu)}\rho_{k-1}^{(\mu,m)} \tag{5.57}$$

where $\{c^{(\mu)}\}$ is a set of real coefficients which describe the channel $\mathcal{E}$ and $\forall\mu: \left|c^{(\mu)}\right| \leq 1$. But, since for spin-$j$ representation of SO(3) the irreducible tensor operator basis $\{T_m^{(\mu)}\}$ are multiplicity-free it holds that $\rho_k^{(\mu,m)} = \mathrm{tr}\left(\rho_k T_m^{(\mu)\dagger}\right) T_m^{(\mu)}$ and therefore

$$\forall(\mu,m): \quad \mathrm{tr}\left(\rho_k T_m^{(\mu)\dagger}\right) = c^{(\mu)}\mathrm{tr}\left(\rho_{k-1} T_m^{(\mu)\dagger}\right) \tag{5.58}$$

So if ρ and ρ_k are respectively the initial state of the quantum reference frame and its state after k times using the quantum reference frame to simulate a fixed quantum operation on the object system then it holds that

$$\forall(\mu,m): \quad \mathrm{tr}\left(\rho_k T_m^{(\mu)\dagger}\right) = \left(c^{(\mu)}\right)^k \mathrm{tr}\left(\rho T_m^{(\mu)\dagger}\right) \tag{5.59}$$

Since $|c^{(\mu)}| \leq 1$ we can conclude that the components of the state of quantum reference frame in different modes either remain constant or decay exponentially.

Example 45 *Here, we consider the scenarios studied in [53] where a spin-j system is used as a quantum reference frame to simulate channels on a spin-half system and measurements on a spin-one system. Furthermore, it is also assumed that the average of the state of the object system is rotationally invariant. This implies that the channel which describes the degradation of quantum reference frame is also rotationally covariant. It is also assumed in this paper that the state of quantum reference frame is initially invariant under rotation around an arbitrary direction which we denote it by $\hat{z}$. Note that since the degradation of quantum reference frame is described by a rotationally covariant channel, the state of quantum reference frame will remain invariant under rotations around $\hat{n}$.*

Now from theorem 43 and corollary 44 we know that the performance of the state ρ of this quantum reference frame for these simulations is uniquely specified by two real

parameters, i.e. the component of ρ in modes $(\mu = 1, m = 0)$ and $(\mu = 2, m = 0)$. But these are specified by

$$tr\left(\rho T_{m=0}^{(\mu=1)\dagger}\right) = A_1 tr\left(\rho L_{\hat{z}}\right) \quad and \quad tr\left(\rho T_{m=0}^{(\mu=2)\dagger}\right) = A_2 tr\left(\rho(3L_z^2 - L^2)\right)$$

where A_1 and A_2 are independent of state ρ. [6]. Note that since the state ρ by assumption is confined to the irrep j of SO(3), then $tr(\rho L^2) = j(j+1)$ and so

$$tr\left(\rho T_{m=0}^{(\mu=2)\dagger}\right) = A_2\left[3tr\left(\rho L_z^2\right) - j(j+1)\right]$$

In other words, the quality of simulation is uniquely specified by the expectation values of the first and the second moments of L_z for state ρ of quantum reference frame.

Now using Eq.(5.59) we can conclude that if the initial state of the quantum reference frame is ρ and if we have used the quantum reference frame k times then the quality of the $k+1$ simulation is uniquely specified by

$$tr(\rho_k L_z) = \left(c^{(1)}\right)^k tr\left(\rho L_z\right) \tag{5.60}$$

and

$$tr(\rho_k L_z^2) = \left[c^{(2)}\right]^k tr\left(\rho L_z^2\right) + \left[1 - \left(c^{(2)}\right)^k\right] \frac{j(j+1)}{3} \tag{5.61}$$

where $\{c^{(\mu)}\}$ is the set of coefficients which describe the degradation channel $\mathcal{E}$. So, in the example studied in [53] the only properties of the channel $\mathcal{E}$ which are relevant to specify the drop in the quality of simulation after using the quantum reference frame arbitrary number of times are specified merely by two real coefficients $c^{(1)}$ and $c^{(2)}$. Finally, note that since $|c^{(1)}| \leq 1$ then Eq.(5.60) implies that the absolute value of $tr(\rho_k L_z)$ is either constant or decay exponentially with k. Similarly, since $|c^{(2)}| \leq 1$ then Eq.(5.61) implies that $tr(\rho_k L_z^2)$ is either constant or exponentially saturates to $j(j+1)/3$, i.e. the expectation value of L_z^2 for the completely mixed state.

5.6.4 Proofs of Theorem 43 and corollary 44

Proof of Theorem 43

We start by the proof in the case of measurements. This proof follows exactly the same as the proof in the special case of spin-half systems. Suppose $\mathcal{H}$ is the Hilbert space of the

[6] $A_1^{-1} = \sqrt{\text{tr}(L_z^2)}$ and $A_2^{-1} = \sqrt{\text{tr}([3L_z^2 - L^2]^2)}$.

system on which we simulate the measurement. Then by assumption the largest irrep of SO(3) showing up in $\mathcal{H}$ is l. Let $g \to U(g)$ denote the projective representation of SO(3) on $\mathcal{H}$.

Then, as we have seen in section 4.1 the set of possible ranks of the irreducible tensor operators acting on $\mathcal{H}$ is the same as the set of all irreps of SO(3) which show up in the representation $g \to U(g) \otimes \bar{U}(g)$. But from section 4.1.1 we know that in the case of SO(3) this set is equal to the set of all irreps which show up in the representation $g \to U(g) \otimes U(g)$. Now since the maximum irrep in the representation $g \to U(g)$ is l then the maximum irrep in the representation $g \to U(g) \otimes U(g)$ is $2l$. Therefore, we conclude that the maximum rank of an irreducible tensor operator acting on $\mathcal{H}$ is $2l$.

Now from lemma 35 we know that the channel describing the informative aspect of an arbitrary measurement on this space has mode in the set $\{(\mu, m) : \ \mu \leq 2l\}$. This together with lemma 37 implies that to specify the performance of state ρ of quantum reference frame to simulate measurements on this system we only need to specify the components of ρ in all modes with $\mu \leq 2l$. But, since the irreducible tensor operators acting on the space of spin-j system have no multiplicity there is only

$$\sum_{k=0}^{2l} (2k+1) = (2l+1)^2$$

independent irreducible tensor operators with rank less than or equal to $2l$. Furthermore, the rank 0 tensor operator is proportional to the identity operator and so the component of ρ in this mode is fixed by the normalization. This implies that the performance of the quantum reference frame is determined by specifying at most $(2l+1)^2 - 1$ complex numbers corresponding to the expectation values of the density operator ρ for all non-trivial irreducible tensor operators with rank less than or equal to $2l$. Furthermore, in the case of SO(3), as we have seen in the discussion after Eq.(4.6), the Hermitian conjugate of a component of an irreducible tensor operator with rank μ is still in the subspace spanned by rank μ irreducible tensor operators. This implies that this subspace has a basis which is formed only from Hermitian operators. This together with the fact that the density operator ρ itself is a Hermitian operator imply that the components of ρ for modes with rank less than or equal $2l$ is uniquely specified by at most $(2l+1)^2 - 1$ *real* parameters. This completes the proof of theorem 43 in the case of measurements.

Proof in the case of channels follows in the same way. The only difference is that the set of all possible modes that a quantum channel acting on the system with Hilbert space $\mathcal{H}$ can have is determined by irreps which show up in the representation

$$g \to U(g) \otimes \bar{U}(g) \otimes U(g) \otimes \bar{U}(g)$$

of SO(3). Now, since the highest angular momentum which shows up in the representation $g \to U(g)$ is l, then the highest angular momentum which shows up in the above representation is $4l$. So an arbitrary channel acting on $\mathcal{H}$ can have mode in the set $\{(\mu, m) : \ \mu \leq 4l\}$. So, from lemma 37 to specify the performance of the quantum reference frame for simulating channels acting on this space we need to specify the components of ρ for all modes with rank less than or equal $4l$. The rest of argument follows exactly the same as the argument for the case of measurements.

Proof of corollary 44

We present the proof for the case of measurements. The proof for the case channels follows exactly in the same way.

From theorem 43 we know that to specify the performance of state ρ as a quantum reference frame we need to specify all components of ρ for all modes $\{(\mu, m) : 1 \leq \mu \leq 2l\}$.

Without loss of generality we assume state ρ is invariant under rotations around $\hat{z}$. Now for each mode $(\mu, m \neq 0)$, the corresponding component of the irreducible tensor operator basis, i.e. $T_m^{(\mu)}$ is not invariant under rotation around $\hat{z}$. Then, it follows that for all modes $(\mu, m \neq 0)$ the component of ρ in those modes are zero, i.e.

$$\forall (\mu, m \neq 0) : \ \rho^{(\mu,m)} \equiv \mathrm{tr}(\rho T_m^{(\mu)\dagger}) = 0.$$

So we conclude that if the state ρ is invariant under rotation around $\hat{z}$, then to specify its as a quantum reference frame we only need to specify its components in modes $\{(\mu, 0) : 1 \leq \mu \leq 2l\}$. Now using Eq. (4.7) we can easily show that the subspace spanned by

$$\{T_{m=0}^{(\mu)} : 1 \leq \mu \leq 2l\}$$

is the same as the subspace spanned by

$$\{\left(T_{m=0}^{(1)}\right)^k : 1 \leq k \leq 2l\}$$

To see this we use Eq. (4.7) to decompose the product of irreducible tensor operators to the sum of irreducible tensor operators. Then Eq. (4.7) implies that the problem of decomposing $\left(T_{m=0}^{(1)}\right)^k$ to irreducible tensor operators is exactly equivalent to the problem of decomposing state $|j = 1, m = 0\rangle^{\otimes k}$ to irreps of SO(3). It follows that that i) $\left(T_{m=0}^{(1)}\right)^k$

has a nonzero component in mode $(\mu = k, 0)$ and ii) $\left(T^{(1)}_{m=0}\right)^k$ does not have any nonzero component in modes $(\mu > k, 0)$.

So it follows that the span of $\{T^{(\mu)}_{m=0} : 1 \leq \mu \leq 2l\}$ is the same as span of $\{\left(T^{(1)}_{m=0}\right)^k : 1 \leq k \leq 2l\}$. So to specify all the components of ρ in modes $\{(\mu, 0) : 1 \leq \mu \leq 2l\}$ one can specify all the moments of $\{\mathrm{tr}(\rho \left(T^{(1)}_{m=0}\right)^k) : 1 \leq k \leq 2l\}$ or equivalently the moments $\{\mathrm{tr}(\rho L_z^k) : 1 \leq k \leq 2l\}$. This completes the proof of corollary 44.

Chapter 6

Asymmetry of pure states

In this chapter we focus on the study of asymmetry of pure states. We find a simple characterization of asymmetry of pure states. Then using this characterization we study different problems about interconvertability of pure states under symmetric operations.

6.1 Unitary G-equivalence

In chapter 2 we defined the notion of G-equivalence classes of states and we argued that the G-equivalence class of a state specifies all its asymmetry properties.

It is useful to introduce another equivalence relation over states that is slightly stronger than G-equivalence. Let $g \to U(g)$ be the projective unitary representation of the symmetry described by group G on the Hilbert space of a system. Then

Definition 46 (Unitary G-equivalence) *Two pure states, ψ and ϕ, are called* unitarily G-equivalent *if they are interconvertible by a G-invariant unitary, that is, if there exists a unitary $V_{G\text{-}inv}$ such that $\forall g \in G : [V_{G\text{-}inv}, U(g)] = 0$ and*

$$V_{G\text{-}inv}|\psi\rangle = |\phi\rangle \tag{6.1}$$

Recall two alternative points of view to the notion of asymmetry introduced in chapter 2, i.e. the constrained-dynamical point of view and the information-theoretic point of view. This definition is based on the constrained-dynamical point of view. Alternatively we can define this concept in the information-theoretic point of view in terms of the unitary

interconvertability of the covariant sets defined by the two states. The equivalence of these two definitions follows trivially from lemma 8.

As we will see later, it turns out that for connected compact Lie groups it is a small step from characterizing unitary G-equivalence to characterizing general G-equivalence. In particular in section 6.3, we will show that for semi-simple connected compact Lie groups the unitary G-equivalence classes are the same as the G-equivalence classes.

6.1.1 The constrained-dynamical characterization: equality of the reductions onto irreps

We here find a characterization of the unitary G-equivalence classes within the restricted-dynamical perspective. We begin by determining the most general form of a G-invariant unitary.

Suppose $\{U(g) : g \in G\}$ is a projective unitary representation of a finite or compact Lie group G on the Hilbert space $\mathcal{H}$. We can always decompose this representation to a discrete set of finite dimensional irreducible projective unitary representations (irreps). This suggests the following decomposition of the Hilbert space [1],

$$\mathcal{H} = \bigoplus_{\mu} \mathcal{M}_\mu \otimes \mathcal{N}_\mu, \tag{6.2}$$

where μ labels the irreducible representations and $\mathcal{N}_\mu$ is the subsystem associated to the multiplicities of representation μ (the dimension of $\mathcal{N}_\mu$ is equal to the number of multiplicities of the irrep μ in this representation). Then $U(g)$ can be written as

$$U(g) = \bigoplus_{\mu} U_\mu(g) \otimes \mathbb{I}_{\mathcal{N}_\mu} \tag{6.3}$$

where $U_\mu(g)$ acts on $\mathcal{M}_\mu$ irreducibly and where $\mathbb{I}_{\mathcal{N}_\mu}$ is the identity operator on the multiplicity subsystem $\mathcal{N}_\mu$. We denote by Π_μ the projection operator onto the subspace $\mathcal{M}_\mu \otimes \mathcal{N}_\mu$, the subspace associated to the irrep μ.

Now we are ready to characterize the unitary G-equivalence classes:

Theorem 47 *Two pure states $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if and only if*

$$\forall \mu : \ \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu \ |\psi\rangle\langle\psi| \ \Pi_\mu) = \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu \ |\phi\rangle\langle\phi| \Pi_\mu) \tag{6.4}$$

Proof. First, we find a simple characterization of G-invariant unitaries. Using decomposition (6.3) and Schur's lemmas, one can show that any arbitrary G-invariant unitary is of the following form [1],

$$V_{\text{G-inv}} = \bigoplus_{\mu} \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}, \tag{6.5}$$

where $V_{\mathcal{N}_\mu}$ acts unitarily on $\mathcal{N}_\mu$.

Now suppose state $|\psi\rangle$ can be transformed to another state $|\phi\rangle$ by a G-invariant unitary $V_{\text{G-inv}}$. Then given that $V_{\text{G-inv}}$ has a decomposition in the form of Eq. (6.5), it follows that for all μ,

$$\Pi_\mu|\phi\rangle = \Pi_\mu V_{\text{G-inv}}|\psi\rangle = \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}\Pi_\mu|\psi\rangle \tag{6.6}$$

Eq. (6.4) then follows from the cyclic property of the trace and the unitarity of $V_{\mathcal{N}_\mu}$.

Now we prove the reverse direction. If Eq. (6.4) holds, then there exists a G-invariant unitary which transforms $|\psi\rangle$ to $|\phi\rangle$. First note that we can think of the two vectors $\Pi_\mu|\psi\rangle$ and $\Pi_\mu|\phi\rangle$ as two different purifications of $\text{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\psi\rangle\langle\psi|\Pi_\mu) = \text{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\phi\rangle\langle\phi|\Pi_\mu)$. So $\Pi_\mu|\psi\rangle$ can be transformed to $\Pi_\mu|\phi\rangle$ by a unitary acting on $\mathcal{N}_\mu$, denoted by $V_{\mathcal{N}_\mu}$, such that

$$\mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}\Pi_\mu|\psi\rangle = \Pi_\mu|\phi\rangle \tag{6.7}$$

(See e.g.[17]). By defining

$$V \equiv \bigoplus_{\mu} \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu} \tag{6.8}$$

we can easily see that V is a G-invariant unitary and moreover $V|\psi\rangle = |\phi\rangle$. This completes the proof. ■

For arbitrary state ρ we call the set of operators $\{\text{tr}_{\mathcal{N}_\mu}(\Pi_\mu\ \rho\ \Pi_\mu)\}$, the *reduction onto irreps* of ρ. So in the above theorem we have proven that the unitary G-equivalence class of a pure state is totally specified by its reduction onto irreps. Note, however, that as we will see in Sec. 6.2.1, this is not true for general mixed states.

Example 48 *Recall the quantum optics example studied in section 1.4.2 where the set of all phase shifts forms a representation of group U(1). There the representation of group U(1) is $e^{i\theta} \to U(\theta)$ where the phase shift operator $U(\theta)$ is*

$$U(\theta) \equiv e^{iN\theta} = \sum_n e^{in\theta} \sum_\alpha |n,\alpha\rangle\langle n,\alpha| \tag{6.9}$$

where N is the number operator with integer eigenvalues such that $N|n,\alpha\rangle = n|n,\alpha\rangle$ and where α is a multiplicity index. In this case all irreps are one dimensional. It follows that the reduction onto irreps of a pure state $|\psi\rangle = \sum_{n,\alpha} \psi_{n,\alpha}|n,\alpha\rangle$ is simply given by

$$p_\psi(n) \equiv \langle\psi|\Pi_n|\psi\rangle = \sum_\alpha |\psi_{n,\alpha}|^2 \tag{6.10}$$

that is, the probability distribution over the number operator induced by $|\psi\rangle$, where Π_n is the projector to the eigen-subspace corresponding to the eigenvalue n of N. Consequently, two pure states are unitarily U(1)-equivalent if and only if they define the same probability distribution over eigen-subspaces of the number operator.

6.1.2 The information-theoretic characterization: equality of characteristic functions

We will show that by taking the information-theoretic point of view, one finds that the unitary G-equivalence class of a pure state is specified entirely by its characteristic function, which is defined as follows.

Definition 49 (Characteristic function) *The* characteristic function *of a state ρ relative to a projective unitary representation $\{U(g) : g \in G\}$ of a group G is a function $\chi_\rho : G \to \mathbb{C}$ of the form*

$$\chi_\rho(g) \equiv tr\,(\rho U(g)) \tag{6.11}$$

Specifically, we have

Theorem 50 *Two pure states $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if and only if their characteristic functions are equal,*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle. \tag{6.12}$$

The benefit of trying to characterize the G-equivalence classes using the information-theoretic perspective is that we can make use of known results concerning the unitary interconvertability of sets of pure states. We express the condition for such interconvertability as a lemma, after recalling the definition of the Gram matrix of a set of states.

Definition 51 (Gram matrix) *Consider the set of states* $\{|\psi_\theta\rangle\}$. *If* θ *is a discrete parameter, then we define the* Gram matrix *of the set* $\{|\psi_\theta\rangle\}$ *by* $X_{\theta,\theta'} \equiv \langle\psi_\theta|\psi_{\theta'}\rangle$. *If* θ *is a continuous parameter, then we can define the function* $X(\theta,\theta') \equiv \langle\psi_\theta|\psi_{\theta'}\rangle$, *which, with a slight abuse of terminology, we will also call the* Gram matrix *of the set* $\{|\psi_\theta\rangle\}$.

Lemma 52 *There exists a unitary operator* V *which transforms* $\{|\psi_\theta\rangle\}$ *to* $\{|\phi_\theta\rangle\}$, *that is,* $\forall\theta:\ V|\psi_\theta\rangle = |\phi_\theta\rangle$, *if and only if the Gram matrices of the two sets of states are equal, i.e.*

$$\forall\theta,\theta':\quad \langle\psi_\theta|\psi_{\theta'}\rangle = \langle\phi_\theta|\phi_{\theta'}\rangle$$

A simple proof of this lemma is provided in the footnote.[1]

It is now straightforward to prove theorem 50.

Proof of theorem 50. By definition 46, $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if there exists a unitary transformation $V_{\text{G-inv}}$ which take $|\psi\rangle$ to $|\phi\rangle$. By lemma 8 there exists such a unitary if and only if there exists a unitary V such that $\forall g\in G:\ VU(g)|\psi\rangle = U(g)|\phi\rangle$. By lemma (52), the necessary and sufficient condition for the existence of such a unitary is the equality of the Gram matrices of the set $\{U(g)|\psi\rangle : g\in G\}$ and the set $\{U(g)|\phi\rangle : g\in G\}$. Given that the elements of these matrices are, respectively,

$$[X_\psi]_{g_1,g_2} = \langle\psi|U^\dagger(g_1)U(g_2)|\psi\rangle = \omega(g_1^{-1},g_2)\langle\psi|U(g_1^{-1}g_2)|\psi\rangle,$$

and

$$[X_\phi]_{g_1,g_2} = \langle\phi|U^\dagger(g_1)U(g_2)|\phi\rangle = \omega(g_1^{-1},g_2)\langle\phi|U(g_1^{-1}g_2)|\phi\rangle,$$

their equality is equivalent to

$$\forall g\in \mathrm{G}:\quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle, \tag{6.13}$$

where we have use the fact $g\to U(g)$ is a projective unitary representation and so

$$U^\dagger(g_1)U(g_2) = U(g_1^{-1})U(g_2) = \omega(g_1^{-1},g_2)$$

for the cocycle ω. Eq.(6.13) is simply the statement that the characteristic functions $\chi_\psi(g)$ and $\chi_\phi(g)$ are equal. ■

[1] The necessity of the equality of the Gram matrices is trivial. Sufficiency is proven as follows. Suppose we use a subset $\{|\psi_{\theta_1}\rangle,|\psi_{\theta_2}\rangle,\cdots\}$ of $\{|\psi_\theta\rangle\}$ to build an orthonormal basis for the subspace spanned by $\{|\psi_\theta\rangle\}$ via the Gram-Schmidt process and call this basis I. Similarly, use the subset $\{|\phi_{\theta_1}\rangle,|\phi_{\theta_2}\rangle,\cdots\}$ of $\{|\phi_\theta\rangle\}$ to build an orthonormal basis for the subspace spanned by $\{|\phi_\theta\rangle\}$ via the Gram-Schmidt process and call this basis II. Recall that the Gram-Schmidt orthogonalization process depends only on the Gram matrix of the set of states. Since, by assumption, the Gram matrix of the two sets of states are equal then for any state $|\psi_\theta\rangle\in\{|\psi_\theta\rangle\}$ its description in basis I is the same as the description of the corresponding $|\phi_\theta\rangle\in\{|\phi_\theta\rangle\}$ in basis II. It follows that if V is the unitary which transforms basis I to basis II, then by linearity for all $|\psi_\theta\rangle\in\{|\psi_\theta\rangle\}$, V maps $|\psi_\theta\rangle$ to the state $|\phi_\theta\rangle$. This proves the lemma.

Example 53 *In example 48 we found the characterization of unitary equivalence classes based the reduction of states to irreps in the case of group U(1) with representation* $e^{i\theta} \to e^{i\theta N}$ *where* N *is the number operator with integer eigenvalues. Here, we use the result of lemma 52 to find another characterization of these unitary equivalence classes in terms of characteristic function of states. In this case, for arbitrary state* $|\psi\rangle = \sum_{n,\alpha} \psi_{n,\alpha}|n,\alpha\rangle$ *the characteristic function of state* $|\psi\rangle$ *is given by the expectation value of the phase shift operator, i.e.*

$$\chi_\psi(\phi) \equiv \langle\psi| \exp(i\phi N)|\psi\rangle = \sum_n p_\psi(n) e^{in\phi} \tag{6.14}$$

where $p_\psi(n) = \sum_\alpha |\psi_{n,\alpha}|^2$ *is the reduction onto irreps.*

As we saw in the above example, in the U(1) case, the reduction onto irreps and the characteristic function are related by a Fourier transform. The Fourier transform can also be defined for arbitrary compact Lie groups (which might be non-Abelian) or for finite groups and in these cases, it also describes the relation between the reduction onto irreps and the characteristic function, as will be shown in section 6.2.

6.1.3 Approximate notion of unitary G-equivalence

We have found the necessary and sufficient condition for the existence of a G-invariant unitary which transforms a pure state ψ to another pure state ϕ. This is the condition for exact transformation. But there might be situations in which we cannot transform ψ to ϕ but we can transform it to some state close to ϕ.

In the following we demonstrate that if the reductions onto irreps of two pure states ψ and ϕ are close (or equivalently their characteristic functions are close) then there exists a G-invariant unitary which transforms ψ to a state close to ϕ.

Recall that the fidelity of two positive operators A_1 and A_2 is defined as

$$\mathrm{Fid}(A_1, A_2) \equiv \|\sqrt{A_1}\sqrt{A_2}\| = \mathrm{tr}(\sqrt{\sqrt{A_1}A_2\sqrt{A_1}}) \tag{6.15}$$

where $\|\cdot\|$ denotes the trace norm. [2]

[2] It is worth mentioning that the fidelity of states is monotone under information processing, i.e. $\mathrm{Fid}(\rho_1, \rho_2) \leq \mathrm{Fid}\left(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)\right)$ for any channel $\mathcal{E}$.

Theorem 54 *Suppose* $\{F_1^{(\mu)}\}$ *and* $\{F_2^{(\mu)}\}$ *are respectively the reductions onto irreps of* ψ_1 *and* ψ_2 *two arbitrary states in the same Hilbert space. Then for any G-invariant unitary* V *acting on this space*

$$|\langle\psi_2|V|\psi_1\rangle| \leq \sum_{\mu} Fid(F_1^{(\mu)}, F_2^{(\mu)}) \tag{6.16}$$

Furthermore there exists a G-invariant unitary V *for which the equality holds.*

According to this theorem if the fidelities of the reductions onto irreps is high then there exists a G-invariant unitary which transforms one of the states to a state very close to the other. On the other hand, if these fidelities are low we can never transform one of the states to a state close to the other via G-invariant unitaries.

Remark 55 *For* $\{F_1^{(\mu)}\}$ *and* $\{F_2^{(\mu)}\}$ *the reductions of arbitrary pairs of states it holds that* $\sum_\mu Fid(F_1^{(\mu)}, F_2^{(\mu)}) \leq 1$ *and the equality holds iff* $\forall\mu : F_1^{(\mu)} = F_2^{(\mu)}$*. So theorem 54 is indeed a generalization of theorem 47.*

We present the proof of theorem 54 as well as some other versions of it and the proof of remark 55 in appendix A.5.

Example 56 *Recall our quantum optics example where the set of all phase shifts forms a representation of group U(1) (see example 48). Suppose* $\{p_\psi(n)\}$ *and* $\{p_\phi(n)\}$ *are reductions onto irreps for two states* ψ *and* ϕ *(So they are two probability distributions over integers). Then theorem 54 implies that for any U(1)-invariant unitary* V*,*

$$|\langle\psi|V|\phi\rangle| \leq \sum_{n} \sqrt{p_\psi(n)p_\phi(n)} \tag{6.17}$$

and furthermore there exists a U(1)-invariant unitary for which the equality holds.

6.2 What are the reduction onto irreps and the characteristic function?

We have found two different characterizations of the unitary G-equivalence class of of pure states, namely the characteristic function of states and the reduction onto irreps of states. In this section, we will show that the reduction onto the irreps and the characteristic

function are simply two particular representations of the reduction of the state to the associative algebra (for the degree of freedom associated to the symmetry transformation) and that these representations are related to one another by a generalized Fourier transform. Furthermore, we provide a list of properties of characteristic functions which will be useful in the rest of this chapter.

In appendices A.3 and A.4 we present more discussions about the meaning of characteristic functions of states. In appendix A.3 we discuss about the interpretation of the absolute value of the characteristic function of state ψ,

$$|\chi_\psi(g)| = \langle\psi|U(g)|\psi\rangle| \,,$$

in terms of the pairwise distinguishability of states in the set $\{U(g)|\psi\rangle : g \in G\}$. In particular, we argue that though the function $|\chi_\psi(g)|$ uniquely specifies all the pairwise distinguishabilities in this set, nevertheless it cannot specify the information that can be transferred using the encoding $g \to U(g)|\psi\rangle$ and so it can not specify the asymmetry of state ψ. Also, in appendix A.4 we show that the characteristic function of a quantum state can be thought as a natural generalization of the notion of the characteristic function of a probability distribution.

6.2.1 Two representations of the reduction to the associative algebra

If we are interested in only some particular degree of freedom of a quantum system then we do not need the full description of the state in order to infer the statistical features (expectation values, variances, correlations between two different observables, etcetera) of that degree of freedom. In particular suppose we are interested in the statistical properties of the set of operators $\{O_i \in \mathcal{B}(\mathcal{H})\}$. Closing this set under the operator product and sum yields the associative algebra generated by $\{O_i\}$, which is the set of all polynomials in $\{O_i\}$. We denote this associative algebra by $\text{Alg}\{O_i\}$. To specify all the statistical properties of the state $\rho \in \mathcal{B}(\mathcal{H})$ for the set of observables $\{O_i\}$ it is necessary and sufficient to specify all the expectation value of the state for the operators in $\text{Alg}\{O_i\}$. The object that contains all and only this information is called the reduction of the state to the associative Algebra, denoted $\rho|_{\text{Alg}\{O_i\}}$.

$\text{Alg}\{O_i\}$, considered as a finite-dimensional C^*-algebra, has a unique decomposition (up to unitary equivalence) of the form

$$\bigoplus_J \mathfrak{M}_{m_J} \otimes \mathbb{I}_{n_J} \tag{6.18}$$

where $\mathfrak{M}_{m_J}$ is the full matrix algebra $\mathcal{B}(\mathbb{C}^{m_J})$ and $\mathbb{I}_{n_J}$ is the identity on $\mathbb{C}^{n_J}$ [58]. This means that there is a basis in which any element A of the algebra can be written as

$$A = \bigoplus_J A^{(J)} \otimes \mathbb{I}_{n_J} \tag{6.19}$$

where $A^{(J)} \in \mathcal{B}(\mathbb{C}^{m_J})$. Furthermore, if we consider the set of all elements of the algebra, that is, all $A \in \text{Alg}\{O_i\}$, and look at the set of corresponding $A^{(J)}$ for fixed J, this set of operators acts irreducibly on $\mathbb{C}^{m_J}$ and spans $\mathcal{B}(\mathbb{C}^{m_J})$. Clearly this decomposition induces the following structure on the Hilbert space

$$\mathcal{H} = \bigoplus_J \mathcal{M}_J \otimes \mathcal{N}_J. \tag{6.20}$$

where $\mathcal{M}_J$ is isomorphic to $\mathbb{C}^{m_J}$ and $\mathcal{N}_J$ is isomorphic to $\mathbb{C}^{n_J}$.

Suppose Π_J is the projective operator to the subspace $\mathcal{M}_J \otimes \mathcal{N}_J$. Then to specify all the relevant information about the observables in the Algebra for the given state ρ it is necessary and sufficient to know all of the operators

$$\rho^{(J)} \equiv tr_{\mathcal{N}_J}(\Pi_J \rho \Pi_J). \tag{6.21}$$

Then for any arbitrary observable A in the Algebra we have

$$\text{tr}(A\rho) = \sum_J \text{tr}(A^{(J)}\rho^{(J)}) \tag{6.22}$$

and so specifying the set $\{\rho^{(J)}\}$ we know all the relevant information about the state. In other words, $\{\rho^{(J)}\}$ uniquely specifies the reduction to the Algebra $\rho|_{\text{Alg}\{O_i\}}$.

The above discussion applies to any arbitrary set of observables. Here, we will be interested in the case where this set describes the degree of freedom associated to some symmetry transformation. If the symmetry transformation is associated with the symmetry group G and projective unitary representation $\{U(g) : g \in G\}$ on the Hilbert space of the system, then the set of observables to consider are all those in the linear span of $\{U(g) : g \in G\}$. In particular, in the case of Lie groups this set contains the representation of all generators of the Lie Algebra (associated to the group) and all the polynomials formed by these generators. For example, in the case of SO(3) the set includes all the observables in the linear span of $\{U(\Omega) : \Omega \in SO(3)\}$ and so it clearly contains all the generators, which in this case are angular momentum operators, as well as all polynomials of these generators.

Decomposition of this algebra in the form of Eq. (6.18) in fact coincides with the decomposition of the unitary projective representation $\{U(g) : g \in G\}$ to irreps

$$U(g) \cong \bigoplus_{\mu} U^{(\mu)}(g) \otimes \mathbb{I}_{N_\mu} \tag{6.23}$$

where μ labels the irreps and $\mathbb{I}_{N_\mu}$ is the identity acting on the multiplicity subsystem associated to irrep μ (Remember that G is by assumption a finite or compact Lie group and so it is completely reducible.). Here we can think of μ playing the same role as J in the decomposition of the arbitrary Algebra in Eq. (6.18). Each irrep index μ appearing in the decomposition of $\{U(g) : g \in G\}$ corresponds to one J in Eq. (6.18) and the set $\{U^\mu(g) : g \in G\}$ for a fixed μ spans the full matrix algebra $\mathfrak{M}_{m_J}$ of the corresponding J. Consequently, the spaces on which the projective unitary representation of G acts irreducibly are simply the $\mathcal{M}_J$. So it follows that in this case, where the associative Algebra coincides with the span of the elements of the projective unitary representation of the group, $\{U(g) : g \in G\}$, the set of operators $\{\rho^{(J)}\}$ (defined by Eq.(6.21)) is simply the reduction onto the irreps of the state ρ, the generalization to mixed states of the notion defined in the section 6.1.1, and therefore we can conclude that the reduction onto the irreps is a representation of the reduction onto the associative algebra.

Another way to specify the reduction of the state onto the associative algebra is to specify the Hilbert-Schmidt inner product of ρ with each of the $U(g)$, namely, $\mathrm{tr}(\rho U(g))$ for all $g \in$ G. So if we define the characteristic function associated to the state ρ as the function $\chi_\rho : G \to \mathbb{C}$ defined by $\chi_\rho(g) \equiv \mathrm{tr}(\rho U(g))$, then the characteristic function is a particular representation of the reduction to the associative algebra. It is clear that this definition constitutes a generalization to mixed states of the notion of characteristic functions introduced in the section 6.1.2.

To summarize, we have

Remark 57 *For a state $\rho \in \mathcal{B}(\mathcal{H})$ and a projective unitary representation U of a group G, the reduction of ρ to the associative algebra $Alg\{U(g) : g \in G\}$ can be represented either in terms of the* reduction onto irreps *of ρ, defined as*

$$\{\rho^{(\mu)} \equiv tr_{\mathcal{N}_\mu}(\Pi_\mu \rho \Pi_\mu)\}, \tag{6.24}$$

(where the Hilbert space decomposition induced by U is $\mathcal{H} = \bigoplus_\mu \mathcal{M}_\mu \otimes \mathcal{N}_\mu$ and Π_μ projects onto $\mathcal{M}_\mu \otimes \mathcal{N}_\mu$), or in terms of the characteristic function *of ρ, defined as*

$$\chi_\rho(g) \equiv tr(\rho U(g)). \tag{6.25}$$

Finally, we note that the relationship between these two representations is the Fourier transform over the group.

Proposition 58 *The characteristic function and reduction onto irreps can be computed one from the other via*

$$\chi_\rho(g) = \sum_\mu tr(\rho^{(\mu)} U^{(\mu)}(g)) \tag{6.26}$$

and

$$\rho^{(\mu)} = d_\mu \int dg \chi_\rho(g^{-1}) U^{(\mu)}(g). \tag{6.27}$$

Proof. The expression for $\chi_\rho(g)$ in terms of $\{\rho^{(\mu)}\}$, Eq. (6.26), follows directly from Eqs. (6.23) and (6.25). Conversely, to find the $\{\rho^{(\mu)}\}$ in terms of $\chi_\rho(g)$ we use the Fourier transform over the group. The idea is based on the following orthogonality relations which are part of the Peter-Weyl theorem (See e.g. [12]):

$$\int_G dg U^{(\mu)}_{i,j}(g) \overline{U}^{(\nu)}_{k,l}(g) = \frac{\delta_{\mu,\nu}\delta_{i,k}\delta_{j,l}}{d_\mu} \tag{6.28}$$

where dg is the unique Haar measure on the group, bar denotes complex conjugate and d_μ is the dimension of irrep μ. According to this theorem any continuous function on a compact Lie group can be uniformly approximated by linear combinations of matrix elements $U^{(\mu)}_{i,j}(g)$. Note that for the finite groups, we can get the same orthogonality relations by replacing the integral with a summation. Furthermore any function over a finite group can be expressed as a linear combination of the matrix elements of irreps. So basically all the properties we use hold for finite groups as well as compact Lie groups.

An arbitrary operator $A^{(\mu)}$ in $\mathcal{B}(\mathcal{M}_\mu)$ can be written as a linear combination of elements of $\{U^{(\mu)}(g) : \ g \in G\}$. The above orthogonality relations implies that this expansion has a simple form as

$$A^{(\mu)} = d_\mu \int dg \ U^\mu(g) \ \ \mathrm{tr}(A^{(\mu)} U^\mu(g^{-1})) \tag{6.29}$$

Clearly this can be considered as a completeness relation where we have decomposed the identity map on $\mathcal{B}(\mathcal{M}_\mu)$ as the sum of projections to a basis (which is generally overcomplete). Also note that the orthogonality relations imply that for $\nu \neq \mu$

$$\int dg \ U^\nu(g) \mathrm{tr}(A^{(\mu)} U^\mu(g^{-1})) = 0 \qquad (\nu \neq \mu) \tag{6.30}$$

Using these orthogonality relations, we obtain Eq. (6.27). ■

We should emphasize that the reduction onto the associative algebra, though sufficient for deciding G-equivalence of pure states, is not in general sufficient for deciding G-equivalence of arbitrary states, i.e., mixed and pure. Its sufficiency in the case of pure states follows from its sufficiency for deciding unitary G-equivalence (proven in Sec. 6.1.2) and the fact that the unitary G-equivalence classes are a fine-graining of the G-equivalence classes. Its insufficiency in the case of mixed states can be established by the following simple example of two states (one pure and one mixed) that have the same characteristic function but fall in different G-equivalence classes. The example is for the case of U(1)-covariant operations, and the two states are $\frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)$ and $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. The second is clearly U(1)-invariant while the first is not and so they must lie in different U(1)-equivalence classes. Nonetheless, the characteristic function for both equals $\chi(\theta) = 1/2(1 + \exp(i\theta))$.

We close this section by mentioning another consequence of the orthogonality relations Eq.(6.28) which is useful later. Suppose A, B are arbitrary operators in $\mathcal{B}(\mathcal{M}_\mu)$ and

$$\chi_A(g) \equiv \mathrm{tr}(AU^{(\mu)}(g)), \quad \chi_B(g) \equiv \mathrm{tr}(BU^{(\mu)}(g)), \quad \text{and} \quad \chi_{AB}(g) \equiv \mathrm{tr}(ABU^{(\mu)}(g))$$

are respectively the characteristic functions of A, B and AB. Then

$$\chi_{AB} = d_\mu \; \chi_A * \chi_B \tag{6.31}$$

where $*$ is the convolution of two functions [3]

$$f_1 * f_2(g) \equiv \int dh f_1(gh^{-1}) f_2(h) \tag{6.32}$$

In particular, since $\mathrm{tr}(AB) = \chi_{AB}(e)$ (where e is the identity of group) the above formula can be used to find $\mathrm{tr}(AB)$ in terms of the characteristic functions of A and B. Using Eq.(6.31) we get

$$\begin{aligned} \mathrm{tr}(AB) = \chi_{AB}(e) &= d_\mu \; [\chi_A * \chi_B](e) \\ &= d_\mu \int dh \; \chi_A(h)\chi_B(h^{-1}) \end{aligned}$$

6.2.2 Properties of characteristic functions

The characteristic functions introduced here are quantum analogues of those used in classical probability theory. The connection is discussed in detail in Appendix A.4. Here we simply summarize some useful properties of characteristic functions.

[3] Note that for non-Abelian groups $f_1 * f_2$ is not necessarily equal to $f_2 * f_1$.

1. A function $\phi(g)$ from the finite or compact Lie group G to complex numbers is the characteristic function of a physical state iff it is (continuous in the case of Lie groups) positive definite (as defined in appendix A.4) and normalized (i.e. $\phi(e) = 1$ where e is the identity of group.). (This property assumes that all irreps are physically accessible.)

2. The characteristic function of a state is invariant under G-invariant unitaries acting on that state,
$$\chi_{\mathcal{V}_{\text{G-inv}}[\rho]}(g) = \chi_\rho(g),$$
where $\mathcal{V}_{\text{G-inv}}[\cdot] = V_{\text{G-inv}}(\cdot)V_{\text{G-inv}}^\dagger$ and $[V_{\text{G-inv}}, U(g)] = 0$ for all $g \in G$.

3. Characteristic functions multiply under tensor product,
$$\chi_{\rho\otimes\sigma}(g) = \chi_\rho(g)\chi_\sigma(g). \tag{6.33}$$

4. $|\chi_\rho(g)| \leq 1$ for all $g \in G$ and $\chi_\rho(e) = 1$ where e is the identity of group.

5. If $|\chi_\rho(g_s)| = 1$ for $g_s \in G$ then g_s is a symmetry of ρ. If ρ is a pure state, then g_s is a symmetry of ρ if and *only if* $|\chi_\rho(g_s)| = 1$.

6. So $|\chi_\rho(g)| = 1$ for all $g \in G$ implies that the state is invariant; in this case $\chi_\rho(g)$ is a 1-d representation of group.

7. Suppose L is the representation of a generator of the Lie group on the Hilbert space of system such that $\{e^{i\theta L} : \theta \in (0, 2\pi]\}$ is the representation of a U(1)-subgroup of the group. Then we can find all moments of L using the characteristic function.
$$\text{tr}(\rho L^k) = i^{-k}\frac{\partial^k}{\partial\theta^k}\chi_\rho(e^{i\theta L})\mid_{\theta=0} \tag{6.34}$$
(Note that by $\chi_\rho(e^{i\theta L})$ we really mean $\chi_\rho(g)$ for the group element $g \in G$ which is represented by $e^{i\theta L}$.)

Proof. Item 1 is proven in Appendix A.4.2. All the rest of these properties can simply be proved by using the definition of the characteristic function, $\chi_\rho(g) = \text{tr}(\rho U(g))$, and group representation properties. For example to prove item 3 we use the fact that if the representation of the symmetry G on the systems A (with state ρ) and B (with state σ) are $g \to U_A(g)$ and $g \to U_B(g)$ then the representation of the symmetry on the joint system AB is $g \to U_A(g) \otimes U_B(g)$. Then
$$\chi_{\rho\otimes\sigma}(g) = \text{tr}\left(\rho \otimes \sigma U_A(g) \otimes U_B(g)\right) = \text{tr}\left(\rho U_A(g)\right)\text{tr}\left(\sigma U_B(g)\right) = \chi_\rho(g)\chi_\sigma(g)$$

To prove 5 we note that if $|\chi_\rho(g_s)| = 1$ for $g_s \in G$ then all eigenvectors of ρ are eigenvectors of $U(g_s)$ with the same eigenvalue. As a result we get $[\rho, U(g_s)] = 0$ and so the state has the symmetry g_s. On the other hand, $[\rho, U(g_s)] = 0$ does not imply that $|\chi_\rho(g_s)| = 1$. For instance, the state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ where $|n\rangle$ is a number eigenstate is U(1)-invariant, but nonetheless, for $\phi \neq 0$, $|\chi_\rho(\phi)| \neq 1$. Therefore the points for which the amplitude of the characteristic function is one are a subset of the symmetries of the state. Meanwhile, if a *pure* state $|\psi\rangle$ has symmetry g_s, such that $U(g_s)|\psi\rangle = e^{i\theta}|\psi\rangle$ for some θ, then obviously $|\chi_\psi(g_s)| = 1$. So for pure states the points for which the amplitude of the characteristic function is one are exactly the state's symmetries.

To prove 6, we first note that if $|\chi_\rho(g)| = 1$ for all $g \in G$, then the symmetry subgroup of ρ is the entire group G, which is the definition of ρ being G-invariant. Furthermore, for each g, the eigenvectors of ρ all live in the same eigenspace of $U(g)$. Since the eigenvalue of a unitary is a phase factor, each such eigenvector $|\nu\rangle$ must satisfy $U(g)|\nu\rangle = e^{i\theta(g)}|\nu\rangle$ for some phase $e^{i\theta(g)}$. It is then clear that $\chi_\rho(g) = e^{i\theta(g)}$ and is a 1-dimensional representation of the group. ■

Among the above properties, the fact that the tensor product of states is represented by the product of their characteristic functions (property 3) turns out to be particularly useful. This is because the alternative representation, in terms of reductions onto irreps, does not provide a simple expression for the reduction of $\rho \otimes \sigma$ in terms of the reduction of ρ and the reduction of σ. It involves Clebsch-Gordon coefficients and is generally quite complicated for non-Abelian groups.

For this and other reasons, the characteristic function is generally our preferred way of representing the reduction of the state onto the algebra, and consequently we will make heavy use of it to answer various questions about the manipulation of asymmetry of pure states to answer various questions about the manipulation of asymmetry of pure states.

6.3 G-equivalence classes

We have seen that the characteristic function of a pure state uniquely specifies its unitary G-equivalence class. However, it is G-equivalence rather than unitary G-equivalence that implies that two states have the same asymmetry properties, so we must ultimately characterize the former. Fortunately, for the connected compact Lie groups, the conditions under which two states are G-equivalent can also be stated simply in terms of their characteristic functions, as is shown presently.

Theorem 59 *For G a connected compact Lie group, two pure states $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent (i.e. they can be reversibly interconverted one to the other by G-covariant operations) iff there exists a 1-dimensional representation of G, $e^{i\Theta(g)}$, such that*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = e^{i\Theta(g)}\langle\phi|U(g)|\phi\rangle. \tag{6.35}$$

Since the Semi-simple compact Lie groups do not have any non-trivial 1-dimensional representation, the above theorem implies

Corollary 60 *For G a semi-simple compact connected Lie group, two pure states $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent iff their characteristic functions are equal i.e.*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle. \tag{6.36}$$

The above theorem applies only to connected compact Lie groups. Putting a restriction on the states we can prove the following theorem which applies to both compact Lie groups and finite groups

Theorem 61 *Two pure states $|\psi\rangle$ and $|\phi\rangle$ for which $\langle\psi|U(g)|\psi\rangle$ and $\langle\phi|U(g)|\phi\rangle$ are nonzero for all $g \in G$ are G-equivalent (i.e. they can be reversibly interconverted one to the other by G-covariant operations) iff there exists a 1-dimensional representation of G, $e^{i\Theta(g)}$, such that*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = e^{i\Theta(g)}\langle\phi|U(g)|\phi\rangle. \tag{6.37}$$

Proof. (Theorems 59 and 61) The main tool we use in this proof is the Stinespring's dilation theorem for G-covariant channels discussed and proved in the section 4.4. According to this result any G-covariant channel can be implemented by coupling the system to an environment which is initially in a G-invariant state and the coupling can also be chosen to be a G-invariant unitary.

First we prove that Eq. (6.35) implies that $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent. Suppose $|\nu_0\rangle$ is a G-invariant state of the environment whose characteristic function is constant and equal to 1 for all group elements and $|\nu\rangle$ is a state of environment with characteristic function $e^{i\Theta(g)}$ where by assumption $e^{i\Theta(g)}$ is a 1-dimensional representation of the group (such states always exists by virtue of property 1 of characteristic functions listed in section 6.2.2). Then according to Eq. (6.35) and property 3 of characteristic functions (listed in the section 6.2.2), the characteristic function of $|\psi\rangle \otimes |\nu_0\rangle$ is the same as the characteristic function of $|\phi\rangle \otimes |\nu\rangle$. It follows from Theorem 50 that there exists a G-invariant unitary

which maps $|\psi\rangle \otimes |\nu_0\rangle$ to $|\phi\rangle \otimes |\nu\rangle$. So by coupling the system to an environment in state $|\nu_0\rangle$ via this G-invariant unitary and then discarding the environment we can transform $|\psi\rangle$ to $|\phi\rangle$. Note that such a transformation clearly would be a G-covariant operation. (Alternatively, let $|\nu^*\rangle$ be the state with characteristic function $e^{-i\Theta(g)}$. Note that since $e^{-i\Theta(g)}$ is also a 1-d representation of the group then by property 1 there exists a state $|\nu^*\rangle$ whose characteristic function is $e^{-i\Theta(g)}$. Then since $|\psi\rangle \otimes |\nu^*\rangle$, and $|\phi\rangle \otimes |\nu_0\rangle$ have the same characteristic function, by Theorem 50 there exists a G-invariant unitary which transforms one to the other. Because $|\nu^*\rangle$ is a G-invariant state and because the unitary is G-invariant, the overall operation is G-covariant.)

Using an analogous argument, we can easily deduce that there also exists a G-covariant operation which maps $|\phi\rangle$ to $|\psi\rangle$. Therefore $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent.

We now prove the other direction of the theorem. If $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent, then there exists a G-covariant operation from $|\psi\rangle$ to $|\phi\rangle$ and vice versa. It then follows from the Stinespring's dilation theorem that there exists a G-invariant unitary V and a G-invariant pure state $|\eta_1\rangle$ such that

$$V|\psi\rangle|\eta_1\rangle = |\phi\rangle|\eta_2\rangle \tag{6.38}$$

for some pure state $|\eta_2\rangle$, and there exists a G-invariant unitary V' and a G-invariant pure state $|\eta_1'\rangle$ such that

$$V'|\phi\rangle|\eta_1'\rangle = |\psi\rangle|\eta_2'\rangle$$

for some pure state $|\eta_2'\rangle$. These two equations together imply that

$$V'V|\psi\rangle|\eta_1\rangle|\eta_1'\rangle = |\psi\rangle|\eta_2\rangle|\eta_2'\rangle \tag{6.39}$$

Since V' and V are both G-invariant we can deduce that the characteristic functions of $|\psi\rangle|\eta_1\rangle|\eta_1'\rangle$ and $|\psi\rangle|\eta_2\rangle|\eta_2'\rangle$ are equal. i.e.

$$\chi_\psi \chi_{\eta_1} \chi_{\eta_1'} = \chi_\psi \chi_{\eta_2} \chi_{\eta_2'} \tag{6.40}$$

Since $|\eta_1\rangle$ and $|\eta_1'\rangle$ are both G-invariant states the amplitude of their characteristic functions are always one and so

$$|\chi_\psi| = |\chi_\psi||\chi_{\eta_2}\chi_{\eta_2'}| \tag{6.41}$$

Now suppose G is a connected compact Lie group. Then for any state ψ in a finite dimensional Hilbert space, $|\chi_\psi|$ is 1 at identity and is non-vanishing for a neighbourhood around identity in any direction. This implies that $|\chi_{\eta_2}\chi_{\eta_2'}|$ has value 1 for a neighbourhood around identity in any direction. By analyticity of the characteristic functions in finite dimension, this implies that $|\chi_{\eta_2}\chi_{\eta_2'}|$ is 1 everywhere. Therefore $|\eta_2\rangle|\eta_2'\rangle$ is an invariant

state. Note that it is this step of the proof which necessitates the restriction to connected compact Lie groups.

Since $|\eta_2\rangle|\eta_2'\rangle$ is G-invariant then $|\eta_2\rangle$ is also G-invariant. Therefore Eq. (6.38) implies that

$$\chi_\psi(g) = \chi_\phi(g) e^{i[\Theta_2(g) - \Theta_1(g)]} \tag{6.42}$$

where $e^{i\Theta_1(g)}$ and $e^{i\Theta_2(g)}$ are respectively the characteristic functions of $|\eta_1\rangle$ and $|\eta_2\rangle$. Finally, because $e^{i\Theta_1(g)}$ and $e^{i\Theta_2(g)}$ are 1-dimensional representations of G, it follows that $e^{i[\Theta_2(g) - \Theta_1(g)]}$ is as well. This completes the proof of Theorem 59.

As we mentioned above, there is only one point in the proof in which we use the assumption that the group is a connected Lie group: the fact that $|\chi_\psi| = |\chi_\psi||\chi_{\eta_2}\chi_{\eta_2'}|$ implies $|\chi_{\eta_2}\chi_{\eta_2'}| = 1$. This follows from the analyticity of the characteristic functions for finite dimensional representations of Lie groups. For finite groups, where we cannot appeal to the analyticity, if $|\chi_\psi|$ is zero at some $g \in G$ then $|\chi_\psi| = |\chi_\psi||\chi_{\eta_2}\chi_{\eta_2'}|$ does not imply $|\chi_{\eta_2}\chi_{\eta_2'}| = 1$ at that point. However, if we assume the function χ_ψ is nonzero for all $g \in G$ then we can again deduce $|\chi_{\eta_2}\chi_{\eta_2'}| = 1$ and the rest of the argument goes through as before. This completes the proof of theorem 61. ■

Example 62 *Recall our quantum optics example where the set of all phase shifts forms a representation of group U(1) (see example 48). For this representation of the symmetry U(1) it turns out that the criterion of U(1)-equivalence of pure states has a simple form in terms of reductions onto irreps. Suppose that the probability distributions* $\{p_\psi(n)\}_{n\in\mathbb{Z}}$ *and* $\{p_\phi(n)\}_{n\in\mathbb{Z}}$ *are the reductions onto the irreps of* ψ *and* ϕ *respectively, so that the characteristic functions are the Fourier transforms of these. Theorem 59 implies that* ψ *and* ϕ *are U(1)-equivalent if and only if there exists an integer* Δ *such that* $\sum_n p_\psi(n)e^{in\theta} = e^{i\Delta\theta}\sum_n p_\phi(n)e^{in\theta}$*, or equivalently, using the Fourier transform, such that*

$$p_\psi(n) = p_\phi(n + \Delta), \tag{6.43}$$

which is precisely the condition found in Ref. [16]. As a specific example, we can see that the states $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *and* $|\phi\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle)$ *are U(1)-equivalent either by noting that* $\chi_\psi(\theta) = e^{i2\theta}\chi_\phi(\theta)$ *or by noting that* $p_\psi(n) = p_\phi(n-2)$*.*

In the above proof, free operations V and V' together generate a closed reversible cycle: we start with state $|\psi\rangle$ (the resource) and use invariant states $|\eta_1\rangle$ (non-resources) to generate $|\phi\rangle|\eta_1'\rangle$ and then use $|\psi\rangle$ and couple it to $|\eta_2\rangle$ to get the state $|\psi\rangle|\eta_2'\rangle$. Using the properties of characteristic functions, we showed that the residue states $|\eta_2\rangle$ and $|\eta_2'\rangle$

should be invariant (non-resource). However this property can be derived from more general considerations. Suppose $|\eta_2\rangle|\eta_2'\rangle$ is not invariant. This implies that by going through this cycle we have generated some additional resource without consuming any. This should be impossible if the state $|\psi\rangle$ contains only a finite amount of the resource, which is indeed the case for any state on a finite-dimensional Hilbert space if the group is not finite.

6.4 Deterministic transformations

In this section we find the necessary and sufficient condition to determine whether a pure state ψ can be transformed to ϕ by a G-covariant channel. This is distinct from the question of G-equivalence because the transformation is not required to be reversible.

Theorem 63 *There exists a deterministic G-covariant map $\mathcal{E}$ transforming ψ to ϕ if and only if there exists a positive definite function f over group G such that $\chi_\psi(g) = \chi_\phi(g)f(g)$ for all $g \in G$.*

Note that if χ_ϕ is nonzero for all $g \in G$ then $f(g) = \chi_\psi(g)/\chi_\phi(g)$. So, in this case we can conclude that there exists a G-covariant map $\mathcal{E}$ transforming ψ to ϕ if and only if $\chi_\psi(g)/\chi_\phi(g)$ is a positive definite function. As it is discussed in the appendix A.4.2 one can test positive definiteness of $f(g)$ by verifying that the set of operators defining its Fourier transform are all positive.

Proof. (Theorem 63)

Similar to the proof of theorems 59 and 61 the main tool we use in this proof is the Stinespring's dilation theorem (also known as purification) of G-covariant channels discussed and proved in the section 4.4. By this result we know that the transformation can be achieve if and only if one can find an initial invariant ancilla state η and a final (possibly non-invariant) ancilla state ν such that $\psi\otimes\eta$ and $\varphi\otimes\nu$ are unitarily G-equivalent. One then discards ν at the end. In terms of characteristic functions it means that

$$\chi_\psi(g)e^{i\Theta(g)} = \chi_\varphi(g)\chi_\nu(g). \tag{6.44}$$

where $e^{i\Theta(g)}$ is a 1-d representation of the group, the characteristic function of the invariant state η, and $\chi_\nu(g)$ is the characteristic function of the discarded state ν. This implies $\chi_\psi(g) = \chi_\varphi(g)\left[\chi_\nu(g)e^{-i\Theta(g)}\right]$. Since $\chi_\nu(g)$ and $e^{-i\Theta(g)}$ are both positive definite then so is their product (see appendix). This proves one direction of the theorem. To prove the other direction, suppose there exists a a positive definite function $f(g)$ such that

$\chi_\psi(g) = \chi_\phi(g)f(g)$ for all $g \in G$. This obviously implies $f(e) = \chi_\psi(e)/\chi_\varphi(e) = 1$ and so the function is normalized. Then according to property 1 of characteristic functions, there exists a normalized state ν whose characteristic function is equal to $f(g)$. Now because the characteristic function of $\phi \otimes \nu$, i.e. $\chi_\varphi(g)f(g)$, is equal to χ_ψ, they are unitarily G-equivalent. Therefore, there exists a G-invariant unitary transforming $\psi \otimes \nu_0$ to $\phi \otimes \nu$ where ν_0 is the G-invariant state whose characteristic function is constant and equal to one for all group elements. So by applying this G-invariant unitary to $\psi \otimes \nu_0$ and transforming it to $\phi \otimes \nu$ and then discarding ν we can transform ψ to ϕ. Obviously this transformation is G-covariant. ■

It is worth noting that the necessary and sufficient condition for G-equivalence (Theorems 59 and 61) can also be obtained from the above result on deterministic transformations: If ψ and ϕ are G-equivalent, then there exist a G-covariant transformation from ψ to ϕ and a G-covariant transformation from ϕ to ψ. Then the above results implies that there exist normalized positive definite functions f_1 and f_2 such that $\chi_\psi(g) = \chi_\phi(g)f_1(g)$ and $\chi_\phi(g) = \chi_\psi(g)f_2(g)$. This implies that

$$\chi_\psi(g) = \chi_\psi(g)f_1(g)f_2(g) \tag{6.45}$$

and so if $\chi_\psi(g)$ is nonzero for all group elements it follows that $\forall g \in G : f_1(g)f_2(g) = 1$. But the absolute value of a positive definite function for all g is always less than or equal to its absolute value at the identity of the group. Then it follows that f_1 and f_2 should be 1-dimensional representations of the group which is the content of theorem 61. Similarly one can prove theorem 59 for the case of connected compact Lie groups.

In the following we present two examples for groups $U(1)$ and Z_N.

Example: U(1)-covariant deterministic transformations

Recall our quantum optics example where the set of all phase shifts forms a representation of group U(1) (see example 48). According to the theorem 63 there exists a deterministic U(1)-covariant map transforming ψ to ϕ if and only if there exists a positive definite $f(\theta)$ such that

$$\chi_\psi(\theta) = f(\theta)\chi_\phi(\theta) \tag{6.46}$$

Since $f(\theta)$ is positive definite all Fourier components of this function $\{q_n\}$ are positive. Furthermore, since $\chi_\psi(0) = \chi_\phi(0) = 1$ we conclude that $f(0) = 1$ which implies that $\sum_n q_n = 1$ and so the set $\{q_n\}$ is also a probability distribution. Suppose the set of probabilities $\{p_n^\psi\}$ and $\{p_n^\phi\}$ are the Fourier transformation of χ_ψ and χ_ϕ respectively.

Then the Fourier transform of the above equation implies

$$p_n^{\psi} = \sum_k p_{n-k}^{\phi} q_k \tag{6.47}$$

So the U(1)-covariant transformation from ψ to ϕ exists iff there exists a set of probabilities $\{q_n\}$ which satisfies the above equality. This is indeed the condition for deterministic interconversion in the U(1) case found in Ref. [16].

Example: Z_N-covariant deterministic transformations

Suppose the group under consideration is the group Z_N, the cyclic group of order N. For any N, the group Z_N is isomorphic to the group of integers $\{0, ...N-1\}$ where the group action is addition modulo to N. From now on we use this isomorphism to denote the group elements. These groups are clearly Abelian and so all of their irreps are one dimensional. We can easily see that these irrep can be identified by an integer J in the set $\{0, ...N-1\}$ such that the irreducible representation of group labeled by J is

$$k \in Z_N \to U_J(k) = e^{i2\pi Jk/N} \tag{6.48}$$

So an arbitrary (non-projective) unitary representation of Z_N, $k \in Z_N \to U(k)$, can be decomposed as

$$U(k) = \bigoplus_{J,\alpha} e^{iJk2\pi/N} |J,\alpha\rangle\langle J,\alpha| \tag{6.49}$$

where α labels multiplicities of irrep J and $\{|J,\alpha\rangle\}$ is a basis for the Hilbert space. An arbitrary state ψ in this basis can be expanded as

$$|\psi\rangle = \sum_{J,\alpha} \psi(J,\alpha)|J,\alpha\rangle \tag{6.50}$$

As with any other Abelian group, the reduction of the state onto the irreps is simply the probability distribution that the state induces over the irreps. So the reduction of ψ is specified by the probability distribution

$$\{p_\psi(J) \equiv \sum_\alpha |\psi(J,\alpha)|^2 : J = 0, ..., N\}.$$

On the other hand, the characteristic function of ψ is by definition the function $k \in \{0 \cdots N-1\} \to \langle\psi|U(k)|\psi\rangle$. So the characteristic function of ψ is

$$\chi_\psi(k) = \sum_{J,\alpha} |\psi(J,\alpha)|^2 e^{i2\pi Jk/N} \tag{6.51}$$

Clearly the characteristic function is the discrete Fourier transform of the reduction of the state onto the irreps.

Now we are interested to know whether there exists a Z_N-covariant quantum operation which transforms ψ to ϕ. Assuming the characteristic function of ϕ, i.e. $\chi_\phi(k)$ is nonzero for all k's, it follows from theorem 63 that such a Z_N-covariant map exists iff $\chi_\psi(k)/\chi_\phi(k)$ is a positive definite function. But this function is positive definite iff its Fourier transform is always positive, i.e. iff

$$q(J) \equiv \sum_k \frac{\chi_\psi(k)}{\chi_\phi(k)} e^{i2\pi Jk/N} \tag{6.52}$$

is positive for all $J = 0, ..., N$. So to summarize, the necessary and sufficient condition for existence of a Z_N-covariant channel which transforms ψ to ϕ is that

$$\forall J \in \{0, ..., N\} : \quad \sum_k \frac{\chi_\psi(k)}{\chi_\phi(k)} e^{i2\pi Jk/N} \geq 0 \tag{6.53}$$

Consider the case of Z_2 which has only two group elements denoted by $\{e, \pi\}$ where e is the identity of group and $\pi^2 = e$. Using the above convention we denote e by $k = 0$ and π by $k = 1$. This group has only two inequivalent irreps: The trivial representation $(J = 0)$ in which

$$U_{J=0}(0) = U_{J=0}(1) = 1$$

and the nontrivial $(J = 1)$ in which

$$U_{J=1}(1) = -U_{J=1}(0) = -1.$$

Then the reduction of ψ onto irreps is specified by the probability assigned to each of these irreps and in this case since there are only two irreps we only need to specify one of the probabilities, say $p_\psi(J = 0)$. The characteristic function of ψ is

$$\chi_\psi(k) = p_\psi(J = 0) + (-1)^k p_\psi(J = 1) \tag{6.54}$$

So $\chi_\psi(0) = 1$ and $\chi_\psi(1) = 2p_\psi(J = 0) - 1$. Then Eq.(6.53) implies that the transformation $\psi \xrightarrow{\text{G-cov}} \phi$ is possible iff

$$q(0) = \frac{\chi_\psi(0)}{\chi_\phi(0)} + \frac{\chi_\psi(1)}{\chi_\phi(1)} \geq 0 \tag{6.55}$$

and

$$q(1) = \frac{\chi_\psi(0)}{\chi_\phi(0)} - \frac{\chi_\psi(1)}{\chi_\phi(1)} \geq 0. \tag{6.56}$$

Since $\frac{\chi_\psi(0)}{\chi_\phi(0)}$ is always equal to one it turns out that the above two inequalities are equivalent to $|\chi_\psi(1)| \leq |\chi_\phi(1)|$, i.e.

$$|p_\psi(J=0) - p_\psi(J=1)| \leq |p_\phi(J=0) - p_\phi(J=1)| \tag{6.57}$$

Since

$$p_\psi(J=0) + p_\psi(J=1) = p_\phi(J=0) + p_\phi(J=1) = 1$$

the above condition is equivalent to the condition

$$\min\{p_\phi(J=0), p_\phi(J=1)\} \leq \min\{p_\psi(J=0), p_\psi(J=1)\} \tag{6.58}$$

which is exactly the same condition previously obtained in [16] using a totally different approach. Eq. (6.53) is the generalization of this specific result for arbitrary cyclic group Z_N.

6.5 Catalysis

In any resource theory, if state ψ cannot be converted to state ϕ deterministically under the restricted operations, it may still be the case that it is possible to do so using a *catalyst*, which is an ancillary system that is prepared in a state that is *not* free relative to the restriction that defines the resource theory but which must be returned to its initial state at the end of the procedure. For example, in the resource theory of entanglement it is a well-known fact that a transformation from a given state to another might be forbidden under LOCC but that transformation can be performed using LOCC and an appropriate catalysts [60].

In the case of the resource theory of asymmetry, a catalyst is a finite dimensional ancillary system in an *asymmetric* state which can be used to achieve the interconversion but only in such a way that its state remains unchanged at the end of process.

We shall say that the conversion ψ to ϕ is a nontrivial example of catalysis if there is no deterministic G-covariant channel under which ψ goes to ϕ, but there is a deterministic G-covariant channel and a catalyzing state ζ such that $\psi \otimes \zeta$ goes to $\phi \otimes \zeta$.

In the resource theory of asymmetry, whether there is nontrivial catalysis or not depends on the nature of the group. In the following we prove that in the case of compact connected Lie groups catalysts are totally useless. We also present an example which shows how catalysts can be useful in the case of finite groups.

It turns out that in the case of pure state transformations, characteristic functions give us a powerful insight into how a catalyst can make a transformation possible. Assume χ_ψ and χ_ϕ are respectively the characteristic functions of states ψ and ϕ for which there is no G-covariant transformations which take ψ to ϕ. Then from theorem 63 we know that if there is no G-covariant transformation from ψ to ϕ then there is no analytical positive definite function f over group G such that it satisfies

$$\forall g \in G: \ \chi_\psi(g) = \chi_\phi(g) f(g) \tag{6.59}$$

On the other hand, if this transformation is possible using a catalyst ζ with characteristic function χ_ζ then there should exists an analytical positive definite function f' such that $\forall g \in G$

$$\chi_\psi(g)\chi_\zeta(g) = \chi_\phi(g)\chi_\zeta(g) f'(g) \tag{6.60}$$

Now clearly for all points $g \in G$ for which $\chi_\zeta(g) \neq 0$, Eq.(6.60) implies $\chi_\psi(g) = \chi_\phi(g) f'(g)$. But we know that this equality cannot hold for all group elements, otherwise there exists a G-covariant channel which transform ψ to ϕ, in contradiction with our assumption. This argument shows that the role of a catalyst is specified by the elements of group in which the characteristic function of the catalysts are zero; For this specific group elements even though $\chi_\psi(g) \neq \chi_\phi(g) f'(g)$ but $\chi_\psi(g)\chi_\zeta(g) = \chi_\phi(g)\chi_\zeta(g) f'(g)$. This argument shows that there is an important distinction between the the cases of compact connected Lie groups and finite groups or Lie groups which are not connected.

6.5.1 Compact connected Lie groups

In the case of connected compact Lie groups, using the above argument and by virtue of the analyticity of characteristic functions one can argue that catalysts cannot help, i.e. if a transformation is possible with a catalysts it is also possible without any catalyst. To see this first note that for any finite dimensional representation of compact Lie groups there is a neighborhood around the identity element of group in which the characteristic function of all pure states are nonzero (Otherwise there will be a unitary which is arbitrary close to identity for which $\langle\psi|U|\psi\rangle = 0$ for some state ψ. But in a finite dimensional Hilbert space this is not possible.). This implies that in this neighborhood if Eq.(6.60) holds then the following equation holds

$$\chi_\psi(g) = \chi_\phi(g) f'(g) \tag{6.61}$$

But since all these functions are analytical and since the group G is connected, if the above equality is true for a neighbourhood around the identity element of G then it will be true for all G. Then by theorem 63 we can conclude that there exists a G-covariant

channel which transform ψ to ϕ (without help of any catalyst). So if this transformation is possible with the use of a catalyst then it is also possible without using the catalyst. So to summarize we have proven that

Theorem 64 *For symmetries associated with compact connected Lie groups, there are no examples of nontrivial catalysis using a finite catalyst.*

6.5.2 Finite groups

The above argument clearly does not work in the case of finite groups. Indeed, as we will see in the following it turns out that in the case of finite groups there are representations of symmetry and states for which the characteristic function is zero for all $g \in G$ except the identity. So for these states Eq. (6.60) always holds for all group elements. Therefore, using these states as catalysts one can always transform any state ψ to any arbitrary state ϕ. (Indeed as we show in the following using these states as catalyst one can always transform any mixed state to any other mixed state as well.)

Suppose the the symmetry described by group G is represented by $g \to T_L(g)$ the left regular representation of G on the Hilbert space $\mathcal{H}$ of a system such that

$$\forall g \in G: \quad T_L(g)|h\rangle = |gh\rangle \tag{6.62}$$

where $\{|h\rangle : h \in G\}$ is an orthonormal basis for $\mathcal{H}$. Let $e \in G$ be the identity element of G. Now one can easily see that the characteristic function $|e\rangle$ is the delta function over group G, i.e. the function $\langle e|T_L(g)|e\rangle$ is zero for all elements of G except for the identity element. Also it is straightforward to show that for any pair of states ρ and σ there exists a G-covariant channel which transform $\rho \otimes |e\rangle\langle e|$ to $\sigma \otimes |e\rangle\langle e|$. One realization of this G-covariant map is the following

$$\mathcal{E}(X) = \sum_{g \in G} \mathrm{tr}\left([\mathbb{I} \otimes |g\rangle\langle g|]\, X\right) U(g)\sigma U^\dagger(g) \otimes |g\rangle\langle g| \tag{6.63}$$

where $g \to U(g)$ is the representation of the symmetry on the space where σ lives and $\mathbb{I}$ is the identity operator acting on the Hilbert space which ρ belongs to.

So unlike the case of connected compact Lie groups, in the case symmetries described by finite groups, catalysts can be helpful.

6.6 State to ensemble and stochastic transformations

In this section we study the problem of transforming one pure state to an ensemble of pure states using G-covariant transformations. We are interested to know whether it is possible to transform a given state ψ to the state $\phi_i, i = 1, ..., N$ with probability p_i. The transformation is such that at the end we know i and so we know which ϕ_i is generated.

Theorem 65 *There exists a G-covariant map transforming ψ to $\{p_i, |\phi_i\rangle\}$ if and only if there exists positive definite (and continuous when G is a Lie group) functions $f_i(g)$ for which $f_i(e) = 1$ such that*

$$\chi_\psi(g) = \sum_i p_i f_i(g) \chi_{\phi_i}(g). \tag{6.64}$$

One important special case is when we are interested in just one of the outcome states. In particular we are interested to know whether we can transform state $|\psi\rangle$ to $|\phi\rangle$ with probability p. We call these transformations *stochastic transformations*. The above theorem implies the following corollary about stochastic transformations.

Corollary 66 *There exists a G-covariant map taking ψ to ϕ with probability p iff there exists a positive definite (and continuous when G is a Lie group) function $f(g)$ for which $f(e) = 1$ such that $\chi_\psi(g) - p\chi_\phi(g)f(g)$ is positive definite.*

Example: U(1) covariant stochastic maps

Recall our quantum optics example where the set of all phase shifts forms a representation of group U(1) (see example 48). Let $\text{Irrep}_{\text{U(1)}}(\psi)$ be the set of eigenvalues of the number operator N for which the pure state ψ has nonzero weight in the associated eigenspace. Assuming that ψ can be transformed to ϕ with nonzero probability under a U(1)-covariant operation, one can easily show that

1. The cardinality of $\text{Irrep}_{\text{U(1)}}(\psi)$ is larger than or equal to the cardinality of $\text{Irrep}_{\text{U(1)}}(\phi)$, i.e.,
$$\left|\text{Irrep}_{\text{U(1)}}(\phi)\right| \leq \left|\text{Irrep}_{\text{U(1)}}(\psi)\right| \tag{6.65}$$
2. $$\max\{\text{Irrep}_{\text{U(1)}}(\phi)\} - \min\{\text{Irrep}_{\text{U(1)}}(\phi)\} \leq \max\{\text{Irrep}_{\text{U(1)}}(\psi)\} - \min\{\text{Irrep}_{\text{U(1)}}(\psi)\}$$

Here, we prove item 2 by contradiction. Assume this condition does not hold. Then for any positive definite function $f(\theta)$, $\chi_\phi(\theta)f(\theta)$ has a nonzero component of $e^{im\theta}$ for some m such that $m < n_{\min}(\psi)$ or $m > n_{\max}(\psi)$. Since both $\chi_\phi(\theta)$ and $f(\theta)$ are positive definite the coefficient of $e^{im\theta}$ will be positive. This implies that for any nonzero probability p, the coefficient of $e^{im\theta}$ in $\chi_\psi(\theta) - p\chi_\phi(\theta)f(\theta)$ is negative and so the function $\chi_\psi(\theta) - p\chi_\phi(\theta)f(\theta)$ is not positive definite for any nonzero p. This proves the claim. Item 1 is proven similarly.

Item 2 was obtained by a different argument in Ref. [16] [4]

Example: SO(3) covariant stochastic maps

Let $\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)$ be the set of all angular momentums j corresponding to the different irreps of SO(3) for which the pure ψ has nonzero weight in the associated eigenspaces.

Using a similar argument to the one we used for the case of U(1), one can easily conclude that if ψ can be transformed to ϕ under an SO(3)-covariant channel then

1. the cardinality of $\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)$ is larger than or equal to the cardinality of $\mathrm{Irrep}_{\mathrm{SO}(3)}(\phi)$, i.e.,
$$\left|\mathrm{Irrep}_{\mathrm{SO}(3)}(\phi)\right| \leq \left|\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)\right|. \tag{6.66}$$
2. $$\max\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\phi)\} - \min\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\phi)\} \leq \max\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)\} - \min\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)\}$$
3. $$\max\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\phi)\} \leq \max\{\mathrm{Irrep}_{\mathrm{SO}(3)}(\psi)\} \tag{6.67}$$

The proofs of items 1 and 2 are similar to the case of U(1). To prove item 3 note that the maximum j for which $\chi_\phi(\theta)f(\theta)$ has a nonzero weight in the associated eigenspace, is greater than or equal to $j_{\max}(\phi)$. So if $j_{\max}(\phi)$ is strictly greater than $j_{\max}(\psi)$, then for any nonzero p, $\chi(\psi) - p\chi_\phi(\theta)f(\theta)$ cannot be positive definite.

Item 3 implies that if a pure state does not have any component of angular momentum higher than j then by rotationally covariant operations it cannot be transformed with nonzero probability to another pure state which does have a component of angular momentum higher than j.

We end this section by providing the proof of theorem 65.

[4] The quantity $\mathrm{Irrep}_{\mathrm{U}(1)}(\phi)$ was called the "number spectrum" of ϕ in Ref. [16].

Proof of theorem 65

According to a version of the Stinespring dilation theorem, a general state to ensemble transformation can always be purified in the following way: First, the input system (with Hilbert space $\mathcal{H}_{\text{inp}}$) unitarily interacts with an ancillary system (with Hilbert space $\mathcal{H}_{\text{anc}}$). Now we consider the total Hilbert space $\mathcal{H}_{\text{inp}} \otimes \mathcal{H}_{\text{anc}}$ as

$$\mathcal{H}_{\text{inp}} \otimes \mathcal{H}_{\text{anc}} = \bigoplus_i \mathcal{H}_i \otimes \mathcal{H}'_i \otimes |i\rangle\langle i| \tag{6.68}$$

After the unitary time evolution we perform a projective measurement on the third subsystem in the basis $\{|i\rangle\langle i|\}$ and according to the outcome of measurement we discard the subsystem $\mathcal{H}'_i$ the output would be the system described by $\mathcal{H}_i$. This procedure realizes the most general state to ensemble transformation.

Suppose a transformation maps $|\psi\rangle$ to $|\phi_i\rangle$ with probability p_i. Since the output is pure clearly it cannot be entangled with the discarded system. In other words, after applying the unitary V which couples the system and ancilla the total state should be in the form of

$$V|\psi\rangle|\nu\rangle = \sum_i \sqrt{p_i}|\phi_i\rangle|\eta_i\rangle|i\rangle \tag{6.69}$$

where $|\psi\rangle$ is the initial state of system and $|\nu\rangle$ is the initial state of ancilla.

Now according to an extension of Stinespring's dilation theorem for G-covariant quantum operation, if the state to ensemble transformation is G-covariant then one can choose $|\nu\rangle$ the initial state of ancilla to be G-invariant, the unitary V to be G-invariant unitary and the basis $\{|i\rangle\}$ to be G-invariant [48] .

Assuming V is a G-invariant unitary then the characteristic function of the right hand side should be equal to the characteristic function of $|\psi\rangle|\nu\rangle$. This implies

$$\chi_\psi(g)e^{i\theta(g)} = \sum_i p_i \ \chi_{\nu_i}(g)\chi_{\phi_i}(g)e^{i\alpha_i(g)} \tag{6.70}$$

where $e^{i\theta(g)}$ is the characteristic function of the G-invariant ancilla $|\nu\rangle$ and $\{e^{i\alpha_i(g)}\}$ are the characteristic functions of the G-invariant states $\{|i\rangle\}$. Now because the product of two characteristic functions is also a characteristic function, $\chi_{\nu_i}(g)e^{i\alpha_i(g)}e^{-i\theta(g)}$ is a valid characteristic function. So if there exists a G-covariant transformation which maps state ψ to ϕ_i with probability p_i, then the equation (6.64) should hold. This completes the proof of one direction of the theorem. To prove the other direction, we note that property (1) of characteristic functions implies that there exists a set of states $\{|\nu_i\rangle\}$ which have

characteristic functions equal to $\{f_i\}$. Now we choose $|\nu\rangle$, the initial state of the ancilla, to be a G-invariant state and we assume that its characteristic function is equal to one for all group elements (i.e. any group element maps $|\nu\rangle$ exactly to itself). Similarly we choose a basis $\{|i\rangle\}$ to be a set of G-invariant orthonormal states and assume the characteristic functions of all of them are constant and equal to one. Then, equation (6.64) implies that the characteristic function of $|\psi\rangle|\nu\rangle$ is equal to the characteristic function of $\sum_i \sqrt{p_i}|\phi_i\rangle|\eta_i\rangle|i\rangle$ and so there exists a G-invariant unitary which maps the former state to the latter. Now by performing a measurement in the basis $\{|i\rangle\}$ and discarding the subsystem with the state $|\eta_i\rangle$ we can realize the desired map. This completes the proof of theorem.

6.7 Asymptotic transformations

Here, we present a short summary of an unfinished project about asymmetry of pure states. The goal is to characterize the asymmetry properties of pure quantum states when we are given infinitely many copies of the state. Then, it turns out that to specify the asymmetry properties in this case one requires less information about the state than is contained in its characteristic function.

This problem can be thought of as the analogue of the problem of characterizing entanglement of states in the limit where one has many copies of an entangled state. In the case of bipartite pure entangled states, it is well-known that all the entanglement properties of a state at the limit of many copies can be specified by just a single number, the *entanglement entropy* of the state (See e.g. [15]). More precisely, it can be shown that for any two pure bipartite entangled states many copies of one can be reversibly transformed to many copies of the other by Local Operations and Classical Communications at the rate which is given by the ratio of the entanglement entropy of the two states. Here, we try to find similar results in the asymmetry theory.

We say that there exists an **asymptotic G-covariant** transformation from state ψ to ϕ at rate $R(\psi \to \phi)$ iff $\psi^{\otimes N} \xrightarrow{G-cov} \phi_{M(N)}$ such that

$$\lim_{N\to\infty} \mathrm{Fid}\left(\phi_{M(N)}, \phi^{\otimes M(N)}\right) = 1$$

where $M(N) = \lfloor NR(\psi \to \phi) \rfloor$ and $\mathrm{Fid}(\psi_1, \psi_2)$ is the fidelity between ψ_1 and ψ_2.

We will state the main result without proof [65]

Theorem 67 *If there exists an asymptotic G-covariant transformation from ψ to ϕ at rate $R(\psi \to \phi)$ then*

1. $Sym_G(\psi) \subseteq Sym_G(\phi)$,
2. $R(\psi \to \phi) C_{\mathfrak{g}}(\phi) \leq C_{\mathfrak{g}}(\psi)$ *where* $C_{\mathfrak{g}}(\psi)$ *and* $C_{\mathfrak{g}}(\phi)$ *are respectively the* covariance matrices [5] *of states* ψ *and* ϕ.

We say that there exists a **reversible asymptotic G-covariant** transformation from ψ to ϕ at rate $R(\psi \to \phi)$ if there is an asymptotic G-covariant transformation from ψ to ϕ at rate $R = R(\psi \to \phi)$ and an asymptotic transformation from ϕ to ψ at rate R^{-1}.

Theorem 68 *For a compact connected Lie group G, if there exists a reversible asymptotic G-covariant transformation between ψ and ϕ at rate $R(\psi \to \phi)$ then*

1. $Sym_G(\psi) = Sym_G(\phi)$,
2. $C_{\mathfrak{g}}(\psi) = R(\psi \to \phi) C_{\mathfrak{g}}(\phi)$,
3. $\langle L \rangle_\psi = R(\psi \to \phi) \langle L \rangle_\phi$ *for L any arbitrary element of the commutator subalgebra* $[\mathfrak{g}, \mathfrak{g}]$[6].

We conjecture that these conditions are also sufficient if the group is connected. If this conjecture is true, then at the limit where we are given many copies of a pure state ψ, the asymmetry properties of ψ can be uniquely specified by i) Symmetries of ψ, i.e. $\mathrm{Sym}_G(\psi)$, ii) the covariance matrix of ψ, and iii) the expectation value for ψ of a basis in the commutator subalgebra $[\mathfrak{g}, \mathfrak{g}]$ of the Lie algebra $\mathfrak{g}$.

[5] Let $\{L_k\}$ be a basis for the Lie algebra $\mathfrak{g}$ associated to the compact Lie group G. Then we define the covariance matrix of the state ψ as

$$[C_{\mathfrak{g}}]_{kl}(\psi) \equiv 1/2 \langle \psi | L_k L_l + L_l L_k | \psi \rangle - \langle \psi | L_k | \psi \rangle \langle \psi | L_l | \psi \rangle$$

[6] The *commutator subalgebra* $[\mathfrak{g}, \mathfrak{g}]$ (also known as the derived subalgebra) is the subalgebra spanned by $[L_1, L_2]$ for all $L_1, L_2 \in \mathfrak{g}$.

Conclusion (Part I)

In the first part of this thesis we introduced and studied the notion of asymmetry of states. Our main motivation for this study has been to find the appropriate concepts and framework for a systematic study of the consequences of symmetry of time evolutions for open and closed systems. In particular, we have been interested to find the maximal constraints imposed by the symmetry of time evolution on the final state of a time evolution for a given initial state. Another important motivation comes from the field of quantum metrology where in many cases the parameter to be estimated is an unknown element of a group.

We started by defining the asymmetry of a state ρ relative to the symmetry described by group G as the properties of state ρ which are required to specify the set of all final states which can be reached form ρ via G-covariant time evolutions; we called it the constrained-dynamical approach. We demonstrated that there is another approach for characterizing the asymmetry of a state which does not emphasize G-covariant dynamics-the information-theoretic approach. Here, the asymmetry of a state ρ is specified by the properties of the covariant set $\{\mathcal{U}_g(\rho) : g \in G\}$. We have shown that the two points of views yield the same notion of asymmetry.

The information theoretic point of view to asymmetry implies that some previously known results in the field of information theory have non-trivial implications about the consequences of symmetry of a dynamics. For instance, as we saw in chapter 3, the monotonicity of the Holevo quantity under information processing implies a non-trivial lower bound on the entropy generation in an open system dynamics with symmetry. We also showed that using information monotones one can construct asymmetry monotones, functions which quantify the amount of asymmetry of a state. Any asymmetry monotone puts a restriction on the possible final states of an open system dynamics which has a symmetry, namely, the amount of asymmetry of the final state should be less than or equal to the amount of asymmetry of the initial state.

Also, we observed that in the case of closed system dynamics with symmetry G any

G-asymmetry monotone is a constant of motion. We proved that in the case of pure states the constraints imposed by the conservation of these quantities are not independent of the standard conservation laws implied by Noether's theorem. On the other hand, we proved that in the case of mixed states in a closed system dynamics with symmetry G, the conservation of any non-trivial continuous G-asymmetry monotone give constraints which are independent of the conservation laws implied by Noether's theorem.

As another example of an application of the information theoretic point of view to asymmetry, we used both constrained dynamical and information-theoretic approaches to asymmetry to find two characterizations of unitary G-equivalence classes of pure states: the reduction of the state to the irreps and the characteristic function of the state. We observed that these two characterizations are related to one another by a Fourier transform and that they are in fact two different representations of one object, namely, the reduction of the state to the associative algebra generated by the representation of the group. We focused on the characteristic function as the preferred representation of the reduction of the state to the associative algebra. Furthermore, using the nice mathematical properties of characteristic functions and by virtue of the Stinespring dilation theorem for G-covariant channels (proved in chapter 4) we proved that in the case of connected compact Lie groups two pure states are G-equivalent (i.e. can be transformed to each other via G-covariant channels and so have exactly the same asymmetry properties relative to the group G) iff their characteristic functions are equal up to a 1-dimensional representation of group. Also, making an extra assumption that the characteristic function be non-zero for all group elements, we could extend this result to the case of finite groups as well as all compact Lie groups.

Furthermore, we showed how to use characteristic functions to answer different interesting questions about the manipulation of the asymmetry of pure states. In particular, we identified the conditions for the possibility of a conversion of one pure state to another using G-covariant operations that are deterministic, stochastic or assisted by an asymmetric catalyst. So, in the case of compact Lie groups and finite groups we have been able to answer the basic questions in the resource theory of asymmetry for the case of pure states.

On the other hand, we presented examples which show that the characteristic function of a mixed state ρ, i.e. the function $\chi_\rho(g) = \mathrm{tr}\,(\rho U(g))$ fails to specify the asymmetry properties of the state. The problem is that, roughly speaking, this function cannot see the coherence between different irreps of the group. Furthermore, it cannot see the correlations between the subsystems of the Hilbert space in which the symmetry acts irreducibly and the corresponding multiplicity subsystems in which the symmetry acts trivially. But, both of these factors play important role in specifying the asymmetry of a mixed state.

So, in the case of mixed states the main tools for the study of asymmetry are asymmetry monotones and modes of asymmetry, a notion which we introduced in chapter 5. The idea here is that symmetry of a linear map induces a natural structure on the input and output spaces such that they decompose to different linearly independent modes and an input state which has nonzero component in only a given set of modes can generate output states with nonzero components only in that set of modes. [7]

In the case of G-covariant super-operators the notion of modes can be understood in terms of irreducible tensor operators. More precisely, the subspace spanned by all the irreducible tensor operators which only differ with each other in their multiplicity index defines a mode. Then, one rough characterization of asymmetry of states can be found by specifying the modes of asymmetry in which a given state has nonzero components: If a state does not have a component in a particular mode of asymmetry then under G-covariant transformations it cannot evolve to a state which has nonzero component in that mode of asymmetry, and this holds even in the case of stochastic transformations. We also provided a more refined version of this characterization of asymmetry by introducing asymmetry monotones which quantify the amount of asymmetry in each mode.

The notion of a mode decomposition of states naturally extends to a mode decomposition of measurements and time evolutions. This type of decomposition is particularly useful for answering a problem which has been previously studied using different techniques, i.e. the problem of simulating measurements and time evolutions using symmetric dynamics and a given bounded size quantum reference frame. We showed that the ability of a quantum reference frame to simulate a particular channel or measurement can be determined by specifying its components only in those modes for which the target channel or measurement has a nonzero component. This simple observation provides a powerful insight into the problem.

Future work

There are many open questions left in this field of research. One interesting question is to find the necessary and sufficient conditions for $\rho \xrightarrow{\text{G-cov}} \sigma$, i.e. the necessary and sufficient condition under which there exists a G-covariant dynamics which maps a given state ρ to state σ when these are not assumed to be pure states. From lemma 7 we know that

[7] This is basically why the Fourier analysis is particularly useful for the study of Linear Time Invariant systems. Here, the symmetry of maps is time invariance and different modes correspond to signals with different frequencies.

this question is equivalent to the following question: What is the necessary and sufficient conditions for existence of a channel $\mathcal{E}$ such that $\forall g \in G: \ \mathcal{E}\left(U(g)\rho U^\dagger(g)\right) = U(g)\sigma U^\dagger(g)$? It is likely to be a very difficult problem.

The more general problem of finding the necessary and sufficient conditions for the existence of a channel which transforms an arbitrary given set of states to another set of states has been previously studied, but little progress has been made on this problem. Any progress in that direction will also be a progress in solving the above question about interconversion of states under G-covariant channels.

Another related open problem, which might be slightly easier, is to characterize the asymmetry of mixed states, i.e. to find the necessary and sufficient condition under which for a given pair of states ρ and σ both transformations $\rho \xrightarrow{\text{G-cov}} \sigma$ and $\sigma \xrightarrow{\text{G-cov}} \rho$ are possible. As we mentioned before, in this case the characteristic function of a state cannot specify its asymmetry. Indeed, as we have proven in theorem 15 there does not exist any non-trivial continuous G-asymmetry monotone which can be expressed in terms of the characteristic functions of states. This implies that specifying only the characteristic function of the state does not give any information about the amount of asymmetry of the state.

A simpler open question about mixed states is to find all the consequences of a symmetry of a closed system dynamics in which a mixed state evolves to another mixed state. In other words, to find all the constraints one can put on the final state of a dynamics according to the initial state based on the symmetry of dynamics. To find this, we need to answer the following question: What are the necessary and sufficiency conditions under which a given mixed state ρ can be transformed to another mixed state σ by a G-invariant unitary V such that $\sigma = V\rho V^\dagger$?

Clearly, the equality of the characteristic functions of states, i.e. $\forall g \in G: \ \mathrm{tr}\left(\rho U(g)\right) = \mathrm{tr}\left(\sigma U(g)\right)$ is a necessary but not sufficient condition, as it is shown in the example discussed in section 3.6. So, to find the sufficient condition one may need to consider more complicated functions of states. A reasonable guess for such a generalization could be the equations

$$\forall g_1, g_2 \in G, \forall k_1, k_2 \in \mathbb{N}: \mathrm{tr}\left(\rho^{k_1} U(g_1) \rho^{k_2} U(g_2)\right) = \mathrm{tr}\left(\sigma^{k_1} U(g_1) \sigma^{k_2} U(g_2)\right)$$

But we still do not know if these conditions are actually sufficient or not.

Even in the case of pure states there are still some problems left. For example, in the case of finite groups the criterion we have found for G-equivalence of pure states, given in theorem 61, only works if the characteristic functions of states are nonzero for all group elements. The next natural step here is to relax this extra assumption and find

the necessary and sufficient conditions for the G-equivalence for arbitrary states. Also, proving (or disproving) the sufficiency of the three necessary conditions in theorem 68 for asymptotic reversible transformation between pure states is still an open question.

In the following we list some other directions for future research in this field.

1. **Hidden asymmetry:** In this thesis we have explored some consequences of the information-theoretic point of view to asymmetry. But, there is much more to say about these consequences. For instance, there are many exotic phenomena in quantum information theory that do not have any counterpart in classical information theory and therefore one expects that *quantum asymmetry* may have interesting features not found for *classical asymmetry*. In particular, a symmetry of the quantum dynamics may have consequences which have no counterpart in the case of classical dynamics. A candidate example is based on the quantum phenomenon called *locking of classical information in quantum states* [77]. To see the connection, consider the decomposition of Hilbert space induced by decomposing the representation of the symmetry of dynamics to irreducible representations, i.e.

$$\mathcal{H} = \bigoplus_{\mu} \mathcal{M}_\mu \otimes \mathcal{N}_\mu$$

   Then, the asymmetry of states completely depends on the correlations between the subsystems $\mathcal{M}_\mu$ and $\mathcal{N}_\mu$ for all μ's.

   Now one can easily show that under unitary or non-unitary dynamics which are invariant under the group action, information can never flow from a subsystem associated to a given irreducible representation to its multiplicity subsystem. This implies that, under the restriction to G-covariant dynamics correlations between $\mathcal{M}_\mu$ and $\mathcal{N}_\mu$ can be locked in the same sense that classical information can be locked in quantum states. Combining these ideas we can make an example which could be an example of an asymmetry phenomenon that is genuinely quantum.

2. **Noise in quantum amplifiers:** One interesting question which came out of this study on asymmetry is about the noise in quantum amplifiers. The traditional explanation of the noise generated by quantum amplifiers is based on the commutation relations in quantum mechanics together with the linearity of the equations of motion [76]. But one can also argue that the noise at the output is inevitable because otherwise the distinguishability of states at the output will be higher than the distinguishability of states at the input (which would violate the data processing inequality). This consideration leads to some lower bounds on the minimum noise at

the output. In other words, thinking of the amplifier as an example of information processing can put a bound on the minimum noise. A clear advantage of this approach is that one can find constraints which also hold for nonlinear and stochastic amplifiers.

3. **Applications in the study of non-unitary theories:** By the study of asymmetry we have now different tools for finding the consequences of symmetry in open system dynamics where Noether's theorem cannot be applied. One interesting type of application [8] is to use these tools to find the consequences of symmetry in non-unitary theory modifications of quantum theory which have been proposed as possible solutions to the black hole information loss paradox.

[8] This possible application is proposed by Rafael Sorkin.

Part II

A Generalization of Schur-Weyl duality with applications in quantum estimation

Chapter 7

Preliminaries

In this chapter we introduce the preliminary notions and the notations we use in part II of this thesis.

7.1 Commutant and Centralizer

For a complex vector space $\mathcal{V}$, define $\mathrm{End}(\mathcal{V})$ to be the set of linear maps from $\mathcal{V}$ to itself (endomorphism). This set has a natural structure of algebra and is called the *full matrix algebra* over $\mathcal{V}$. Any matrix algebra defined on $\mathcal{V}$ is a subalgebra of $\mathrm{End}(\mathcal{V})$. Here, we only consider finite dimensional vector spaces.

For any vector space $\mathcal{V}$, and any set $\{A_i \in \mathrm{End}(\mathcal{V})\}$ we call the set of all operators in $\mathrm{End}(\mathcal{V})$ which commute with $\{A_i\}$ the *commutant* of $\{A_i\}$ and denote it by $\mathrm{Comm}\{A_i\}$. Note that for any arbitrary set $\{A_i \in \mathrm{End}(\mathcal{V})\}$, its commutant, i.e. $\mathrm{Comm}\{A_i\}$, is an algebra.

Let $\{A_i \in \mathrm{End}(\mathcal{V})\}$ be a set of Hermitian operators, i.e. $A_i = A_i^\dagger$. Then it holds that

$$\mathrm{Comm}\{\mathrm{Comm}\{A_i\}\} = \mathrm{Alg}\{A_i, \mathbb{I}\} \tag{7.1}$$

where by $\mathrm{Alg}\{A_i, \mathbb{I}\}$ we mean the complex matrix algebra generated by the set $\{A_i\}$ and $\mathbb{I}$ (identity operator on $\mathcal{V}$). Any such complex matrix algebra which includes identity operator and is closed under adjoint ($\dagger$) is called a *finite dimensional von Neumann algebra*. Note that Eq.(7.1) means that for any finite dimensional von Neumann algebra $\mathcal{A}$

$$\mathrm{Comm}\{\mathrm{Comm}\{\mathcal{A}\}\} = \mathcal{A} \tag{7.2}$$

which is the defining property of these algebras. In part II of this thesis we only use this type of algebras and whenever we refer to an object as an algebra we mean a finite dimensional von Neumann algebra. Note that for any subgroup H of the unitary group the algebra spanned by H, $\mathrm{Alg}\{H\}$, is a von Neumann algebra.

A finite dimensional von Neumann algebra, as a finite dimensional matrix C*-algebra, has a unique decomposition up to unitary equivalence of the form

$$\mathcal{A} \cong \bigoplus_J (\mathcal{M}_{m_J} \otimes \mathbb{I}_{n_J}) \tag{7.3}$$

where $\mathcal{M}_{m_J}$ is the full matrix algebra $\mathrm{End}(\mathbb{C}^{m_J})$ and $\mathbb{I}_{n_J}$ is the identity on $\mathbb{C}^{n_J}$. A von Neumann algebra by definition includes identity. Therefore for these algebras $\sum_J m_J n_J$ is equal to the dimension of the vector space.

For two algebras $\mathcal{A}_1 \subseteq \mathrm{End}(\mathcal{V}_1)$ and $\mathcal{A}_2 \subseteq \mathrm{End}(\mathcal{V}_2)$ it holds that

$$\mathrm{Comm}\{\mathcal{A}_1 \otimes \mathcal{A}_2\} = \mathrm{Comm}\{\mathcal{A}_1\} \otimes \mathrm{Comm}\{\mathcal{A}_2\} \tag{7.4}$$

this is called *commutation theorem for tensor products*.

In this thesis we will use the notion of *centralizer* in a different way than *commutant*. By the *centralizer* of a subgroup H_0 in group H we mean the set of all elements of group H which commute with all elements of the subgroup H_0. We denote the centralizer of H_0 by H_0'. Note that the centralizer of any subgroup of a group is also a subgroup of that group.

Let H be a subgroup of $\mathrm{U}(d)$ and H' be its centralizer in this group. Then it holds that

$$\mathrm{Comm}\{H\} = \mathrm{Alg}\{H'\} \tag{7.5}$$

7.1.1 Dual reductive pairs and Schur-Weyl duality

Let H_1,H_2 be two groups of unitaries acting on the complex vector space $\mathcal{V}$ and assume that they commute with each other, that is, H_1 and H_2 are each within one another's centralizer in the group of all unitaries on $\mathcal{V}$. Then, under the action of H_1 and H_2, the space $\mathcal{V}$ decomposes as follows

$$\mathcal{V} \cong \sum_{\mu,\nu} \mathcal{M}_\mu \otimes \mathcal{N}_\nu \otimes \mathbb{C}^{m_{\mu,\nu}} \tag{7.6}$$

where H_1 and H_2 act irreducibly on $\mathcal{M}_\mu$ and $\mathcal{N}_\mu$ respectively, where μ and ν label distinct irreducible representations (irreps) of H_1 and H_2 respectively and where $m_{\mu,\nu}$ is the multiplicity of irreps μ, ν. Then for some specific commuting groups the following equivalent properties hold [13, 66].

Proposition 69 *Let H_1,H_2 be two groups acting on $\mathcal{V}$. Then the following are equivalent*

1. *The complex algebra spanned by H_1 is the commutant of the complex algebra spanned by H_2 in End($\mathcal{V}$) and vice versa.*
2. *In the decomposition 7.6 each $m_{\mu,\nu}$ is either 0 or 1 and at most one $m_{\mu,\nu}$ is nonzero for each μ and each ν.*

Any two groups with these properties are called a dual reductive pair *of subgroups of $GL(\mathcal{V})$ the general linear group on $\mathcal{V}$.*

Note that using the notation we have introduced before the first statement can be written as $\mathrm{Alg}\{H_1\} = \mathrm{Comm}\{H_2\}$ and by virtue of Eq.(7.2) this equation is equivalent to $\mathrm{Alg}\{H_2\} = \mathrm{Comm}\{H_1\}$.

Consider the following representation of the unitary group $\mathrm{U}(d)$ on $(\mathbb{C}^d)^{\otimes n}$:

$$\forall V \in \mathrm{U}(d): \quad \mathbf{Q}(V)|i_1\rangle \otimes \cdots \otimes |i_n\rangle = V|i_1\rangle \otimes \cdots \otimes V|i_n\rangle \tag{7.7}$$

For a subgroup H of $\mathrm{U}(d)$ we denote the group $\{\mathbf{Q}(V) : V \in H\}$ by $\mathbf{Q}(H)$ and we call it the *collective action* of H on $(\mathbb{C}^d)^{\otimes n}$. Consider also the *canonical representation* of the symmetric group of degree n, $\mathcal{S}_n$, on $(\mathbb{C}^d)^{\otimes n}$

$$\forall s \in \mathcal{S}_n: \quad \mathbf{P}(s)|i_1\rangle \otimes \cdots \otimes |i_n\rangle = |i_{s^{-1}(1)}\rangle \otimes \cdots \otimes |i_{s^{-1}(n)}\rangle \tag{7.8}$$

We denote the group $\{\mathbf{P}(s) : s \in \mathcal{S}_n\}$ by $\mathbf{P}(\mathcal{S}_n)$. Then Schur-Weyl duality states that

Theorem 70 *(**Schur-Weyl duality**) The following two algebras are commutants of one another in End($(\mathbb{C}^d)^{\otimes n}$)*

1. *Alg$\{\boldsymbol{Q}(U(d))\}$, the complex algebra spanned by $\boldsymbol{Q}(U(d))$.*
2. *Alg$\{\boldsymbol{P}(\mathcal{S}_n)\}$, the complex algebra spanned by $\boldsymbol{P}(\mathcal{S}_n)$.*

In other words, the subgroups $\boldsymbol{Q}(U(d))$ and $\boldsymbol{P}(\mathcal{S}_n)$ are dual reductive pairs in $GL((\mathbb{C}^d)^{\otimes n})$.

Using our notation, Schur-Weyl duality can be expressed as $\mathrm{Comm}\{\mathbf{Q}(\mathrm{U}(d))\} = \mathrm{Alg}\{\mathbf{P}(\mathcal{S}_n)\}$ or equivalently as $\mathrm{Alg}\{\mathbf{Q}(\mathrm{U}(d))\} = \mathrm{Comm}\{\mathbf{P}(\mathcal{S}_n)\}$.

This theorem together with the proposition 69 implies that there is a one-to-one correspondence between the irreps of the group $\mathrm{U}(d)$ which show up in representation $\mathbf{Q}(\mathrm{U}(d))$ and the irreps of the group $\mathcal{S}_n$ which show up in representation $\mathbf{P}(\mathcal{S}_n)$. Furthermore, the theorem implies that the action of $\mathbf{Q}(\mathrm{U}(d)) \times \mathbf{P}(\mathcal{S}_n)$ is multiplicity-free on $(\mathbb{C}^d)^{\otimes n}$.

In the following section, we present a generalization of Schur-Weyl duality for the case of *gauge* subgroups of U(d).

Chapter 8

A Generalization of Schur-Weyl duality

In this chapter we present a generalization of Schur-Weyl duality which holds for specific subgroups of the unitary group which we call *gauge groups*. We start the chapter by defining and characterizing gauge groups. Then, in section 8.2, based on the notion of gauge groups, we introduce new dual reductive pairs acting on the space $(\mathbb{C}^d)^{\otimes n}$. We show that the standard Schur-Weyl duality is indeed a special case of these new dual reductive pairs.

Then, in section 8.3 we consider the symmetric and anti-symmetric subspaces of $(\mathbb{C}^d)^{\otimes n}$ and will show that a stronger form of the duality holds in this subspaces. The main result of this section, i.e. theorem 76, will be particularly useful in the next chapters where we study applications of these results in estimation theory. This theorem is proven at the end of this chapter.

8.1 Gauge groups and their characterizations

For any subgroup G of $\mathrm{U}(d)$ let G' denote the centralizer of G in $\mathrm{U}(d)$, i.e. the set of all elements of $\mathrm{U}(d)$ which commutes with all elements of G. Also denote the centralizer of the centralizer of G by $G'' \equiv (G')'$. Then in general $G \subseteq G''$. We call a unitary group G a *gauge group* if $G = G''$. The fact that in any arbitrary group and for any arbitrary subgroup H, $H \subseteq H''$ implies that $((H')')' = H'$. So for arbitrary subgroup H of $\mathrm{U}(d)$, its centralizer H' is a gauge group.

Equivalently, one can think of a gauge group as the set of all unitaries in $\mathrm{End}(\mathbb{C}^d)$ which commute with a von Neumann algebra $\mathcal{A} \subseteq \mathrm{End}(\mathbb{C}^d)$. This is true because for any subgroup G of $\mathrm{U}(d)$, G'' is equal to all the unitaries which commute with G' or equivalently all the unitaries which commute with $\mathrm{Alg}\{G'\}$ (which is a von Neumann algebra). So if $G = G''$ then G is equal to the set of all unitaries which commute with an algebra, namely $\mathrm{Alg}\{G'\}$. On the other hand, if G is equal to the set of all unitaries in $\mathrm{End}(\mathbb{C}^d)$ which commute with an algebra $\mathcal{A} \subseteq \mathrm{End}(\mathbb{C}^d)$ then G' is equal to the set of all the unitaries in the algebra $\mathcal{A}$ and so is a basis for this algebra. Since G'' is equal to the set of all the unitaries which commute with G', and G' is a basis for $\mathcal{A}$, then G'' is equal to the set of all unitaries which commute with the algebra $\mathcal{A}$ and so is equal to G. Therefore, these two definitions of gauge group are equivalent.

This discussion implies that one way to specify a gauge group is to specify the von Neumann algebra of operators which commute with the gauge group, for instance by specifying the generators of that algebra. We call the gauge group formed by all unitaries which commute with a von Neumann algebra $\mathcal{A}$ *the gauge group of* $\mathcal{A}$ and denote it by $G_{\mathcal{A}}$. Note that if $G_{\mathcal{A}}$ is the gauge group of $\mathcal{A}$ then it holds that

$$\mathrm{Comm}\{G_{\mathcal{A}}\} = \mathrm{Alg}\{G'_{\mathcal{A}}\} = \mathcal{A}. \tag{8.1}$$

Using this together with commutation theorem for tensor product Eq.(7.4) and Eq.(7.5) we find

$$\mathrm{Comm}\{G_{\mathcal{A}}^{\times n}\} = \mathrm{Alg}\{(G'_{\mathcal{A}})^{\times n}\} = \mathcal{A}^{\otimes n} \tag{8.2}$$

Also note that Eq.(8.1) implies that any von Neumann algebra can be uniquely specified by its gauge group.

Now, based on this observation that any gauge group can be thought as the set of unitaries commuting with a von Neumann algebra, characterizing the set of all gauge groups is equivalent to characterizing all von Neumann algebras which is done by Eq.(7.3). This decomposition implies that $G_{\mathcal{A}}$, the gauge group of $\mathcal{A}$, has a unique decomposition up to unitary equivalence of the form

$$G_{\mathcal{A}} \cong \bigoplus_J (\mathbb{I}_{m_J} \otimes \mathrm{U}(n_J)) \tag{8.3}$$

where $\mathbb{I}_{m_J}$ is the identity on $\mathbb{C}^{m_J}$ and $\sum_J n_J m_J = d$. In other words, for any set of integers $0 \leq n_1 \leq \cdots \leq n_d \leq d$ there is a gauge group acting on $\mathbb{C}^d$ which is isomorphic to $\mathrm{U}(n_1) \times \cdots \times \mathrm{U}(n_d)$ iff there is a set of positive integers $1 \leq m_1, \cdots, m_d \leq d$ such that $\sum_{i=1}^d n_i m_i = d$ (Here, we use the convention that $U(0)$ is the trivial group which

includes only one element.). In particular, for any vector space $\mathbb{C}^d$, there are gauge groups isomorphic to $\mathrm{U}(1)^{\times d}$ and $\mathrm{U}(d)$. These gauge groups can be respectively thought as the gauge group of the algebra of all diagonal matrices in some orthonormal basis and the algebra generated by the identity matrix.

For instance, in the case of $d = 2$ the set of all gauge groups can be classified in the following three types: i) $n_1 = 0, n_2 = 1$ which corresponds to the group $\{e^{i\theta}\mathbb{I} : \theta \in (0, 2\pi]\}$ where $\mathbb{I}$ is the identity operator , ii) $n_1 = 0, n_2 = 2$ which corresponds to the group $\mathrm{U}(2)$ iii) $n_1 = 1, n_2 = 1$ which corresponds to the group

$$\{e^{i\theta_0}|0\rangle\langle 0| + e^{i\theta_1}|1\rangle\langle 1| : \theta_0, \theta_1 \in (0, 2\pi]\}$$

for any arbitrary orthonormal basis $\{|0\rangle, |1\rangle\}$.

Note that this characterization implies that any non-trivial gauge group is a unimodular Lie group, i.e. its left invariant measure is equal to the right invariant measure (up to a constant) and so it has a unique invariant measure.

Throughout the rest of this thesis we will extensively use the uniform twirling over subgroups of unitary group with respect to their unique (normalized) Haar measure. For subgroup H of $\mathrm{U}(d)$ we denote this uniform twirling by

$$\mathcal{T}_H(\cdot) \equiv \int_H d\mu(V)\ V(\cdot)V^\dagger \tag{8.4}$$

where $d\mu$ is the normalized Haar measure of H. Since $d\mu$ is the uniform measure any operator in the image of $\mathcal{T}_H$ commutes with H. Therefore if $G_{\mathcal{A}}$ is the gauge group of a von Neumann algebra $\mathcal{A}$ then the image of $\mathcal{T}_{G_{\mathcal{A}}}$ is inside the algebra $\mathcal{A}$.

Finally, it is worth noting that if G is a gauge group then the two groups G and G' are dual reductive pairs. However, the inverse is not true, i.e. if two groups are dual reductive pairs, they are not necessarily each other's centralizers in the group of all unitaries. For example, according to the Schur-Weyl duality, the canonical representation of the permutation group on $(\mathbb{C}^d)^{\otimes n}$, i.e. $\mathbf{P}(\mathcal{S}_n)$, and the collective action of $\mathrm{U}(d)$, i.e. $\mathbf{Q}(\mathrm{U}(d))$, are dual reductive pairs but they are surely not equal to one another's centralizer in the group of all unitares acting on $(\mathbb{C}^d)^{\otimes n}$.

8.2 From gauge groups to dual reductive pair on product spaces

For a subgroup H of $\mathrm{U}(d)$ we denote $H^{\times n}$ to be the group $H^{\times n} \equiv \{U_1 \otimes \cdots \otimes U_n : U_i \in H\}$. Also, let $\langle H^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ denote the group acting on $(\mathbb{C}^d)^{\otimes n}$ which is generated by the two

groups $H^{\times n}$ and $\mathbf{P}(\mathcal{S}_n) = \{\mathbf{P}(s) : s \in \mathcal{S}_n\}$. Note that every element of $\langle H^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ can be written in the canonical form of $W\mathbf{P}(s)$ for a unique $W \in H^{\times n}$ and a unique $s \in \mathcal{S}_n$. This implies a homomorphism from $\langle H^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ to $\mathbf{P}(\mathcal{S}_n)$ with the kernel $H^{\times n}$, and therefore $\langle H^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle = H^{\times n} \rtimes \mathbf{P}(\mathcal{S}_n)$.

Then one can prove the following generalization of Schur-Weyl duality

Theorem 71 *(**Generalization of Schur-Weyl duality**) Suppose G and G' are one another's centralizers in the group of unitaries $U(d)$. Then the following two algebras are commutants of one another in $End((\mathbb{C}^d)^{\otimes n})$*

1. *$Alg\{\boldsymbol{Q}(G)\}$, the complex algebra spanned by $\boldsymbol{Q}(G)$.*
2. *$Alg\{(G')^{\times n}, \boldsymbol{P}(\mathcal{S}_n)\}$, the complex algebra spanned by $\langle (G')^{\times n}, \boldsymbol{P}(\mathcal{S}_n)\rangle$.*

In other words, the subgroups $\boldsymbol{Q}(G)$ and $\langle (G')^{\times n}, \boldsymbol{P}(\mathcal{S}_n)\rangle$ are dual reductive pairs in $GL((\mathbb{C}^d)^{\otimes n})$.

Using Eq.(8.2) we can rephrase the theorem as

Corollary 72 *Let $G_{\mathcal{A}}$ be the gauge group of the von Neumann algebra $\mathcal{A} \subseteq End(\mathbb{C}^d)$. Then*

$$Comm\{\boldsymbol{Q}(G_{\mathcal{A}})\} = Alg\{\mathcal{A}^{\otimes n}, \boldsymbol{P}(\mathcal{S}_n)\}\,. \tag{8.5}$$

This form of theorem is particularly useful and has a straightforward physical interpretation which will be studied in chapter 12.

Theorem 71 together with the proposition 69 implies that there is a one-to-one correspondence between the irreps of the group G which show up in representation $\mathbf{Q}(G)$ on $(\mathbb{C}^d)^{\otimes n}$ and the irreps of the group $\langle (G')^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ which show up in this space. Furthermore, the theorem implies that the representation of $\mathbf{Q}(G) \times \langle (G')^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ is multiplicity-free on $(\mathbb{C}^d)^{\otimes n}$. Note that in the specific case of $G = \mathrm{U}(d)$ (where G' is the trivial group) this dual reductive pair reduces to the Schur-Weyl duality (see theorem 70).

Also note that the fact that each of the algebras in this theorem is in the commutant of the other algebra is trivial. In other words, for any subgroup $H \subseteq \mathrm{U}(d)$ it holds that

$$\mathrm{Alg}\{\mathbf{Q}(H)\} \subseteq \mathrm{Comm}\{(H')^{\times n}, \mathbf{P}(\mathcal{S}_n)\}$$

The non-trivial content of the theorem is that for gauge groups these two algebras are equal. For H a subgroup of $\mathrm{U}(d)$ that is not equal to its bicommutant in $\mathrm{U}(d)$, and so is

not a gauge group, the above two algebras are not necessarily equal. We provide a simple example illustrating this fact in section 8.2.1.

To prove theorem 71 we use the following property of gauge groups which is proven in section 8.4.

Lemma 73 *For a gauge group G, the complex algebra spanned by $\boldsymbol{Q}(G)$ is equal to the permutationally invariant subalgebra of the complex algebra spanned by $G^{\times n}$.*

The result can be summarized as

$$\begin{aligned} G'' = G \quad \Rightarrow \quad \mathrm{Alg}\{\mathbf{Q}(G)\} &= \mathrm{Alg}\{G^{\times n}\} \ \cap \ \mathrm{Comm}\{\mathbf{P}(\mathcal{S}_n)\} \\ &= \mathrm{Alg}\{G\}^{\otimes n} \ \cap \ \mathrm{Comm}\{\mathbf{P}(\mathcal{S}_n)\}. \end{aligned}$$

Using this lemma the proof of theorem 71 is then straightforward and proceeds as follows.

Proof. (**Theorem** 71) Since both algebras are von Neumann algebras, we only need to show that one is the commutant of the other, the other direction follows from Eq.(7.2). So to prove the theorem it is sufficient to show that $\mathrm{Comm}\{G'^{\times n}, \mathbf{P}(\mathcal{S}_n)\} = \mathrm{Alg}(\mathbf{Q}(G))$. To show this, we note that

$$\mathrm{Comm}\{G'^{\times n}, \mathbf{P}(\mathcal{S}_n)\} = \mathrm{Comm}\{G'^{\times n}\} \ \cap \ \mathrm{Comm}\{\mathbf{P}(\mathcal{S}_n)\}.$$

Then since $\mathrm{Comm}\{G'^{\times n}\} = \mathrm{Alg}\{G^{\times n}\}$ we conclude that

$$\mathrm{Comm}\{G'^{\times n}, \mathbf{P}(\mathcal{S}_n)\} = \mathrm{Alg}\{G^{\times n}\} \ \cap \mathrm{Comm}\{\mathbf{P}(\mathcal{S}_n)\}.$$

This together with lemma 73 completes the proof of theorem. ■

Finally, it is worth mentioning the following corollary of lemma 73 which applies to arbitrary subgroup of $\mathrm{U}(d)$

Corollary 74 *For any unitary subgroup $H \subseteq U(d)$, permutationally invariant subalgebra of $Comm\{H^{\times n}\}$ is equal to $Alg\{\boldsymbol{Q}(H')\}$.*

Proof. First note that Eq.(7.5) together with commutation theorem for tensor products, i.e. Eq.(7.4), implies

$$\mathrm{Comm}\{H^{\times n}\} = \mathrm{Alg}\{(H')^{\times n}\}$$

Then, from section 8.1 we know that the centralizer of H an arbitrary subgroup of $\mathrm{U}(d)$ is a gauge group and so one can apply lemma 73 for gauge group H' which implies that the permutationally invariant subalgebra of $\mathrm{Alg}\{(H')^{\times n}\}$ is equal to $\mathrm{Alg}\{\mathbf{Q}(H')\}$. ■

8.2.1 Global symmetry with respect to non-gauge groups

We demonstrate here that a group that does not have the gauge property does not yield a dual reductive pair in the manner specified by theorems 71. That is, we present an example for a non-gauge group $H \subseteq \mathrm{U}(d)$ for which the commutant of the algebra spanned by $\mathbf{Q}(H)$ in $\mathrm{End}((\mathbb{C}^d)^{\otimes n})$ is larger than the algebra spanned by $\langle (H')^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$. (Recall that for any group $H \subseteq \mathrm{U}(d)$ it always holds that $\mathrm{Alg}\{(H')^{\times n}, \mathbf{P}(\mathcal{S}_n)\} \subseteq \mathrm{Comm}\{\mathbf{Q}(H)\}$).

As a simple example, consider $d = 3$, $n = 2$ where the group H is the $j = 1$ irreducible representation of SU(2) which is a subgroup of U(3). This group is not a gauge group: Schur's lemma implies that $H' = \{e^{i\theta}\mathbb{I}\}$ where $\theta \in (0, 2\pi]$ and $\mathbb{I}$ is identity on $\mathbb{C}^3$ and so $H'' = \mathrm{U}(3) \neq H$.

Since $H' = \{e^{i\theta}\mathbb{I}\}$ then

$$\begin{aligned}\mathrm{Alg}\{(H')^{\times 2}, \mathbf{P}(\mathcal{S}_2)\} &= \mathrm{Alg}\{\mathbf{P}(\mathcal{S}_2)\} \\ &= \{c_+\Pi_+ + c_-\Pi_- : c_\pm \in \mathbb{C}\}\end{aligned}$$

where Π_+ and Π_- are respectively the projectors to the symmetric and anti-symmetric subspace of $(\mathbb{C}^3)^{\otimes 2}$. On the other hand, one can easily see that $\mathrm{Comm}\{\mathbf{Q}(H)\}$, the algebra of operators commuting with $\mathbf{Q}(H)$, is

$$\{c_0 P_{j=0} + c_1 P_{j=1} + c_2 P_{j=2}, c_{0,1,2} \in \mathbb{C}\}$$

where P_j is the projector to the subspace of $(\mathbb{C}^3)^{\otimes 2}$ with total angular momentum j. Therefore the algebra of operators commuting with $\mathbf{Q}(H)$ is larger than $\mathrm{Alg}\{(H')^{\times 2}, \mathbf{P}(\mathcal{S}_2)\}$[1].

8.3 Duality within the symmetric and antisymmetric subspaces

In the special case where the support of operators are restricted to the symmetric or anti-symmetric subspace, theorem 71 has an interesting corollary. Let $\Pi_\pm$ be the projector to $\left[(\mathbb{C}^d)^{\otimes n}\right]_\pm$, the symmetric (respectively antisymmetric) subspace of $(\mathbb{C}^d)^{\otimes n}$. Then we can prove that

[1] One can show that $P_{j=1} = \Pi_-$, in other words in this space any anti-symmetric state has the total angular momentum $j = 1$ and any state with total angular momentum $j = 1$ is anti-symmetric. This implies that $P_{j=0} + P_{j=2} = \Pi_+$.

Theorem 75 *Suppose G and G' are one another's centralizers in the group of unitaries $U(d)$. Then the following two algebras are the commutants of one another in End($\left[(\mathbb{C}^d)^{\otimes n}\right]_\pm$)*

1. *Alg$\{\Pi_\pm \boldsymbol{Q}(G)\Pi_\pm\}$, the complex algebra spanned by $\Pi_\pm \boldsymbol{Q}(G)\Pi_\pm$.*
2. *Alg$\{\Pi_\pm \boldsymbol{Q}(G')\Pi_\pm\}$, the complex algebra spanned by $\Pi_\pm \boldsymbol{Q}(G')\Pi_\pm$.*

In other words, $\Pi_\pm \boldsymbol{Q}(G)\Pi_\pm$ and $\Pi_\pm \boldsymbol{Q}(G')\Pi_\pm$ are dual reductive pairs in GL($\left[(\mathbb{C}^d)^{\otimes n}\right]_\pm$).

Again, the fact that each of these algebras is in the commutant of the other is trivial. The non-trivial fact is that each is *equal* to the commutant of the other. We can summarize the theorem by

$$G'' = G \quad \Longrightarrow \quad \mathrm{Comm}\{\Pi_\pm \mathbf{Q}(G)\Pi_\pm\} = \mathrm{Alg}\{\Pi_\pm \mathbf{Q}(G')\Pi_\pm\}\,. \tag{8.6}$$

where here by Comm$\{\Pi_\pm \mathbf{Q}(G)\Pi_\pm\}$ we mean the set of all operators in End($\left[(\mathbb{C}^d)^{\otimes n}\right]_\pm$) which commute with $\Pi_\pm \mathbf{Q}(G)\Pi_\pm$.

Proof. (**Theorem** 75) Again since both algebras are von Neumann algebra, we only need to show that Comm$\{\Pi_\pm \mathbf{Q}(G')\Pi_\pm\}$ = Alg$\{\Pi_\pm \mathbf{Q}(G)\Pi_\pm\}$. Let M be an arbitrary operator in End$((\mathbb{C}^d)^{\otimes n})$ such that $\Pi_\pm M \Pi_\pm$ commutes with $\Pi_\pm \mathbf{Q}(G')\Pi_\pm$. Then $\Pi_\pm M \Pi_\pm$ clearly commutes with $\mathbf{Q}(G')$ and therefore theorem 71 implies that it is in the span of $\langle G^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$. Now recall that, every arbitrary element of $\langle G^{\times n}, \mathbf{P}(\mathcal{S}_n)\rangle$ can be written in the canonical form of $W\mathbf{P}(s)$ for a unique $W \in G^{\times n}$ and a unique $s \in \mathcal{S}_n$. So

$$\Pi_\pm M \Pi_\pm = \sum_{W\in G^{\times n},\ s\in\mathcal{S}_n} c_{W,s}\ \ W\mathbf{P}(s) \tag{8.7}$$

for some complex coefficients $c_{W,s}$. Then

$$\Pi_\pm M \Pi_\pm = \Pi_\pm \left[\sum_{W\in G^{\times n},\ s\in\mathcal{S}_n} (-1)^{p_\pm(s)}\ c_{W,s}\ \ W\right] \Pi_\pm \tag{8.8}$$

where $\mathbf{P}(s)\Pi_\pm = (-1)^{p_\pm(s)}\Pi_\pm$ for arbitrary $s \in \mathcal{S}_n$, $(-1)^{p_+(s)} = 1$ for all $s \in \mathcal{S}_n$ and $(-1)^{p_-(s)} = \pm 1$ dependent on whether s is an odd or even permutation. Therefore, there exists an operator $\bar{M}$ in the span of $G^{\times n}$ such that $\Pi_\pm \bar{M} \Pi_\pm = \Pi_\pm M \Pi_\pm$. Then

$$\Pi_\pm \left[\sum_{s\in\mathcal{S}_n} \mathbf{P}(s)\bar{M}\mathbf{P}^\dagger(s)\right] \Pi_\pm = \Pi_\pm \bar{M} \Pi_\pm = \Pi_\pm M \Pi_\pm \tag{8.9}$$

where we have used the fact that $\Pi_\pm \mathbf{P}(s) = \mathbf{P}^\dagger(s)\Pi_\pm = (-1)^{p_\pm(s)}\Pi_\pm$ and two negative signs cancel each other. Since $\bar{M}$ is in the span of $G^{\times n}$ then $\tilde{M} \equiv \sum_{s\in\mathcal{S}_n} \mathbf{P}(s)\bar{M}\mathbf{P}^\dagger(s)$ is in the permutationally invariant subalgebra of the span $G^{\times n}$. Now since G is gauge group using lemma 73 we can conclude that $\tilde{M} \in \mathrm{Alg}\{\mathbf{Q}(G)\}$. So for any arbitrary $M \in \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ if $\Pi_\pm M \Pi_\pm$ commutes with $\Pi_\pm \mathbf{Q}(G')\Pi_\pm$ then there exists an operator $\tilde{M}$ in $\mathrm{Alg}\{\mathbf{Q}(G)\}$ such that $\Pi_\pm \tilde{M}\Pi_\pm = \Pi_\pm M \Pi_\pm$. This completes the proof of theorem. ■

Again, using the proposition 69 one can see that theorem 75 implies: (i) a one-to-one correspondence between the irreps of G which show up in the representation $\mathbf{Q}(G)$ in the symmetric (antisymmetric) subspace and the irreps of G' which show up in the representation $\mathbf{Q}(G')$ in the symmetric (antisymmetric) subspace, and (ii) that in these subspaces $\mathbf{Q}(G) \times \mathbf{Q}(G')$ is multiplicity-free. The special case of this result is known in the representation theory for the case of symmetric subspace of $(\mathbb{C}^{d_1 d_2})^{\otimes n}$ and the collective representation of $G = \mathrm{U}(d_1) \times e$ and $G' = e \times \mathrm{U}(d_2)$ as two subgroups of $\mathrm{U}(d_1 d_2)$

Applying theorem 75 for $G_\mathcal{A}$ the gauge group of a von Neumann algebra $\mathcal{A}$ one can show that for any given operator $\Pi_\pm M \Pi_\pm$ which commutes with $\mathbf{Q}(G_\mathcal{A})$ there is an operator $\tilde{M}_\pm$ in the permutationally invariant subalgebra of $\mathcal{A}^{\otimes n}$ such that

$$\Pi_\pm \tilde{M}_\pm \Pi_\pm = \Pi_\pm M \Pi_\pm.$$

However, this argument is not constructive and for a given M it is not clear how we can find such an operator $\tilde{M}_\pm$ with this property. In the following theorem, we introduce a completely positive unital quantum operation which does this transformation.

Theorem 76 *Let $G_\mathcal{A} \subseteq U(d)$ be the gauge group of a von Neumann algebra $\mathcal{A} \subseteq End(\mathbb{C}^d)$. Then there exists a superoperator $\mathcal{L}_\pm$ from $End\left((\mathbb{C}^d)^{\otimes n}\right)$ to itself such that*

1. *$\mathcal{L}_\pm$ is unital and completely positive,*
2. *The image of $\mathcal{L}_\pm$ is in permutationally invariant subalgebra of $\mathcal{A}^{\otimes n}$ and*
3. *if $\Pi_\pm M \Pi_\pm$ commutes with $\boldsymbol{Q}(G_\mathcal{A})$ then*

$$\Pi_\pm \mathcal{L}_\pm(M)\Pi_\pm = \Pi_\pm M \Pi_\pm$$

An instance of such a superoperator is given by

$$\mathcal{L}_\pm(\cdot) \equiv \Phi_\pm(\cdot) + \mathrm{tr}(\cdot)\frac{\mathbb{I}^{\otimes n} - \Phi_\pm(\mathbb{I}^{\otimes n})}{d^n} \tag{8.10}$$

with

$$\Phi_{\pm}(\cdot) \equiv \bigoplus_{\mu} p_{\mu,\pm}^{-1} \; P_{\mu}[\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_{\pm}(\cdot)\Pi_{\pm})]P_{\mu} \tag{8.11}$$

where μ labels all the irreps of $G'_{\mathcal{A}}$ which show up in the representation $\boldsymbol{Q}(G'_{\mathcal{A}})$, P_{μ} is the projector to the subspace of $(\mathbb{C}^d)^{\otimes n}$ associated to irrep μ, $p_{\mu,\pm} \equiv tr\left(P_{\mu}\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_{\pm})\right)$ and the summation in Eq. (8.11) is over all the irreps μ for which p_{μ} is nonzero.

This is proven at the end of this chapter in section 8.4. This theorem will be particularly useful in the rest of this thesis.

8.3.1 Lack of duality outside the symmetric and antisymmetric subspaces

Here, we show that the restriction to the symmetric and anti-symmetric subspaces plays an essential role in theorem 75 and the other results of section 8.3. Recall that theorem 75 implies that for symmetric and anti-symmetric subspaces of $(\mathbb{C}^d)^{\otimes n}$, denoted by $\left[(\mathbb{C}^d)^{\otimes n}\right]_{\pm}$, and for any gauge group $G \subseteq \mathrm{U}(d)$ it holds that

$$\mathrm{Alg}\{\Pi_{\pm}\mathbf{Q}(G')\Pi_{\pm}\} = \mathrm{Comm}\{\Pi_{\pm}\mathbf{Q}(G)\Pi_{\pm}\}$$

Let λ labels different irreps of the permutation group and Π_{λ} be the projector to the subspace $\left[(\mathbb{C}^d)^{\otimes n}\right]_{\lambda}$ of $(\mathbb{C}^d)^{\otimes n}$ in which the representation $\mathbf{P}(\mathcal{S}_n)$ acts like the irrep λ of $\mathcal{S}_n$. The goal is to see whether in theorem 75, or equivalently in the above equation, one can substitute the projection to the symmetric (anti-symmetric) subspace by the projection to an arbitrary irrep λ of $\mathcal{S}_n$.

Clearly for any other irrep λ of $\mathcal{S}_n$ it holds that

$$\mathrm{Alg}\{\Pi_{\lambda}\mathbf{Q}(G')\Pi_{\lambda}\} \subseteq \mathrm{Comm}\{\Pi_{\lambda}\mathbf{Q}(G)\Pi_{\lambda}\}$$

where by $\mathrm{Comm}\{\Pi_{\lambda}\mathbf{Q}(G)\Pi_{\lambda}\}$ we mean the commutant of $\Pi_{\lambda}\mathbf{Q}(G)\Pi_{\lambda}$ in $\mathrm{End}(\left[(\mathbb{C}^d)^{\otimes n}\right]_{\lambda})$.

However, for subspaces other than symmetric and anti-symmetric subspaces, the elements of $\mathrm{Comm}\{\Pi_{\lambda}\mathbf{Q}(G)\Pi_{\lambda}\}$ are not necessarily permutationally invariant while $\mathrm{Alg}\{\Pi_{\lambda}\mathbf{Q}(G')\Pi_{\lambda}\}$ is permutationally invariant. So to generalize theorem 75 to other representations of the permutation group one should make an extra assumption to guarantee that the elements of both sides are permutationally invariant. Then one may expect the following to be true: a natural generalization of theorem 75 will be

$$\mathrm{Alg}\{\Pi_{\lambda}\mathbf{Q}(G')\Pi_{\lambda}\} = \mathrm{Comm}\{\Pi_{\pm}\mathbf{Q}(G)\Pi_{\pm}\} \; \cap \; \mathrm{Comm}\{\Pi_{\lambda}\mathbf{P}(\mathcal{S}_n)\Pi_{\lambda}\}$$

where Π_λ is the projector to the subspace of $(\mathbb{C}^d)^{\otimes n}$ which carries irrep λ of $\mathcal{S}_n$. From theorem 75 we know that for the special case of 1-d representations of $\mathcal{S}_n$, i.e. for symmetric and anti-symmetric subspaces, the above equality hold. Here, we build an explicit counter-example to this equality for other irreps of $\mathcal{S}_n$.

First, notice that the action of $\mathbf{Q}(G)$, $\mathbf{Q}(G')$ and $\mathbf{P}(\mathcal{S}_n)$ on $(\mathbb{C}^d)^{\otimes n}$ all commute with each other. This implies that for irrep λ of $\mathcal{S}_n$ the subspace $\left[(\mathbb{C}^d)^{\otimes n}\right]_\lambda$ can be decomposed as

$$\left[(\mathbb{C}^d)^{\otimes n}\right]_\lambda \cong \left(\bigoplus_{\mu,\nu} \mathcal{M}_\mu \otimes \mathcal{N}_\nu \otimes \mathbb{C}^{m_{\mu,\nu}}\right) \otimes \mathcal{K}_\lambda \tag{8.12}$$

where μ labels irreps of G and ν labels irreps of G' and furthermore $\mathbf{Q}(G)$, $\mathbf{Q}(G')$ and $\mathbf{P}(\mathcal{S}_n)$ act nontrivially only on $\mathcal{M}_\mu$, $\mathcal{N}_\nu$ and $\mathcal{K}_\lambda$ respectively. Note that any permutationally invariant operator should be proportional to identity on the subsystem $\mathcal{K}_\lambda$.

Now to build the counterexample we find two gauge groups G and G' for which there is no one-to-one relation between the irreps of G and G' which show up in $\left[(\mathbb{C}^d)^{\otimes n}\right]_\lambda$. In other words, we find an example in which there is some irrep μ of G for which $m_{\mu,\nu}$ is nonzero for more than one ν (irrep of G'). This in turn will imply that there exist permutationally invariant operators $\Pi_\lambda M \Pi_\lambda$ which commute with $\Pi_\lambda \mathbf{Q}(G) \Pi_\lambda$ but are not block diagonal between $\mathcal{N}_{\nu_1}$ and $\mathcal{N}_{\nu_2}$ for two different irrep ν_1 and ν_2 of G'. This implies that $\Pi_\lambda M \Pi_\lambda$ cannot be in $\text{Alg}\{\Pi_\lambda \mathbf{Q}(G') \Pi_\lambda\}$.

Note that from theorem 75 we know that in the specific case where irrep λ is a 1-d representations of $\mathcal{S}_n$ the conjecture holds. So to find a counter-example we need to look at $n > 2$ where the permutation group can have irreps other than the symmetric and anti-symmetric. In the following, we present a counter-example in the case of $n = 3$. In this case the permutation group $\mathcal{S}_3$ has a two dimensional irrep denoted by λ_2.

Counter-example

Consider the Hilbert space $\mathbb{C}^4 \cong \mathcal{H}_L \otimes \mathcal{H}_R$ where $\mathcal{H}_L$ and $\mathcal{H}_R$ are both isomorphic to $\mathbb{C}^2$. Suppose $G = \{V \otimes I : V \in U(2)\}$, i.e. the group of all unitaries which act trivially on $\mathcal{H}_R$. Clearly G' is the set of all unitaries acting trivially on $\mathcal{H}_L$ and so $G = (G')'$. Note that both G and G' are isomorphic to U(2). So in decomposition 8.12 we can label irreps of G and G' with irreps of U(2).

Using decomposition $(\mathbb{C}^4)^{\otimes 3} \cong \mathcal{H}_L^{\otimes 3} \otimes \mathcal{H}_R^{\otimes 3}$ we can think of the collective representation of G and G' on $(\mathbb{C}^4)^{\otimes 3}$ as

$$V \otimes \mathbb{I}_R \in G \to \mathbf{Q}(V \otimes \mathbb{I}_R) = \mathbf{Q}_L(V) \otimes \mathbb{I}_R^{\otimes 3}$$

and

$$\mathbb{I}_L \otimes V \in G' \to \mathbf{Q}(\mathbb{I}_L \otimes V) = \mathbb{I}_L^{\otimes 3} \otimes \mathbf{Q}_R(V)$$

respectively where $V \to \mathbf{Q}_{L/R}(V) = V^{\otimes 3}$ can be thought as the collective representation of U(2) on $\mathcal{H}_{L/R}^{\otimes 3}$, $\mathbb{I}_{L/R}$ is the identity operator on $\mathcal{H}_{L/R}$ and so $\mathbb{I}_{L/R}^{\otimes 3}$ is the identity operator on $\mathcal{H}_{L/R}^{\otimes 3}$.

Similarly we can think of the canonical representation of $\mathcal{S}_3$ on $(\mathbb{C}^4)^{\otimes 3}$ as

$$\mathbf{P}(s \in \mathcal{S}_3) = \mathbf{P}_L(s) \otimes \mathbf{P}_R(s)$$

where $\mathbf{P}_L(\mathcal{S}_3)$ and $\mathbf{P}_R(\mathcal{S}_3)$ are the canonical representation of $\mathcal{S}_3$ on $\mathcal{H}_L^{\otimes 3}$ and $\mathcal{H}_R^{\otimes 3}$ respectively.

Now according to Schur-Weyl duality there is a one to one relation between the irreps of U(2) which show up in representation $\mathbf{Q}_{L/R}(\mathrm{U}(2))$ on $(\mathcal{H}_{L/R})^{\otimes 3}$ and irreps of $\mathcal{S}_3$ which show up in representation $\mathbf{P}_{L/R}(\mathcal{S}_3)$ on $(\mathcal{H}_{L/R})^{\otimes 3}$. Note that under the action of $\mathcal{S}_3$, $\mathcal{H}_{L/R}^{\otimes 3}$ decomposes as

$$\mathcal{H}_{L/R}^{\otimes 3} \cong \left[\mathcal{H}_{L/R}^{\otimes 3}\right]_+ \oplus \left[\mathcal{H}_{L/R}^{\otimes 3}\right]_{\lambda_2}$$

(the anti-symmetric irrep of $\mathcal{S}_3$ does not exist in this representation.) Now Schur-Weyl duality implies that in the representation $\mathbf{Q}_{L/R}(\mathrm{U}(2))$ of U(2) only one irrep of U(2) shows up in the subspace $\left[\mathcal{H}_{L/R}^{\otimes 3}\right]_+$ and a different one will show up in $\left[\mathcal{H}_{L/R}^{\otimes 3}\right]_{\lambda_2}$.

This implies that there is a one-to-one relation between irreps of U(2) which show up in representation $\mathbf{Q}_L(\mathrm{U}(2)) \otimes I_R$ in the total Hilbert space $(\mathbb{C}^4)^{\otimes 3}$ and irreps of $\mathcal{S}_3$ which show up in the representation $\mathbf{P}_L(\mathcal{S}_3) \otimes I_R$ in the total Hilbert space $(\mathbb{C}^4)^{\otimes 3}$ (though $(\mathbf{P}_L(\mathcal{S}_3) \otimes I_R) \times (\mathbf{Q}_L(\mathrm{U}(2)) \otimes I_R)$ is no longer multiplicity-free). In other words, in representation $\mathbf{Q}_L(\mathrm{U}(2)) \otimes I_R$ only one irrep of U(2) shows up in the subspace

$$\left[\mathcal{H}_L^{\otimes 3}\right]_+ \otimes \left(\left[\mathcal{H}_R^{\otimes 3}\right]_+ \oplus \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}\right)$$

and a different one shows up in

$$\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2} \otimes \left(\left[\mathcal{H}_R^{\otimes 3}\right]_+ \oplus \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}\right)$$

Similarly, under $I_L \otimes \mathbf{Q}_R(\mathrm{U}(2))$ only one irrep of U(2) shows up in the subspace

$$\left(\left[\mathcal{H}_L^{\otimes 3}\right]_+ \oplus \left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2}\right) \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_+$$

and a different one shows up in

$$\left(\left[\mathcal{H}_L^{\otimes 3}\right]_+ \oplus \left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2}\right) \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}$$

Now we find which parts of these subspaces of $(\mathbb{C}^4)^{\otimes 3}$ form $[(\mathbb{C}^4)^{\otimes 3}]_{\lambda_2}$ and we show that in this subspace there is no one-to-one relation between irreps of U(2) which show up in the representation $\mathbf{Q}_L(\mathrm{U}(2)) \otimes I_R$ and irreps of U(2) which show up in the representation $I_L \otimes \mathbf{Q}_R(\mathrm{U}(2))$.

To see this consider the total Hilbert space

$$\begin{aligned}(\mathbb{C}^4)^{\otimes 3} \cong & \\ & \left(\left[\mathcal{H}_L^{\otimes 3}\right]_+ \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_+\right) \\ \oplus & \left(\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2} \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_+\right) \oplus \left(\left[\mathcal{H}_L^{\otimes 3}\right]_+ \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}\right) \\ \oplus & \left(\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2} \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}\right)\end{aligned}$$

and $\mathbf{P}(\mathcal{S}_n)$ the canonical representation of $\mathcal{S}_3$ on it. Then, $\mathbf{P}(s \in \mathcal{S}_n) = \mathbf{P}_L(s) \otimes \mathbf{P}_R(s)$ implies that: i) the subspace in the first line is in the symmetric subspace of $(\mathbb{C}^4)^{\otimes 3}$, i.e. in $[(\mathbb{C}^4)^{\otimes 3}]_+$ (and so we do not care about it), ii) the subspace in the second line is in $[(\mathbb{C}^4)^{\otimes 3}]_{\lambda_2}$ and iii) a nonzero subspace of the subspace in the third line is also in $[(\mathbb{C}^4)^{\otimes 3}]_{\lambda_2}$. To see this we note that the action of $\mathcal{S}_3$ on $\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2} \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}$ is non-commutative and since the only irrep of $\mathcal{S}_3$ in which the representation of $\mathcal{S}_3$ is non-commutative is λ_2, therefore by decomposing the action of $\mathbf{P}(\mathcal{S}_n)$ on $\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2} \otimes \left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}$ to irreps one should find a λ_2 irrep.

This implies that in $[(\mathbb{C}^4)^{\otimes 3}]_{\lambda_2}$, $\left[\mathcal{H}_L^{\otimes 3}\right]_{\lambda_2}$ couples to both $\left[\mathcal{H}_R^{\otimes 3}\right]_+$ and $\left[\mathcal{H}_R^{\otimes 3}\right]_{\lambda_2}$. This in turn will imply that there is no one-to-one relation between the irreps of U(2) which show up in representations $\mathbf{Q}_L(\mathrm{U}(2)) \otimes I_R$ and $I_L \otimes \mathbf{Q}_R(\mathrm{U}(2))$ in the subspace $[(\mathbb{C}^4)^{\otimes 3}]_{\lambda_2}$.

Therefore, this example is a counter-example to the above conjecture.

8.4 Proofs of lemma 73 and theorem 76

Throughout these proofs we use the superoperator $\mathcal{T}_{\mathcal{S}_n} : \mathrm{End}((\mathbb{C}^d)^{\otimes n}) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$

$$\mathcal{T}_{\mathcal{S}_n}(\cdot) \equiv \frac{1}{n!} \sum_{s \in \mathcal{S}_n} \mathbf{P}(s)(\cdot)\mathbf{P}^\dagger(s) \tag{8.13}$$

which maps any operator in $\mathrm{End}((\mathbb{C}^d)^{\otimes n})$ to its symmetrized version (under permutation).

Proof. (**lemma 73**) First note that $\mathrm{Alg}\{\mathbf{Q}(G)\} \subseteq \mathrm{Alg}\{G^{\times n}\}$ and furthermore all elements of $\mathrm{Alg}\{\mathbf{Q}(G)\}$ are permutationally invariant. So $\mathrm{Alg}\{\mathbf{Q}(G)\}$ is included in the permutationally invariant subalgebra of $\mathrm{Alg}\{G^{\times n}\}$. In the following, we prove the converse inclusion.

We prove this by induction. First we prove that for arbitrary $V_0 \in G$, the subspace spanned by $\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes I^{\otimes(n-1)})$ is in $\mathrm{Alg}\{\mathbf{Q}(G)\}$. Then by induction we prove it is true for $\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes \cdots \otimes V_n)$ for arbitrary $V_i \in G : i = 1, \cdots, n$ which proves the claim.

For arbitrary unitary $V_0 \in G$, clearly $V_0 + V_0^\dagger$ and $i(V_0 - V_0^\dagger)$ are both Hermitian operators which commute with G' (the centralizer of G). Therefore, all operators of the form $V_0(\theta, \phi) \equiv \exp\left[i\theta(V_0 + V_0^\dagger) + \phi(V_0 - V_0^\dagger)\right]$, for arbitrary real numbers θ and ϕ are unitary and commute with G'. By virtue of being a gauge group, G includes all unitaries which commute with G', and it therefore follows that $V_0(\theta, \phi) \in G$. We can easily see that

$$\frac{1}{2}\left(\frac{\partial}{\partial\phi} - i\frac{\partial}{\partial\theta}\right)_{|\theta=\phi=0} V_0(\theta, \phi) = V_0 \tag{8.14}$$

This implies that

$$\frac{1}{2}\left(\frac{\partial}{\partial\phi} - i\frac{\partial}{\partial\theta}\right)_{|\theta=\phi=0} V_0^{\otimes n}(\theta, \phi) = \sum_k V_0^{(k)} \tag{8.15}$$

where $V_0^{(k)} \equiv \mathbb{I}^{\otimes(k-1)} \otimes V_0 \otimes \mathbb{I}^{\otimes(n-k)}$. This means that for arbitrary $V_0 \in G$

$$\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes \mathbb{I}^{\otimes(n-1)}) \in \mathrm{Alg}\{\mathbf{Q}(G)\}. \tag{8.16}$$

Next we assume that

$$\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes \cdots \otimes V_{k-1} \otimes \mathbb{I}^{\otimes(n-k)})$$

is in $\mathrm{Alg}\{\mathbf{Q}(G)\}$ for arbitrary $V_i \in G : i = 0, \cdots, k-1$. This together with Eq.(8.16) imply that for arbitrary $V_k \in G$

$$\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes \cdots V_{k-1} \otimes \mathbb{I}^{\otimes(n-k)})\mathcal{T}_{\mathcal{S}_n}(V_k \otimes \mathbb{I}^{\otimes(n-1)})$$

is in $\mathrm{Alg}\{\mathbf{Q}(G)\}$. Expanding this, one can easily see that it can be written as

$$c_1\mathcal{T}_{\mathcal{S}_n}(V_0 \otimes \cdots V_{k-1} \otimes V_k \otimes \mathbb{I}^{\otimes(n-k-1)}) + c_2\mathcal{T}_{\mathcal{S}_n}(U_0 \otimes \cdots U_{k-1} \otimes \mathbb{I}^{\otimes(n-k)})$$

for some nonzero coefficients c_1, c_2 and unitaries $U_i \in G : i = 0, \cdots, k-1$. Now since the sum and the second term each are in the span of $\mathrm{Alg}\{\mathbf{Q}(G)\}$ then we conclude that the

first term is also in $\text{Alg}\{\mathbf{Q}(G)\}$. Note that k and $V_i \in G : i = 0 \cdots k$ are arbitrary. So by induction we have the lemma. ■

Proof. (theorem 76)

Suppose for operator $M \in \text{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ it holds that $\Pi_\pm M \Pi_\pm$ commutes with $\mathbf{Q}(G_\mathcal{A})$, .i.e.

$$\forall V \in G_\mathcal{A} : \Pi_\pm M \Pi_\pm \mathbf{Q}(V) = \mathbf{Q}(V) \Pi_\pm M \Pi_\pm \tag{8.17}$$

Since $V^{\otimes n}$ commutes with $\Pi_\pm$ this implies

$$\Pi_\pm M \Pi_\pm \mathbf{Q}(V) \Pi_\pm = \Pi_\pm \mathbf{Q}(V) \Pi_\pm M \Pi_\pm \tag{8.18}$$

This holds for arbitrary $V \in G_\mathcal{A}$. So we can conclude that for any operator X in $\text{Alg}\{\mathbf{Q}(G_\mathcal{A})\}$ we have

$$\Pi_\pm M \Pi_\pm X \Pi_\pm = \Pi_\pm X \Pi_\pm M \Pi_\pm \tag{8.19}$$

According to lemma 73, $\text{Alg}\{\mathbf{Q}(G_\mathcal{A})\}$ is equal to the span of the permutationally invariant subspace of $G_\mathcal{A}^{\times n}$. Consider $V_1 \otimes \cdots \otimes V_n$ an arbitrary element of $G_\mathcal{A}^{\times n}$. Since $\mathcal{T}_{\mathcal{S}_n}(V_1 \otimes \cdots \otimes V_n)$ is in the permutationally invariant subspace of the span of $G_\mathcal{A}^{\times n}$, it satisfies Eq.(8.19) and so

$$\Pi_\pm M \Pi_\pm \left[\mathcal{T}_{\mathcal{S}_n}(V_1 \otimes \cdots \otimes V_n)\right] \Pi_\pm = \Pi_\pm \left[\mathcal{T}_{\mathcal{S}_n}(V_1 \otimes \cdots \otimes V_n)\right] \Pi_\pm M \Pi_\pm \tag{8.20}$$

For arbitrary permutation $s \in \mathcal{S}_n$, $\mathbf{P}(s)\Pi_\pm = \Pi_\pm \mathbf{P}(s) = \eta \Pi_\pm$ for some $\eta \in \{\pm 1\}$. Therefore Eq.(8.20) implies

$$\Pi_\pm M \Pi_\pm \left[V_1 \otimes \cdots \otimes V_n\right] \Pi_\pm = \Pi_\pm \left[V_1 \otimes \cdots \otimes V_n\right] \Pi_\pm M \Pi_\pm$$

We multiply by $[V_1^\dagger \otimes \cdots \otimes V_n^\dagger]\Pi_\pm$ on the right on both sides of the above equality to obtain

$$\begin{aligned} &\Pi_\pm M \Pi_\pm \left[(V_1 \otimes \cdots \otimes V_n)\Pi_\pm (V_1^\dagger \otimes \cdots \otimes V_n^\dagger)\right] \Pi_\pm \\ &\quad = \Pi_\pm \left[(V_1 \otimes \cdots \otimes V_n)\Pi_\pm M \Pi_\pm (V_1^\dagger \otimes \cdots \otimes V_n^\dagger)\right] \Pi_\pm \end{aligned}$$

Now suppose on both sides we integrate over all elements of $G_\mathcal{A}^{\times n}$ using the Haar measure. Then the above equality implies

$$\Pi_\pm M \Pi_\pm [\mathcal{T}_{G_\mathcal{A}}^{\otimes n}(\Pi_\pm)] \Pi_\pm = \Pi_\pm \mathcal{T}_{G_\mathcal{A}}^{\otimes n}(\Pi_\pm M \Pi_\pm) \Pi_\pm \tag{8.21}$$

Now we demonstrate how one can write $\Pi_\pm M \Pi_\pm$ as $\Pi_\pm \mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm M \Pi_\pm)\Pi_\pm$ times the inverse of $\Pi_\pm[\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)]\Pi_\pm$.

Consider $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ and $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm M \Pi_\pm)$ on the left and right hand sides of the above equality. First of all, since $\Pi_\pm$ and $\Pi_\pm M \Pi_\pm$ are both permutationally invariant then both $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ and $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm M \Pi_\pm)$ are permutationally invariant. Furthermore, since these two operators also commute with $G^{\times n}$ then corollary 74 implies that they are both in $\mathrm{Alg}\{\mathbf{Q}(G'_\mathcal{A})\}$. Second, since $\Pi_\pm$ commutes with $\mathbf{Q}(G'_\mathcal{A})$ in the case of $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ we have another symmetry: $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ commutes with $\mathbf{Q}(G'_\mathcal{A})$. Considering this fact together with the fact that $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ is in $\mathrm{Alg}\{\mathbf{Q}(G'_\mathcal{A})\}$ we conclude that $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm)$ should have the following form

$$\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm) = \bigoplus_\mu p_{\mu,\pm}\ P_\mu \tag{8.22}$$

where μ labels all the irreps of $G'_\mathcal{A}$ which shows up in the representation $\mathbf{Q}(G'_\mathcal{A})$ and P_μ is the projector to these irreps and by virtue of $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}$ being a completely positive map, all $p_{\mu,\pm}$'s are non-negative. Let $\Gamma_\pm$ be the set of all irreps of $G'_\mathcal{A}$ for which $p_\mu, \pm$ is nonzero. So we can write Eq.(8.21) as

$$\Pi_\pm M \Pi_\pm \left(\bigoplus_{\mu\in\Gamma_\pm} p_{\mu,\pm}\ P_\mu \right) \Pi_\pm = \Pi_\pm \left[\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm M \Pi_\pm)\right] \Pi_\pm \tag{8.23}$$

Now consider the inverse of $\mathcal{T}_{G'_\mathcal{A}}^{\otimes n}(\Pi_\pm) = \bigoplus_{\mu\in\Gamma_\pm}(p_{\mu,\pm}P_\mu)$ on its support, i.e., the operator

$$\bigoplus_{\mu\in\Gamma_\pm} p_{\mu,\pm}^{-1}\ P_\mu$$

By multiplying both sides of Eq.(8.23) on the right with this operator and using the facts that

1. $\Pi_\pm$ commutes with $\mathbf{Q}(G'_\mathcal{A})$ and so it commutes with all P_μ's,
2. $$\Pi_\pm \left(\bigoplus_{\mu\in\Gamma_\pm} P_\mu \right) = \left(\bigoplus_{\mu\in\Gamma_\pm} P_\mu \right) \Pi_\pm = \Pi_\pm \tag{8.24}$$
   which is true because all P_μ's commute with $\Pi_\pm$ and Eq.(8.22) implies that the support of $\Pi_\pm$ is a subspace of the support of $\bigoplus_{\mu\in\Gamma_\pm} P_\mu$ and

3. $\forall \mu:\ P_\mu \mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm M \Pi_\pm) = \mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm M \Pi_\pm) P_\mu$, which is true because $\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm M \Pi_\pm)$ is in the span of $\mathbf{Q}(G'_{\mathcal{A}})$

we get

$$\Pi_\pm M \Pi_\pm = \Pi_\pm \left(\bigoplus_{\mu \in \Gamma_\pm} p_{\mu,\pm}^{-1}\ P_\mu \left[\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm M \Pi_\pm) \right] P_\mu \right) \Pi_\pm \tag{8.25}$$

Therefore, defining $\Phi_\pm$ as

$$\Phi_\pm(\cdot) \equiv \bigoplus_{\mu \in \Gamma_\pm} p_{\mu,\pm}^{-1}\ P_\mu [\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm(\cdot)\Pi_\pm)] P_\mu \tag{8.26}$$

we infer that

$$\Pi_\pm M \Pi_\pm = \Pi_\pm \Phi_\pm(M) \Pi_\pm \tag{8.27}$$

Because all P_μ's and $\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}(\Pi_\pm(\cdot)\Pi_\pm)$ are in $\mathrm{Alg}\{\mathbf{Q}(G'_{\mathcal{A}})\}$, the image of $\Phi_\pm$ is as well. Note that since $G'_{\mathcal{A}} \subset \mathcal{A}$ this means that the image of $\Phi_\pm$ is in the permutationally invariant subalgebra of $\mathcal{A}^{\otimes n}$. Now defining $\mathcal{L}_\pm$ in terms of $\Phi_\pm$ via

$$\mathcal{L}_\pm(\cdot) \equiv \Phi_\pm(\cdot) + \left[\mathbb{I}^{\otimes n} - \Phi_\pm(\mathbb{I}^{\otimes n}) \right] \mathrm{tr}(\cdot)/d^n$$

we can infer the same properties for $\mathcal{L}_\pm$. First note that

$$\Phi_\pm(\mathbb{I}^{\otimes n}) = \bigoplus_{\mu \in \Gamma_\pm} P_\mu$$

which together with Eq.(8.24) implies that $\Pi_\pm[\mathbb{I}^{\otimes n} - \Phi_\pm(\mathbb{I}^{\otimes n})]\Pi_\pm = 0$. This together with Eq.(8.27) and definition of $\mathcal{L}_\pm$ implies

$$\Pi_\pm M \Pi_\pm = \Pi_\pm \mathcal{L}_\pm(M) \Pi_\pm\,, \tag{8.28}$$

which is the third claim of theorem 76. Furthermore since the image of $\Phi_\pm$ is in the permutationally invariant subalgebra of $\mathcal{A}^{\otimes n}$ and since $\mathcal{A}$, being a von-Neumann algebra, includes identity, it follows that $\mathbb{I}^{\otimes n} - \Phi_\pm(\mathbb{I}^{\otimes n})$ is in the permutationally invariant subalgebra of $\mathcal{A}^{\otimes n}$. This implies that the image of $\mathcal{L}_\pm(\cdot)$ is in this subalgebra, which is the second claim of theorem 76.

Furthermore, noting that $\mathcal{T}_{G'_{\mathcal{A}}}^{\otimes n}$ is completely positive and the $p_{\mu,\pm}^{-1}$'s are all positive numbers we can conclude that $\Phi_\pm$ as a combination of completely positive maps is completely positive. This together with the fact that $\mathbb{I}^{\otimes n} - \Phi_\pm(\mathbb{I}^{\otimes n})$ is a projector (and so a positive operator) implies that $\mathcal{L}_\pm$ is completely positive. Finally, it is straightforward to verify that $\mathcal{L}_\pm(\mathbb{I}^{\otimes n}) = \mathbb{I}^{\otimes n}$, so that it is unital which proves the first claim of theorem 76. ■

Chapter 9

General applications in Quantum Information

Schur-Weyl duality has many applications in quantum information theory and so we expect that this generalization will as well. Here we present two specific important examples of these applications. The first example is about finding noiseless subsystems for collective noise associated with a gauge group, and the second is about how, for n copies of a system in a pure state confined to the symmetric or antisymmetric subspace, a measurement with *global symmetry* relative to a gauge group can be simulated by one that has *local symmetry* for that group. This second result is the seed of the next chapter, where we will consider the consequences for multi-copy estimation problems in more depth.

9.1 Characterizing the multi-partite operators that are globally symmetric

Many applications of Schur-Weyl duality in quantum information theory are based on the fact that it provides a simple characterization of all operators in $\mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ which commute with $\mathbf{Q}(\mathrm{U}(d))$ or conversely all operators in $\mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ which commute with $\mathbf{P}(\mathcal{S}_n)$.

Theorem 71 and its corollary 72 immediately yield a characterization of operators with global symmetry under a gauge group G, i.e. the operators in $\mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ which commutes with $\mathbf{Q}(G)$ – they lie in the span of the local action of G', i.e. $G'^{\times n}$, and the action of the permutation group, i.e. $\mathbf{P}(\mathcal{S}_n)$. Similarly, corollary 75 yields a characterization of

operators confined to the symmetric and antisymmetric subspaces that have global symmetry under G. These are simply the operators in the span of the collective action of G'.

A straightforward application of this characterization is to find noiseless subsystems. In the following we present a simple example of this.

9.1.1 Example: Finding noiseless subsystems

We begin by reviewing the standard story about noiseless subsystems. Suppose one is going to send quantum information through a noisy qubit channel, where the noise is described by a unitary that is sampled at random, but wherein the same unitary acts on each qubit. For example, the qubits could be spin-half particles with a nonzero magnetic moment and the noise could be due to a random magnetic field. As another example, the qubits could be realized as the polarization of photons sent through a fiber-optic cable and the noise could be due to random strains in the cable that induce changes in the polarization. In many cases, it is a good approximation to assume that the noise varies slowly compared to the interval between the qubits as they pass down the channel (or that it varies little on the distance scale between the qubits in the case of a quantum memory), in which case one can assume that the same random unitary is applied to all n qubits. Then it turns out that, due to the symmetry of the noise, it is possible to encode classical and quantum information in the n qubit system in such a way that it remains unaffected by the noise [68, 69, 70, 71, 72]. To see this, note that under these assumptions, the noise is described by the group $\mathbf{Q}(\mathrm{U}(2))$. Any state in the commutant of $\mathbf{Q}(\mathrm{U}(2))$ is invariant under the noise. Furthermore, any state in the span of $\mathbf{P}(\mathcal{S}_n)$ has this property as well. Now using Schur-Weyl duality one can conclude that the span of $\mathbf{P}(\mathcal{S}_n)$ is equal to the commutant of $\mathbf{Q}(\mathrm{U}(2))$ and therefore *every* state which is unaffected by this type of noise is in the span of $\mathbf{P}(\mathcal{S}_n)$.

In a more general model, the system sent through the channel may have other degrees of freedom which can potentially be used to send quantum information. In other words, the Hilbert space describing each particle sent through the channel is not $\mathbb{C}^2$ but it is $\mathbb{C}^2 \otimes \mathcal{H}$ where the finite dimensional Hilbert space $\mathcal{H}$ describes another degree of freedom which is invariant under the noise in the channel. For example, in the case of photons one can use time-bin encoding in addition to the polarization encoding to encode an extra qubit in each photon. But the time-bin qubit does not suffer from depolarization or polarization mode-dispersion. In other words, this degree of freedom is invariant under polarization noise.

So we assume the noise in the channel is described by a random unitary in the form of $V \otimes \mathbb{I}_{\mathcal{H}}$ where $V \in \mathrm{U}(2)$ and it acts on $\mathbb{C}^2$ and $\mathbb{I}_{\mathcal{H}}$ is the identity operator acting on $\mathcal{H}$. In the case of a single system sent through the channel ($n = 1$), it is clear that any information encoded in the subsystem $\mathcal{H}$ is preserved under this type of noise. Consider the case of many systems sent through the channel ($n > 1$). The question is what are the set of all states of the n systems which are invariant under this type of noise. In other words, what is the set of all states which commute with $\mathbf{Q}(\mathrm{U}(2) \otimes \mathbb{I}_{\mathcal{H}})$? Clearly, in this case, the usual form of Schr-Weyl duality does not apply. But one can use the generalization of Schur-duality we presented in the previous section to find these density operators.

To see this, first note that the group of unitaries $G \equiv \{V \otimes \mathbb{I}_{\mathcal{H}} : V \in \mathrm{U}(2)\}$ is the gauge group of the algebra $\mathbb{I}_2 \otimes \mathrm{End}(\mathcal{H})$ where $\mathbb{I}_2$ is the identity operator on $\mathbb{C}^2$. Then corollary 72 (which is indeed another version of theorem 71) gives the characterization of all operators which commutes with $\mathbf{Q}(G)$: That is basically the set of all operators in $\mathrm{Alg}\{\mathbf{P}(\mathcal{S}_n), (\mathbb{I}_2 \otimes \mathrm{End}(\mathcal{H}))^{\otimes n}\}$. So the set of all density operators in this algebra is exactly the set of all states which remains unaffected under this type of noise. This means that to protect information one needs to encode it in either the invariant degree of freedom of each subsystem ($\mathcal{H}$) or in the permutational degree of freedom. Again note that even without using our results it is straightforward to see that all of these states remains unchanged under this noise. The non-trivial consequence of corollary is that this algebra includes all such density operators.

Note that if the group $H \subseteq \mathrm{U}(d)$ describing the noise is not a gauge group then the $\mathrm{Comm}\{\mathbf{Q}(H)\}$ can be larger than $\mathrm{Alg}\{(H')^{\otimes n}, \mathbf{P}(\mathcal{S}_n)\}$ as it is shown by a simple example in section 8.2.1 (where the group H is the $j = 1$ representation of SU(2) in $\mathbb{C}^3$). This means that, unlike the case of noise described by a gauge group, one can encode quantum information in a space which is larger than the permutational degree of freedom of the systems together with the invariant degrees of freedom of each system.

9.2 Promoting global symmetries to local symmetries

Another important application of this new duality is that in particular cases one can *promote a global symmetry to local symmetry* as we will describe in this section.

For an arbitrary operator $M \in \mathrm{End}(\mathbb{C}^d)^{\otimes n}$ we say that M has *global symmetry* with respect to the subgroup H of $\mathrm{U}(d)$ if it is invariant under the collective action of H, i.e.,

$$\forall V \in H : \; V^{\otimes n} M {V^\dagger}^{\otimes n} = M. \tag{9.1}$$

In other words, M has global symmetry with respect to H iff $M \in \text{Comm}\{\mathbf{Q}(H)\}$. Similarly, we say that M has *local symmetry* with respect to H if it is invariant under the local action of H, i.e.,

$$\forall V \in H \quad \text{and} \quad \forall k : 0 \leq k \leq n-1, \qquad (9.2)$$
$$(I^{\otimes k} \otimes V \otimes I^{\otimes(n-k-1)})M(I^{\otimes k} \otimes V^\dagger \otimes I^{\otimes(n-k-1)}) = M$$

In other words, M has local symmetry with respect to H iff $M \in \text{Comm}(H^{\times n})$.

Note that any operator which has local symmetry with respect to H automatically also has global symmetry with respect to H but the converse implication does not necessarily hold. Indeed, generally the condition of local symmetry is much stronger than that of global symmetry. For example, if H is the group of rotations then global symmetry of a Hamiltonian with respect to H implies that the vector of the total angular momentum of n systems is a constant of the motion in the dynamics generated by this Hamiltonian. However, in this case the angular momenta of the subsystems are not necessarily conserved and the n subsystems can exchange angular momentum with one another. On the other hand, having a Hamiltonian with local symmetry with respect to the group of rotation implies the existence of non-trivial constants of motion defined on each of the n subsystems. So in this case we will have n conserved vectors of angular momentums and under this type of Hamiltonian, subsystems cannot exchange angular momentum.

Now consider the case where the symmetry under consideration is described by a gauge group $G_{\mathcal{A}}$ of a von Neumann algebra $\mathcal{A} \subseteq \text{End}(\mathbb{C}^d)$. Note that if $M \in \text{End}((\mathbb{C}^d)^{\otimes n})$ has global symmetry with respect to $G_{\mathcal{A}}$ then $\Pi_\pm M \Pi_\pm$ will also have global symmetry with respect to $G_{\mathcal{A}}$. Then according to theorem 76 for any operator M with global symmetry with respect to $G_{\mathcal{A}}$ there is an operator $\tilde{M}_\pm$ which has local symmetry with respect to $G_{\mathcal{A}}$ and is equal to M within the symmetric (anti-symmetric) subspace,

$$\Pi_\pm \tilde{M}_\pm \Pi_\pm = \Pi_\pm M \Pi_\pm$$

One can choose $\tilde{M}_\pm = \mathcal{L}_\pm(M)$ where $\mathcal{L}_\pm$ is the completely positive, unital superoperator defined in theorem 76. So using the terminology of local and global symmetry we can interpret theorem 76 as *promoting global symmetry to local symmetry.*

In the following we explore the important consequence of promoting global symmetry to local symmetry for the case of measurements.

9.2.1 Measurements with Global and Local symmetry

The most general type of measurements that can be performed on a quantum system can be described by a POVM (positive operator-valued measure) (See e.g. [21, 10]). Consider

a POVM $M : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$. Here, Ω denotes the space of outcomes of the measurement. This is a measure space equipped with a σ-algebra of subsets, denoted by $\sigma(\Omega)$. The elements of the σ-algebra are subsets of Ω, where $B \subseteq \Omega$ corresponds to the event that the outcome of measurement is an element of B.

We say a POVM $M : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ has global/local symmetry with respect to the group $H \subseteq \mathrm{U}(d)$ if for any $B \in \sigma(\Omega)$, the operator $M(B)$ has global/local symmetry with respect to H, i.e. it satisfies Eq.(9.1) or Eq.(9.2) respectively. Again, typically the local symmetry condition on a measurement is a much more restrictive condition.

Local symmetry of measurements

In the following we first explore the consequences of a measurement having local symmetry and then we see how in the case of gauge symmetries using the generalization of Schur-Weyl duality and in particular theorem 76, one can promote global symmetry of a measurement to a local symmetry (for states whose support is restricted to the symmetric or anti-symmetric subspace). Since the locally symmetric measurements typically are a much smaller class of measurements, this technique will be particularly useful in quantum estimation problems where one seeks to find the measurement that optimizes some figure of merit. Also, this trick is useful for determining whether a given estimation problem requires a nonlocal measurement on the n subsystems (i.e. one that requires a quantum channel or entanglement) or whether a local measurement suffices. More generally, it can set an upper bound on the amount of entanglement required to achieve a particular degree of success in estimation. In the following we explain more about this.

One way to understand the restriction of local symmetry of measurements is via the following observation: Let the subgroup H of $\mathrm{U}(d)$ be a subgroup with unique Haar measure $d\mu$ and consider the twirling superoperator defined in Eq.(8.4). Then local symmetry of POVM $M : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ with respect to H implies that $\mathcal{T}_H^{\otimes n}(M) = M$. This in turn implies that for any event $B \in \sigma(\Omega)$ and for any arbitrary density operator $\rho \in \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ it holds that

$$\begin{aligned}\Pr(B) &= \mathrm{tr}\left(M(B)\rho\right) \\ &= \mathrm{tr}\left(\mathcal{T}_H^{\otimes n}\left(M(B)\right)\rho\right) = \mathrm{tr}\left(M(B)\mathcal{T}_H^{\otimes n}(\rho)\right)\end{aligned}$$

In other words, for any arbitrary state ρ if before measurement M, we apply the local twirling operation $\mathcal{T}_H$, then we do not disturb the statistics of the measurement M. Note that by applying the twirling operation before the measurement, we are mapping the state to $\mathrm{Alg}\{H'\}^{\otimes n}$ which typically can be much smaller than the space of all density operators

in End $\left((\mathbb{C}^d)^{\otimes n}\right)$. Applying this twirling operation decreases the size of the subsystems of the Hilbert space on which the state could be non-trivial and, as we will see later, this fact can set an upper bound on the amount of entanglement required to achieve a particular inference.

This is more clear in the case of gauge groups. Let $G_{\mathcal{A}}$ be the gauge group of a von Neumann algebra $\mathcal{A} \subseteq \text{End}(\mathbb{C}^d)$. Then for any state ρ, the state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ is in $\mathcal{A}^{\otimes n}$. Using the decomposition of the matrix algebra $\mathcal{A}$ given by Eq.(7.3), one can find a simple characterization of the form of state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ for arbitrary ρ.

For instance, consider the Hilbert space $\mathcal{H} = \mathcal{H}_L \otimes \mathcal{H}_R$ where $\mathcal{H}_L$ and $\mathcal{H}_R$ are two finite-dimensional Hilbert spaces. The system of interest decomposed into two subsystems: the left subsystem, described by $\mathcal{H}_L$, and the right subsystem, described by $\mathcal{H}_R$. Let the von Neumann Algebra $\mathcal{A}$ be $\text{End}(\mathcal{H}_L) \otimes \mathbb{I}_{\mathcal{H}_R}$ where $\mathbb{I}_{\mathcal{H}_R} \in \text{End}(\mathcal{H}_R)$ is the identity operator on $\mathcal{H}_R$. As we have seen in the above, for any measurement with local symmetry with respect to the group $G_{\mathcal{A}}$ the statistics of outcomes of the measurement on state ρ is exactly the same as the statistics of the outcomes of that measurement on state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$. But for any state $\rho \in \text{End}\left(\mathcal{H}^{\otimes n}\right)$, it holds that $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho) \in \mathcal{A}^{\otimes n} = \text{End}(\mathcal{H}_L^{\otimes n}) \otimes \mathbb{I}_{\mathcal{H}_R}^{\otimes n}$. In other words, this means that if before a measurement M with local symmetry with respect to $G_{\mathcal{A}}$, we discard all the n right subsystems, we still can simulate the measurement M by performing a measurement on the left subsystems. So, effectively the Hilbert space which is relevant in this problem is $\mathcal{H}_L^{\otimes n}$ which is of a smaller size than the Hilbert space $\mathcal{H}^{\otimes n}$. This clearly put an upper bound on the amount of entanglement required to implement measurement M. We can extend this argument to the case of an arbitrary von Neumann algebra $\mathcal{A}$.

A particularly important case is where $\mathcal{A}$ is a commutative algebra. In this case, for any arbitrary state $\rho \in \text{End}\left((\mathbb{C}^d)^{\otimes n}\right)$, the state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$, as an element of $\mathcal{A}^{\otimes n}$, commutes with all generators of $\mathcal{A}^{\otimes n}$. So, if on each individual qudit we measure an observable (projective von-Neumann measurement) inside the algebra $\mathcal{A}$ we will not change the state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$. But since $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho) \in \mathcal{A}^{\otimes n}$, we can uniquely specify $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ by measuring a set of observables in $\mathcal{A}$ which generates the algebra $\mathcal{A}$ on each individual qudit (note that generators of $\mathcal{A}$ all commute with each other and so can be measured simultaneously). However, after these measurements we know the exact description of state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ and so we can then simulate any other measurement by a post-processing of the data we have gathered in these measurements. Finally, we notice that measuring generators of $\mathcal{A}$ on each individual qudit for state $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ gives exactly the same statistics as measuring these generators on the original state ρ. So we can summarize this discussion as follows.

Proposition 77 *(**Commutative Algebras**) Let $G_{\mathcal{A}}$ be the gauge group of the commutative von Neumann algebra $\mathcal{A} \subseteq$ End$(\mathbb{C}^d)$. Then any measurement on $(\mathbb{C}^d)^{\otimes n}$ which has*

local symmetry with respect to $G_{\mathcal{A}}$ can be realized by measuring a set of observables which generate $\mathcal{A}$ on each qudit individually followed by a classical processing of the outcomes.

Therefore to implement a measurement which has local symmetry with respect to the gauge group $G_{\mathcal{A}}$ of a commutative algebra $\mathcal{A}$ one does not need any entanglement or adaptive measurements.

9.2.2 From Global to Local symmetry

Having studied the consequences of local symmetry for measurements, we now show how the result of previous section and in particular theorem 76 implies that for states whose support is restricted to the symmetric/anti-symmetric subspace, the global symmetry of a measurement with respect to a gauge group can be promoted to a local symmetry.

Corollary 78 *(**Symmetry of Measurements**) Let $G_{\mathcal{A}}$ be the gauge group of a von Neumann algebra $\mathcal{A} \subseteq End(\mathbb{C}^d)$. Then for any POVM $M : \sigma(\Omega) \to End((\mathbb{C}^d)^{\otimes n})$ which has global symmetry with respect to $G_{\mathcal{A}}$ there is a POVM with local symmetry with respect to $G_{\mathcal{A}}$ (i.e. $\tilde{M} : \sigma(\Omega) \to \mathcal{A}^{\otimes n}$) which has exactly the same statistics for all states whose supports are confined to the symmetric (anti-symmetric) subspace. In particular, one can choose $\tilde{M}_{\pm} = \mathcal{L}_{\pm}(M)$ where $\mathcal{L}_{\pm}$ is the superoperator defined in theorem 76.*

Proof. First, recall that if $N : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ is a POVM and $\mathcal{E}$ is a unital, positive quantum operation from $\mathrm{End}((\mathbb{C}^d)^{\otimes n})$ to itself, then $\mathcal{E}(N) : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ is also a POVM. By theorem 76 we know that $\mathcal{L}_{\pm}$ is a unital, completely positive map from $\mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ to itself. So $\tilde{M}_{\pm} \equiv \mathcal{L}_{\pm}(M)$ where $\tilde{M}_{\pm} : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$ is also a POVM. Furthermore, theorem 76 implies that the image of $\mathcal{L}_{\pm}$ has local symmetry with respect to $G_{\mathcal{A}}$ (i.e. it is in $\mathcal{A}^{\otimes n}$). Finally, by definition, if POVM M has global symmetry with respect to $G_{\mathcal{A}}$ then for any $B \in \sigma(\Omega)$, $M(B)$ commutes with $\mathbf{Q}(G_{\mathcal{A}})$. Now since all elements of $\mathbf{Q}(G_{\mathcal{A}})$ are permutationally invariant they are block diagonal in irreps of the permutation group and in particular they commute with $\Pi_{\pm}$. So if $M(B)$ commutes with $\mathbf{Q}(G_{\mathcal{A}})$, then $\Pi_{\pm}M(B)\Pi_{\pm}$ will also commute with $\mathbf{Q}(G_{\mathcal{A}})$. Then using theorem 76 and the definition of $\tilde{M}_{\pm}$ we conclude that for arbitrary event $B \in \sigma(\Omega)$

$$\Pi_{\pm}\tilde{M}_{\pm}(B)\Pi_{\pm} = \Pi_{\pm}M(B)\Pi_{\pm} \tag{9.3}$$

Now consider the probability of event $B \in \sigma(\Omega)$ in the measurement described by POVM $\tilde{M}$ and state $\rho \in \mathrm{End}\left((\mathbb{C}^d)^{\otimes n}\right)$. This probability is given by $\Pr(B) = \mathrm{tr}(\rho\tilde{M}(B))$. Now if

the support of ρ is restricted to the symmetric/anti-symmetric subspace then $\rho = \Pi_\pm \rho \Pi_\pm$ and so

$$\forall \mu : \quad \Pr(B) = \mathrm{tr}(\rho \tilde{M}(B)) = \mathrm{tr}\left(\rho \Pi_\pm \tilde{M}(B) \Pi_\pm\right)$$

Substituting Eq.(9.3) into this we conclude that

$$\begin{aligned} \Pr(B) &= \mathrm{tr}\left(\rho \Pi_\pm \tilde{M}(B) \Pi_\pm\right) \\ &= \mathrm{tr}\left(\rho \Pi_\pm M(B) \Pi_\pm\right) = \mathrm{tr}(\rho M(B)) \end{aligned}$$

But $\mathrm{tr}(\rho M(B))$ is the probability of event B in the measurement described by POVM M performed on state ρ. Therefore measurement $\tilde{M}$ simulates measurement M. ■

Corollary 78 implies that if the support of state ρ is restricted to the symmetric/anti-symmetric subspace then any measurement with global symmetry with respect to $G_{\mathcal{A}}$ on ρ can be simulated by a measurement on $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$. In other words, if one is under the restriction of using measurements which have global symmetry with respect to $G_{\mathcal{A}}$ then by applying the channel $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}$ to a state which is restricted to the symmetric/anti-symmetric subspace one does not loose any information. Note that generally the support of $\mathcal{T}_{G_{\mathcal{A}}}^{\otimes n}(\rho)$ is no longer restricted to the symmetric(anti-symmetric) subspace.

Based on this observation one can put a strong condition on the form of measurements which can be useful, for instance, in finding the optimal measurement in a multi-copy estimation procedure (as we do in the next section). Note that for any given measurement with a global symmetry $G_{\mathcal{A}}$ there are many different other measurements which will have exactly the same statistics on all states whose support are restricted to the symmetric/anti-symmetric subspaces. These measurements may require different amounts of entanglement to be implemented. Finding a measurement with local symmetry with respect to $G_{\mathcal{A}}$ in this set of equivalent measurements has the advantage that one can easily put an upper bound on the amount of entanglement required to realize it. In particular, note that the combination of proposition 77 and corollary 78 implies that if a measurement has global symmetry with respect to $G_{\mathcal{A}}$ the gauge group of a commutative algebra $\mathcal{A}$ then among all possible measurements which can simulate this measurements on states with support in symmetric/anti-symmetric subspace there is one which does not need any entanglement to be realized.

9.2.3 Example

It is useful to consider a concrete example of the simulation of a measurement with global symmetry by one with local symmetry. To this end, consider a pair of qudits with the

total Hilbert space $(\mathbb{C}^d)^{\otimes 2}$ and consider the unitary group of phase shifts $H_d \equiv \{e^{i\phi N} : \phi \in (0, 2\pi]\}$ where $N|i\rangle = i|i\rangle$ and $\{|i\rangle : i = 0 \cdots d-1\}$ is an orthonormal basis for $\mathbb{C}^d$. Note that the unitary group H_d is indeed a representation of U(1) on $\mathbb{C}^d$.

Now one can easily see that a measurement which has global (local) symmetry with respect to H_d has also global (local) symmetry with respect to $\{e^{i\phi_0}e^{i\phi N} : \phi_0, \phi \in (0, 2\pi]\}$ and vice versa. But in the specific case of $d = 2$, the latter group is a gauge group, as we have seen in section 8.1. In the case of $d = 2$ we denote $\{e^{i\phi_0}e^{i\phi N} : \phi_0, \phi \in (0, 2\pi]\}$ by G.

So, in the case of $d = 2$ according to corollary 78, we can infer that for states in the symmetric and antisymmetric subspaces, every measurement with global symmetry with respect to G (or equivalently with respect to H_2) can be simulated with one that has local symmetry with respect to G (or equivalently with respect to H_2).

The measurements that have local symmetry are those for which all the POVM elements are *locally* diagonal in the eigenspaces of N, that is, in the basis $\{|0\rangle, |1\rangle\}$. For a pair of qubits, all such measurements can be realized by a measurement of the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ followed by a classical post-processing of the outcome. Note that measurement in basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ can be realized by measuring observable N individually on each qubit. This is expected from proposition 77 because the algebra of commutants of the gauge group, is the algebra of diagonal matrices in the basis $\{|0\rangle, |1\rangle\}$ which is a commutative algebra.

On the other hand, POVM elements of any measurements that have global symmetry with respect to H_2 (or equivalently with respect to G) are those which commute with total number operator $N \otimes \mathbb{I} + \mathbb{I} \otimes N$ and so are block-diagonal relative to the eigenspaces of $N \otimes \mathbb{I} + \mathbb{I} \otimes N$. For example, for any arbitrary θ the projective measurement in the basis

$$\{|00\rangle, |11\rangle, \cos\theta|01\rangle + \sin\theta|10\rangle, \sin\theta|01\rangle - \cos\theta|10\rangle\}$$

has global symmetry with respect to G. Note that for all the values of θ which are not equal to an integer times $\pi/2$ this measurement would be an entangled measurement.

Let $M : \sigma(\Omega) \to \mathrm{End}\left((\mathbb{C}^2)^{\otimes 2}\right)$ be POVM of an arbitrary measurement on these two qubits which has global symmetry with respect to G. Then, for any arbitrary event $B \in \sigma(\Omega)$, $M(B)$ is block-diagonal relative to the eigenspaces of $N \otimes \mathbb{I} + \mathbb{I} \otimes N$, i.e.

$$P_{00}M(B)P_{00} + P_{11}M(B)P_{11} + [P_{01} + P_{10}]\, M(B)\, [P_{01} + P_{10}] = M(B)$$

where $P_{ij} \equiv |ij\rangle\langle ij|,\ i, j \in \{0, 1\}$. Therefore the probability of event B for arbitrary state ρ is equal to

$$\begin{aligned}\mathrm{tr}\left(M(B)\rho\right) = &\,\mathrm{tr}\left(P_{00}\rho\right)\mathrm{tr}\left(M(B)P_{00}\right) \\ &+ \mathrm{tr}\left(P_{11}\rho\right)\mathrm{tr}(M(B)P_{11}) + \mathrm{tr}\left(\rho\left[P_{01} + P_{10}\right]M(B)\left[P_{01} + P_{10}\right]\right)\end{aligned}$$

Now if the state ρ is promised to be in the symmetric subspace, i.e. $\Pi_+\rho\Pi_+ = \rho$ then

$$\begin{aligned}\mathrm{tr}\left(\rho\left[P_{01}+P_{10}\right]M(B)\left[P_{01}+P_{10}\right]\right) &= \mathrm{tr}\left(\Pi_+\rho\Pi_+\left[P_{01}+P_{10}\right]M(B)\left[P_{01}+P_{10}\right]\right)\\ &= \mathrm{tr}(\rho\left[P_{01}+P_{10}\right])\mathrm{tr}\left(M(B)|\phi^+\rangle\langle\phi^+|\right)\end{aligned}$$

where $|\phi^+\rangle \equiv (1/\sqrt{2})(|01\rangle + |10\rangle)$. In other words,

$$\mathrm{tr}(M(B)\rho) = \Pr(B|00)\mathrm{tr}(P_{00}\rho) + \Pr(B|11)\mathrm{tr}(P_{11}\rho) + \Pr(B|01,10)\mathrm{tr}(\rho\left[P_{01}+P_{10}\right])$$

where

$$\Pr(B|00) \equiv \mathrm{tr}\left(M(B)P_{00}\right), \quad \Pr(B|11) \equiv \mathrm{tr}\left(M(B)P_{11}\right)$$
$$\text{and} \quad \Pr(B|01,10) \equiv \mathrm{tr}\left(M(B)|\phi^+\rangle\langle\phi^+|\right)$$

and they can be interpreted as the conditional probability of event $B \in \sigma(\Omega)$ given each of the four outcomes. This means that to simulate this measurement one can measure N individually on each qubit, i.e. project state of each qubit to $\{|0\rangle, |1\rangle\}$ basis, and based on the outcomes of these measurements choose an outcome $\omega \in \Omega$ consistent with these conditional probabilities.

In other words, although the set of measurements with global symmetry is much larger than the set of measurements with local symmetry, all the information we can extract using a measurement with global symmetry can also be obtained by a measurement with local symmetry. Note that in this example though implementing the measurement with global symmetry may require entanglement, implementing the measurement with local symmetry does not, nor does it require communication among the subsystems. Also, note that from corollary 78 we know that this result holds for any arbitrary number of qubits.

It is worth mentioning that the measurement with local symmetry which we built based on the original measurement is exactly the same measurement as we can get by applying the super-operator $\mathcal{L}_+$ defined in theorem 76 to the POVM of the original measurement.

Finally, based on this example we provide another concrete instance that illustrates how the gauge property of the symmetry group is critical for being able to promote global symmetries to local symmetries. Consider the above example for the case of $d = 3$, i.e. for qu*trits* rather than qubits. In this case, $N|i\rangle = i|i\rangle$ where $\{|i\rangle : i = 0, \cdots, 2\}$. Then, one can easily see that the group $\{e^{i\phi_0}e^{i\phi N} : \phi_0, \phi \in (0, 2\pi]\}$ is no longer a gauge group. So, in general a measurement on two qutrits with global symmetry with respect to this group, cannot be necessarily simulated by a measurement with local symmetry with respect to this group, even under the promise that the state is restricted to the symmetric subspace.

In fact, in this case all the measurements that have local symmetry are those which can be obtained by classical post-processing of a measurement of the product basis $\{|ij\rangle : i, j = 0, 1, 2\}$, while those with global symmetry are merely block-diagonal with respect to the eigenspaces of $N \otimes \mathbb{I} + \mathbb{I} \otimes N$. In particular, a measurement with global symmetry may include the rank-1 projectors onto the vectors $|11\rangle + (|02\rangle + |20\rangle)$ and $|11\rangle - (|02\rangle + |20\rangle)$ which both lie in the symmetric subspace. Such a measurement cannot be simulated by any measurement with local symmetry, which necessarily is unable to detect coherence between $|11\rangle$ and $|02\rangle + |20\rangle$.

Chapter 10

Multi-copy estimation and decision problems

In this chapter we introduce a framework for the study of a family of multi-copy estimation problems, in which one is given several copies of the same qudit state according to some known prior distribution and the goal is to estimate some parameters about that qudit state. The quality of estimation is evaluated with respect to a given figure of merit. Then, we use the result of the previous chapter about promoting the global symmetry of a measurement to the local symmetry to find conditions which guarantee that a measurement with local symmetry can achieve the optimal estimation in a multi-copy estimation problem in this family. We begin by setting up a general framework for such problems.

10.1 General framework for multi-copy estimation problems

Suppose Alice randomly chooses a qudit state ρ from the density operators in $\mathrm{End}(\mathbb{C}^d)$ according to the probability density function p and then prepares n copies of this state and sends them to Bob through a quantum channel $\mathcal{E} : \mathrm{End}((\mathbb{C}^d)^{\otimes n}) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. Bob's goal is to estimate some parameter(s) of state ρ. (We here adopt the convention that the term "estimation problem" includes decision problems as a special case). So upon receiving n systems he performs a measurement and generates some outcome in the outcome space Ω where Ω is a measure space, i.e. a set equipped with a σ-algebra $\sigma(\Omega)$ of subsets. The elements of the σ-algebra are subsets of Ω, where $B \subseteq \Omega$ corresponds to the event that

Bob's measurement outcome is an element of B. The outcome space Ω can be continuous (in the case of general estimation problems) or discrete (in the case of decision problems).

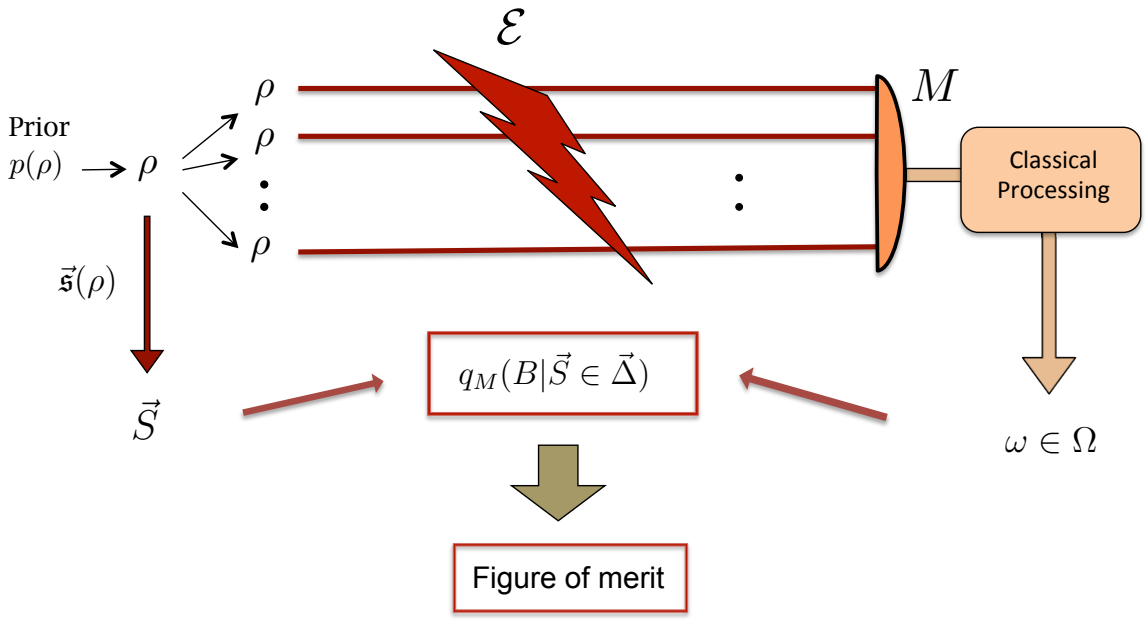

Figure 10.1: Multi-copy estimation problem (see below).

In an arbitrary estimation strategy, Bob measures the n qudits he has received and possibly does some post-processing on the outcome, ultimately generating an output in the set Ω. The entire strategy, which combines the measurement and the data processing, can be described by a POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. For simplicity, we will often refer to the estimation strategy as the measurement.

Therefore, the most general figure of merit which evaluates the performance of different strategies in an estimation problem is a function which assigns real numbers to all POVMs $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. Equivalently, in the case of the multi-copy estimation problems we are considering here, the most general figure of merit can be described as a real functional which acts on the two variable function

$$q_M(B|\rho) = \mathrm{tr}\left(M(B)\mathcal{E}(\rho^{\otimes n})\right) \tag{10.1}$$

the conditional probability that, using the strategy described by POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$, the event $B \in \sigma(\Omega)$ happens given that Alice has chosen the state $\rho \in \mathrm{supp}(p)$

and has sent state $\rho^{\otimes n}$ to Bob through the channel $\mathcal{E}$ (here, $\mathrm{supp}(p)$ denotes the support of the distribution p).

This describes the most general figure of merit one can define for the multi-copy estimation problems we are considering here. However, in the particular cases where for example the goal is to estimate some parameter of ρ, say the expectation value of some observable for state ρ, one might use a figure of merit which only depends on the conditional probability of outcomes for different values of that parameter. Here, we think of the parameter as a random variable defined as a function of the state Alice chooses each time (The state is random and so any function of the state can be thought of as a random variable). Let $\mathfrak{s} : \mathrm{supp}(p) \to \mathbb{R}$ be an arbitrary function from states in $\mathrm{supp}(p)$ to real numbers. Then this function will map the random state ρ chosen by Alice to a random real variable $S = \mathfrak{s}(\rho)$. Then if Bob's goal is to estimate the value of parameter $\mathfrak{s}(\rho)$ for the state ρ which Alice has chosen each time (or to make a decision based on the value of this parameter) a reasonable family of figures of merit to evaluate Bob's performance can be expressed as functionals of

$$q_M(B|S \in \Delta),$$

where Δ is an interval of $\mathbb{R}$. This is the conditional probability that, using the strategy described by POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$, event B happens given that the value of the random variable S is in Δ.

On the other hand, one can imagine the situations where, for example, the cost for wrong estimation of a parameter S not only depends on the estimated value of S and its actual value but also depends on the value of some other parameter, say S', where S' is the random variable induced by the function $\mathfrak{s}' : \mathrm{supp}(p) \to \mathbb{R}$ acting on the random state Alice chooses. For instance, one may imagine situations where the cost of wrong estimation of a parameter S depends also on the energy of state $\mathrm{tr}(\rho H)$ where H is the Hamiltonian. So in this case $\mathfrak{s}'(X) = \mathrm{tr}\,(XH)$ defines a relevant parameter to evaluate the performance of the estimation procedure.

In general, let

$$\vec{\mathfrak{s}}(\cdot) = \left(\mathfrak{s}^{(1)}(\cdot), \cdots, \mathfrak{s}^{(l)}(\cdot)\right)$$

be a set of functions where each $\mathfrak{s}^{(i)}(\cdot)$ is a function from $\mathrm{supp}(p)$ to $\mathbb{R}$. Then based on the set of functions $\vec{\mathfrak{s}}(\cdot) = \left(\mathfrak{s}^{(1)}(\cdot), \cdots, \mathfrak{s}^{(l)}(\cdot)\right)$ we can define a set of random variables $\left(S^{(1)}, \cdots, S^{(l)}\right)$ where the random variable $S^{(i)}$ is $\mathfrak{s}^{(i)}(\rho)$ where ρ is the random state Alice has chosen at each round. So a general figure of merit can be expressed as a functional of

$$q_M(B|\vec{S} \in \vec{\Delta}),$$

where $\vec{\Delta}$ is an l-dimensional interval of $\mathbb{R}^l$. This is the conditional probability that with Bob's strategy described by POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ event B happens given the value of the random variables $\vec{S}$ are in $\vec{\Delta}$.

The other reason to consider $q_M(B|\vec{S} \in \vec{\Delta})$ for more than one parameter $S^{(i)}$ is to study the cases where Bob is interested in estimating more than one parameter of the state.

Note that by having larger number of parameters l we can describe more and more general types of figure of merit. In general, if d is the dimension of $\mathbb{C}^d$ then the set of all (normalized) density operators can be specified by $d^2 - 1$ real parameters. So having $l = d^2 - 1$ real parameters is sufficient to specify the exact density operator Alice has chosen each time, and so $l = d^2 - 1$ parameters are sufficient to describe the most general form of figures of merit one can imagine for this problem. However, generally, having a figure of merit which can be defined using less than $d^2 - 1$ parameters, makes it easier to find the optimal estimation procedure.

To summarize, in the multi-copy estimation problem we are considering here, $q_M(B|\rho)$ has the maximal information required to evaluate the figure of merit of the strategy described by the POVM M. In other words, if for two different strateges described by POVMs $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ and $M' : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ it holds that

$$q_M\left(B|\rho\right) = q_{M'}\left(B|\rho\right) \tag{10.2}$$

for all $B \in \sigma(\Omega)$ and $\rho \in \mathrm{supp}(p)$ then they will have exactly the same performance in the estimation problem with respect to any figure of merit. On the other hand, $q_M(B|\vec{S} \in \vec{\Delta})$ has generally less information, i.e. it can be obtained by a coarse-graining of $q_M\left(B|\rho\right)$ but not necessarily vice versa. However, in many reasonable figures of merit one does not need to specify $q_M\left(B|\rho\right)$ to specify the figure of merit of the measurement M; it is sufficient to specify $q_M(B|\vec{S} \in \vec{\Delta})$. If this is the case, then even if Eq. (10.2) doesn't hold, as long as the weaker constraint

$$q_M\left(B|\vec{S} \in \vec{\Delta}\right) = q_{M'}\left(B|\vec{S} \in \vec{\Delta}\right) \tag{10.3}$$

holds for all $B \in \sigma(\Omega)$ and for all l-dimensional intervals $\vec{\Delta}$ that are assigned nonzero probability, the two strategies yield the same performance for the figure of merit of interest (See Fig. 10.1). Eq. (10.3) states that learning the outcome of measurement M is *precisely as informative about the parameter* $\vec{S}$ as learning the outcome of measurement M'.

An example of common figures of merit, i.e. the average cost function, will be provided in Appendix B.1.

10.2 Main result

Scenario: Suppose that Alice randomly chooses an unknown state ρ from the density operators in $\mathrm{End}(\mathbb{C}^d)$ according to some probability density p (which we call the *single-copy prior*) and send n qudits each prepared in the state ρ to Bob through a quantum channel $\mathcal{E} : \mathrm{End}((\mathbb{C}^d)^{\otimes n}) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. Here, the density p is defined relative to $d\rho$ a reference measure on the space of mixed states which is invariant under unitary transformations.[1]

Suppose that Bob makes measurements on the collection of n systems.

Let parameters $\vec{\mathfrak{s}}(\cdot) = \left(\mathfrak{s}^{(1)}(\cdot), \cdots, \mathfrak{s}^{(l)}(\cdot)\right)$ be an arbitrary set of functions where $\mathfrak{s}^{(i)} : \mathrm{supp}(p) \to \mathbb{R}$, and let $\vec{S}$ be the random variables defined as $\vec{S} \equiv \vec{\mathfrak{s}}(\rho)$ where ρ is the random state Alice chooses. We refer to $\vec{\mathfrak{s}}$ as the *parameters*. We say that the prior p is invariant under a subgroup H of $\mathrm{U}(d)$, or equivalently, *has H as a symmetry* if for all ρ we have

$$\forall V \in H : p(\rho) = p\left(V\rho V^\dagger\right). \tag{10.4}$$

We say that the parameter $\mathfrak{s}$ is invariant under a subgroup H of $\mathrm{U}(d)$, or equivalently, *has H as a symmetry* if for all $\rho \in \mathrm{supp}(p)$, i.e. all ρ assigned non-zero probability by the prior, we have

$$\forall V \in H : \vec{\mathfrak{s}}(\rho) = \vec{\mathfrak{s}}\left(V\rho V^\dagger\right). \tag{10.5}$$

We now present our main results, leaving the proofs to be presented in Sec. 10.3. We begin with a version of the result where the assumptions are particularly simple. These assumptions will be generalized shortly.

Theorem 79 *Let $\mathcal{A} \subseteq End(\mathbb{C}^d)$ be a von Neumann algebra, and let $G_{\mathcal{A}}$ be the gauge group associated with it. Assume that:*

1. *the prior p and the vector of parameters $\vec{\mathfrak{s}}$ have the gauge group $G_{\mathcal{A}}$ as a symmetry;*
2. *the channel $\mathcal{E}$ is the identity channel;*
3. *the prior p has support only on the pure states.*

Then for any given measurement with POVM $M : \sigma(\Omega) \to End((\mathbb{C}^d)^{\otimes n})$, there is another measurement with POVM $M' : \sigma(\Omega) \to End((\mathbb{C}^d)^{\otimes n})$ whose image is entirely confined to $\mathcal{A}^{\otimes n}$ (i.e., $M' : \sigma(\Omega) \to \mathcal{A}^{\otimes n}$), such that M' is as informative about $\vec{S}$ as M is, i.e.,

$$q_M\left(B|\vec{S} \in \vec{\Delta}\right) = q_{M'}\left(B|\vec{S} \in \vec{\Delta}\right) \tag{10.6}$$

[1] For example we can use the measure induced by the Hilbert-Schmidt inner product defined in [73].

for all $B \in \sigma(\Omega)$ and all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability.

Remark 80 *An instance of the measurement described in theorem 79 is $M' \equiv \mathcal{L}_+(M)$, where $\mathcal{L}_+$ is the unital quantum channel defined in Eq. (8.10).*

One can generalize this theorem in two ways: from the identity channel to a class of nontrivial channels, and from a prior that has support only on pure states to a certain class of priors that have support on mixed states. We begin by defining the classes in question.

We define a channel $\mathcal{E}$ to be *noiseless on* $\mathcal{A}^{\otimes n}$ if for all states ρ in $\mathrm{End}((\mathbb{C}^d)^{\otimes n})$, $\mathcal{E}(\rho)$ and ρ have the same reduction on the algebra $\mathcal{A}^{\otimes n}$, i.e.,

$$\forall R \in \mathcal{A}^{\otimes n} : \mathrm{tr}(R\mathcal{E}(\rho)) = \mathrm{tr}(R\rho), \tag{10.7}$$

or equivalently, $\mathcal{T}_{G_\mathcal{A}}^{\otimes n} \circ \mathcal{E} = \mathcal{T}_{G_\mathcal{A}}^{\otimes n}$.

Let prior density $\tilde{p}$ be one with support confined to the pure states. Define a prior density p to be a *$G_\mathcal{A}$-distortion* of $\tilde{p}$ via channel $\mathcal{N}$ if it can be realized by sampling a pure state from $\tilde{p}$ and then applying a quantum channel $\mathcal{N} : \mathrm{End}(\mathbb{C}^d) \to \mathrm{End}(\mathbb{C}^d)$ to the state, where $\mathcal{N}$ is noiseless on $\mathcal{A}$ and is also $G_\mathcal{A}$-covariant i.e. $\forall V \in G_\mathcal{A} : \ \mathcal{N}(\cdot) = \mathcal{N}(V \cdot V^\dagger)$. (Recall that all these densities are defined relative to a fixed unitary invariant measure.) We then have the following generalization of the theorem 79.

Theorem 81 *(Generalization of theorem 79) the implication in theorem 79 still holds if one weakens assumptions 2 and 3 to:*
2′. the channel $\mathcal{E}$ is noiseless on $\mathcal{A}^{\otimes n}$;
3′. the prior p is a $G_\mathcal{A}$-distortion of one that has support only on the pure states.

Remark 82 *Assume the prior p is a $G_\mathcal{A}$-distortion of a prior over pure states via channel $\mathcal{N}$. Then, an instance of the measurement described in theorem 81 is $M' \equiv \mathcal{L}_+ \circ (\mathcal{N}^\dagger)^{\otimes n} \circ \mathcal{E}^\dagger(M)$, where $\mathcal{L}_+$ is the unital quantum channel defined in Eq. (8.10).*

We now make explicit what our main theorem implies for multi-copy estimation problems.

Corollary 83 *If the figure of merit for a strategy M in the n-copy estimation problem can be expressed as a functional of $q_M(B|\vec{S} \in \vec{\Delta})$ for some set of parameters $\vec{\mathfrak{s}}$, then if the assumptions of the theorem 81 (or theorem 79) hold for a von Neumann algebra $\mathcal{A}$, it follows that the POVM elements of the optimal measurement can be chosen to be in $\mathcal{A}^{\otimes n}$.*

Corollary 83 implies that the optimal measurement has the gauge group $\mathrm{G}_{\mathcal{A}}$ as a local symmetry. Then, in the special case wherein the algebra $\mathcal{A}$ is commutative, by proposition 77, it follows that it can be implemented by measuring a set of observables which generates $\mathcal{A}$ separately on each of the n qudits and then performing a classical processing on the outcomes.

To apply corollary 83, the figure of merit for an estimation strategy M must be a functional of the conditional $q_M(B|\vec{S} \in \vec{\Delta})$. In appendix B.1, we demonstrate in an example how a common figure of merit, i.e. the expected cost for an arbitrary cost function, can be written in this form.

10.2.1 The reduction of the state to the algebra

We here describe an alternative way to state assumption 1 of theorem 79 in the case where the prior p has support only on pure states.

We begin with a definition. We say that a function g from states in $\mathrm{End}(\mathbb{C}^d)$ to $\mathbb{R}$ *depends only on the reduction of the state to the algebra* $\mathcal{A}$ if it can be expressed as

$$g(\rho) = f\left(\mathrm{tr}(\rho\tilde{A}_1), \cdots, \mathrm{tr}(\rho\tilde{A}_D)\right)$$

for some function $f : \mathbb{C}^D \to \mathbb{R}$, where $\{\tilde{A}_1, \cdots, \tilde{A}_D\} \subset \mathcal{A}$ is a basis for $\mathcal{A}$.

In terms of this notion, the alternative statement of assumption 1 is:

1′. *The prior p and the vector of parameters $\vec{\mathfrak{s}}$ depend only on the reduction of the state to the algebra $\mathcal{A}$.*

The fact that assumption 1′ implies assumption 1 is clear: If $V \in G_{\mathcal{A}}$ then $\mathrm{tr}(\rho V^\dagger A V) = \mathrm{tr}(\rho A)$ for arbitrary density operator ρ in $\mathrm{End}(\mathbb{C}^d)$ and arbitrary $A \in \mathcal{A}$. Then since according to assumption 1′, p and $\vec{\mathfrak{s}}$ can be expressed as a function of $\left(\mathrm{tr}(\rho\tilde{A}_1), \cdots, \mathrm{tr}(\rho\tilde{A}_D)\right)$ we conclude that $p(V\rho V^\dagger) = p(\rho)$ and $\vec{\mathfrak{s}}(V\rho V^\dagger) = \vec{\mathfrak{s}}(\rho)$ for arbitrary ρ and arbitrary $V \in G_{\mathcal{A}}$.

The fact that assumption 1 implies assumption 1′ is true because of the following: Consider an arbitrary pair of pure states $|\psi_1\rangle$ and $|\psi_2\rangle$ in the support of p. If for this pair of states there exists a unitary $V \in G_{\mathcal{A}}$ such that $V|\psi_1\rangle = |\psi_2\rangle$ then assumption 1 implies that

$$\vec{\mathfrak{s}}(|\psi_2\rangle\langle\psi_2|) = \vec{\mathfrak{s}}\left(V|\psi_1\rangle\langle\psi_1|V^\dagger\right) = \vec{\mathfrak{s}}\left(|\psi_1\rangle\langle\psi_1|\right)$$

On the other hand, if there does not exist a unitary $V \in G_{\mathcal{A}}$ such that $V|\psi_1\rangle = |\psi_2\rangle$ then $\vec{\mathfrak{s}}(|\psi_2\rangle\langle\psi_2|)$ could be different from $\vec{\mathfrak{s}}(|\psi_1\rangle\langle\psi_1|)$. In other words, to specify the value

of $\vec{\mathfrak{s}}$ for a particular state $|\psi\rangle$ it is sufficient to know the orbit of $G_{\mathcal{A}}$ that $|\psi\rangle$ belongs to. From previous results in chapter 6 we know that there exists a unitary $V \in G_{\mathcal{A}}$ for which $V|\psi_1\rangle = |\psi_2\rangle$ if and only if the reduction of two states $|\psi_1\rangle$ and $|\psi_2\rangle$ to the algebra $\mathcal{A}$ is the same, i.e. if $\langle\psi_1|\tilde{A}_i|\psi_1\rangle = \langle\psi_2|\tilde{A}_i|\psi_2\rangle$ for $\{\tilde{A}_1, \cdots, \tilde{A}_D\}$ a basis of $\mathcal{A}$. This implies that by specifying the reduction of a state to the algebra one has enough information to infer the orbit that the state belongs to and so has enough information to find the value of $\vec{\mathfrak{s}}$. As similar argument can be applied for the density p. So, in general, if the prior p is nonzero only on pure states, then any function which satisfies assumption $1'$ also satisfies assumption 1 and vice versa.

Note that the restriction to pure states plays an essential role in the equivalence of assumptions 1 and $1'$ and this equivalence cannot be extended to the case of mixed states, i.e. in general a parameter $\mathfrak{s}$ which satisfies assumption 1, $\mathfrak{s}(\rho)$ cannot be expressed as a function of $\mathrm{tr}(\rho\tilde{A}_1), \ldots, \mathrm{tr}(\rho\tilde{A}_D)$ if ρ is mixed. For instance, consider the case where $\mathcal{A}$ is the trivial algebra generated by the identity operator, so that $G_{\mathcal{A}}$ is the group of all unitaries on $\mathbb{C}^d$. In this case, the identity operator is a basis for $\mathcal{A}$ and consequently every state ρ has the same reduction to $\mathcal{A}$. This means that the only functions that depend only on the reduction of the state to $\mathcal{A}$ are constant functions. However, there exist non-constant functions $\mathfrak{s}$, such as $\mathfrak{s}(\rho) = \mathrm{tr}(\rho^2)$, which are invariant under the group of all unitaries and therefore have the symmetry property required to satisfy assumption 1. So the equivalence of assumption 1 and assumption $1'$ cannot be extended to the case of mixed states.

10.2.2 Examples

(i) Estimating parameters defined by a single observable

A very simple example of such a multi-copy estimation problem is the one considered by Hayashi *et al.* [67]. A pure state is chosen uniformly according to the Haar measure, and n copies of the state are prepared. The goal is to estimate the expectation value of an observable A for the state. Hayashi *et al.* have shown that for a squared-error figure of merit, the optimal estimation scheme is to simply measure the observable A separately on each system. Our generalization of Schur-Weyl duality can be used to provide a very elementary proof of this result. It can also be used to simplify the solution of estimation problems that are much more complicated, as we shall show.

Casting this in our language, the vector of parameters to be estimated, $\vec{\mathfrak{s}}(\rho)$, has only a single component, $\mathfrak{s}(\rho) = \mathrm{tr}(A\rho)$. The figure of merit considered in Ref. [67] is the expected

cost where the cost function is the squared error, i.e.

$$C(s_{est}, \mathfrak{s}(\rho)) = (s_{est} - \mathfrak{s}(\rho))^2.$$

Finally, the prior they consider is the unitarily-invariant measure over pure states and the channel $\mathcal{E}$ between the source and the estimator is the identity channel. It follows that the assumptions of theorem 79 are all satisfied for the algebra $\mathcal{A} = \text{Alg}\{A, I\}$. Furthermore, one can show that the squared error for a measurement M is a functional of the conditional $q_M(s_{est} \in \Delta_{est} | S \in \Delta)$ in which S is the actual value of the parameter, s_{est} is the estimated value, Δ and Δ_{est} are two arbitrary intervals in $\mathbb{R}$ (see Appendix B.1). So the assumptions of corollary 83 are satisfied. Consequently, the optimal measurement can be confined to $\mathcal{A}^{\otimes n}$, but given that $\mathcal{A}$ is commutative, it follows from corollary 77 that it can be implemented by measuring the observable A separately on each system and performing classical data processing on the outcomes. So we have shown that the result of Hayashi *et al.* is recovered as a special case of ours.

It is worth noting that for estimation problems involving only a single observable A (or a set of commuting observables, which amounts to the same), there is in fact a very broad class of problems for which the optimal estimation can be achieved by separate measurements of A on each system. Indeed, one can consider the estimation of any parameter that depends only on A, i.e. any function of the form $f(\text{tr}(\rho A), \text{tr}(\rho A^2), \text{tr}(\rho^2 A^2), \dots)$. This includes the estimation of higher order moments of A, decisions about the sign of the expectation value of A, etcetera. One can also take the prior p to be arbitrary over pure states as long as it depends only on A. Also prior p can be nonzero on mixed states as long as p is a $G_{\mathcal{A}}$-distortion of a prior which is nonzero only on pure states. Finally, there are many choices for the figure of merit. We mention only two. We could take the mutual information between the estimated values of the parameters and their actual values, or we could take the expected cost for an arbitrary cost function that depends only on A. For all of these cases, the figure of merit for an estimation strategy M is a functional of $q_M(B|\vec{S} \in \vec{\Delta})$ (see App. B.1), so as long as the prior p and the channel $\mathcal{E}$ satisfy assumptions $2'$ and $3'$ of theorem 81, all the assumptions of corollary 83 are satisfied, and separate measurements of A suffice. Our result therefore constitutes a very significant generalization of the previously known results.

(ii) Decision problem for a single qubit

Suppose we are given n copies of qubit state ρ, a density operator in $\text{End}(\mathbb{C}^2)$. For $b \in 0, 1$, define

$$|\psi(\theta, b)\rangle \equiv \cos\frac{\alpha_b}{2}|0\rangle + e^{i\theta}\sin\frac{\alpha_b}{2}|1\rangle$$

where α_0 and α_1 are distinct angles in the range $[0, \pi)$ and where $\theta \in [0, 2\pi)$. Assume the single-copy prior $p(\rho)$ is as follows: the state is drawn from the set $\{|\psi(\theta, b)\rangle\}$ where θ is uniformly distributed over $[0, 2\pi)$ and b has uniform distribution over $\{0, 1\}$. This prior is illustrated in Fig. 10.2(a). The goal is to get information about the value of the bit b using n copies of state given according to this single-copy prior (this example is a decision problem). For instance, one might be interested to determine the value of the bit b with minimum probability of error. In general, we assume the goal is to generate an outcome in the outcome set Ω with σ-algebra $\sigma(\Omega)$ and the performance of different strategies are evaluated by a figure of merit which can be expressed as a functional acting on $q(B|b = b_0)$, i.e., the probability of event $B \in \sigma(\Omega)$ while the value of b is $b_0 \in \{0, 1\}$.

In this case, the parameter to be estimated is defined by

$$\mathfrak{s}(|\psi(\theta, b)\rangle\langle\psi(\theta, b)|) = b.$$

Adopting the convention that $|0\rangle$ and $|1\rangle$ are eigenstates of the Pauli observable σ_z, it is clear that the prior p and the parameter to be estimated, $\mathfrak{s}$, are both invariant under unitaries of the form $e^{i\phi'}e^{i\phi\sigma_z}$ where $\phi, \phi' \in [0, 2\pi)$, which describe phase shifts or rotations about the axis $\hat{z}$. As we have seen in the section 8.1 this group is a gauge group. The algebra that corresponds to the commutant of this gauge group is $\mathcal{A} = \text{Alg}\{\sigma_z, I\}$. Finally, since the figure of merit depends only on $q(B|b = b_0)$ the assumptions of corollary 83 are satisfied. [Note that since $\mathfrak{s}(|\psi(\theta, b)\rangle\langle\psi(\theta, b)|) = b$, b can be thought as the random variable defined by parameter $\mathfrak{s}$ acting on states.] Therefore, we can infer that to achieve the optimal estimation, it suffices to consider POVMs inside the algebra $\mathcal{A}^{\otimes n}$ and since $\mathcal{A}$ is commutative, it suffices to measure σ_z on each system individually. In other words, all the information we can get from the state $|\psi(\theta, b)\rangle^{\otimes n}$ about the value of b we can also get from the mixed state $[\cos^2(\alpha_b)|0\rangle\langle 0| + \sin^2(\alpha_b)|1\rangle\langle 1|]^{\otimes n}$.

Note, however, that if one acquires some information about θ, then this information can be useful for estimating b: In the extreme case where we know the exact value of θ, we can perform the Helstrom measurement [74] for distinguishing the two pure states $|\psi(\theta, 0)\rangle^{\otimes n}$ and $|\psi(\theta, 1)\rangle^{\otimes n}$. So one estimation strategy is to use some of the qubits to estimate θ and then use this information to choose an optimal measurement for estimating b using the rest of qubits. But our result shows that by this strategy one cannot get more information than what one gets by ignoring θ and measuring σ_z on individual systems. [Note that this result also implies that to get information about θ from each system we necessarily disturb its information about b. This can be interpreted as an example of information-disturbance tradeoff.]

Generalization to priors whose support is not confined to pure states. Theorem 81 implies that measuring σ_z on each system is optimal even in the case where the single-copy

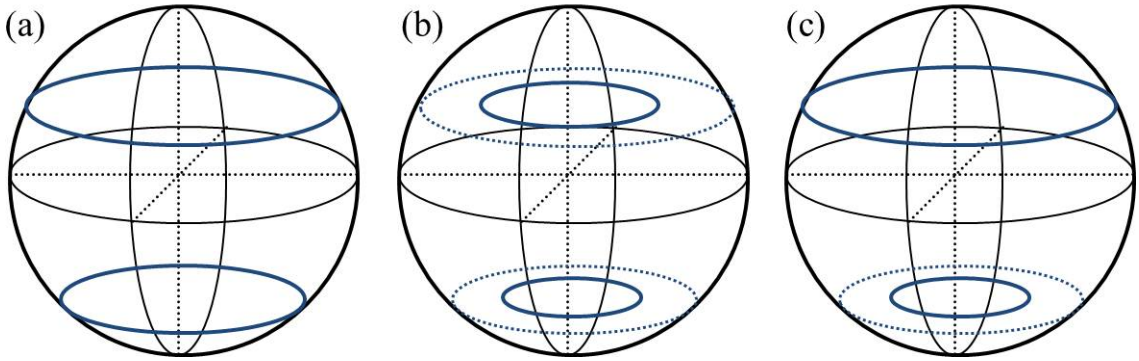

Figure 10.2: The Bloch ball representation of the quantum states of a single qubit for three variations of a decision problem. The pair of circles in each case indicate the support of the single-copy prior over states and the goal is to decide which circle the state is drawn from, given n copies of the state. (a) A prior with support confined to pure states. (b) A prior that is a gauge distortion of the first. (c) A prior for which unentangled measurement will not be generally sufficient to achieve optimal estimation.

prior is a $\mathrm{G}_{\mathcal{A}}$-distortion of the one described above. In this case a $\mathrm{G}_{\mathcal{A}}$-distortion is implemented by a channel $\mathcal{N}$ that is covariant under phase shifts and noiseless on $\mathrm{Alg}\{\sigma_z, I\}$. The only channels having these properties are those corresponding to dephasing about the $\hat{z}$ axis (i.e. $\mathcal{N}(\rho) = (1-r)\rho + r\ \sigma_z\rho\sigma_z$ for $0 < r < 1$). For the single-copy prior that is achieved by this distortion, the state is drawn from the set $\{\rho(\theta, b) \equiv \mathcal{N}(|\psi(\theta, b)\rangle\langle\psi(\theta, b)|)\}$ where b and θ are distributed as before (for a given b, this describes a circle *within* the Bloch ball). This prior is illustrated in Fig. 10.2(b). The parameter to be estimated is $\mathfrak{s}(\rho(\theta, b)) = b$. Note that both the prior and the parameter in this new estimation problem are invariant under the group of phase shifts. Corollary 83 implies that the estimation problem so defined is also one wherein the optimal estimation is achieved by implementing a measurement of σ_z on each qubit.

Example where unentangled measurements are generally not sufficient. Now suppose we are given n copies of state $\{\rho(\theta, b)\}$ where

$$\rho(\theta, 0) = |\psi(\theta, 0)\rangle\langle\psi(\theta, 0)| \quad \text{and} \quad \rho(\theta, 1) = \mathcal{N}(|\psi(\theta, 1)\rangle\langle\psi(\theta, 1)|)$$

where $\mathcal{N}$ is an arbitrary dephasing channel and where again θ is uniformly distributed between $(0, 2\pi]$ and b has arbitrary distribution. Effectively, we have a U(1)-orbit of pure states (a circle on the Bloch sphere) for $b = 0$, and a dephased version of a distinct U(1)-

orbit (a circle within the Bloch ball) for $b = 1$. This prior is illustrated in Fig. 10.2(c). Again the goal is to find the value of the bit b.

This estimation problem satisfies assumption 1 of theorems 79 and 81 because the prior and the parameter have the same gauge group symmetry as the other examples considered in this section. We seek to show that nonetheless, in this case, the optimal measurement is *not* achieved by performing separate measurements of σ_z on each qubit.

To see this, note first that because the $b = 0$ states are pure while the $b = 1$ states are mixed, the purity of the state does contain information about b. Now consider the projective measurement which projects the state to the different irreps of $\mathcal{S}_n$ which show up in the representation $\mathbf{P}(\mathcal{S}_n)$ on $(\mathbb{C}^d)^{\otimes n}$. It is well known that this von Neumann measurement is highly nonlocal and requires interaction between all n systems [75]. This projective measurement is one that reveals information about the eigenvalues of the single-copy density operator and hence about its purity, as the following argument demonstrates.

First, note that if the single-copy state is pure, then the n-copy state is in the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$ and the outcome of the above projective measurement is fixed. On the other hand, if the single-copy state is mixed, then there is always a nonzero probability that the measurement projects the state to a subspace other than the symmetric subspace. In other words, there is a nonzero probability that the outcome of this measurement achieves an unambiguous discrimination between the mixed state case and the pure state case. This implies that there is a nonzero probability of determining the true value of b unambgiuously. However, one can easily see that for the given prior by measuring σ_z on each qubit it is not possible to unambigiously determine the true value of the bit b. Therefore, at least for some figures of merit, entangled measurements have advantage over unentangeled measurements.

Incidentally, note that since the state of the total n systems is a permutationally-invariant state, i.e. it commutes with $\mathbf{P}(\mathcal{S}_n)$ it is block diagonal in the irreps of $\mathcal{S}_n$ that show up in the representation of $\mathbf{P}(\mathcal{S}_n)$. Therefore by performing the von Neumann measurement which projects into these blocks, the final state (forgetting the outcome of this measurement) will be the same as the initial state and therefore the statistics of any subsequent measurement will not be affected, that is, implementing such a measurement does not compromise the informativeness of any other measurement.

This phenomenon is generic. In multi-copy decision problems in which the goal is to distinguish between a mixed state and a pure state, entangled measurements can achieve a better performance than unentangled measurements (at least with respect to some figures of merit).

(iii) Decision problem for pair of qubits

In the previous example we assumed a bit is encoded in the state of one qubit and the goal is to acquire information about that bit using n copies of that qubit state. Now suppose we modify the example in the following way: We assume each system consists of two qubits (rather than one), left and right, i.e. the Hilbert space of each system is $\mathbb{C}^4 \cong \mathcal{H}_L \otimes \mathcal{H}_R$ where $\mathcal{H}_{L/R} \cong \mathbb{C}^2$. Again, we are given n copies of state ρ according to the single-copy prior $p(\rho)$ which is defined as follows: the state is drawn from the set

$$\{(\mathbb{I} \otimes V)|\psi(b)\rangle_{LR}\},$$

where b is uniformly distributed on $b \in \{0, 1\}$, V is distributed according to the Haar measure over U(2), and

$$|\psi(0)\rangle_{LR} = |00\rangle_{LR} \ , \quad |\psi(1)\rangle_{LR} = \frac{|01\rangle_{LR} + |10\rangle_{LR}}{\sqrt{2}}.$$

The goal is again to get information about the bit b and therefore, the parameter to be estimated is defined implicitly by the condition that

$$\mathfrak{s}\left((\mathbb{I} \otimes V)|\psi(b)\rangle_{LR}\right) = b.$$

It is then clear that the group of all unitaries acting on the right qubit, i.e. $\{\mathbb{I} \otimes V : V \in U(2)\}$ is a symmetry group of both the prior p and the parameter $\mathfrak{s}$. Moreover, this group of unitaries is clearly a gauge group, so it is a gauge symmetry of the prior and the parameter. The algebra associated with this gauge group is the full algebra of operators on the left qubit, i.e. $\mathcal{A} \equiv \mathrm{End}(\mathcal{H}_L) \otimes \mathbb{I}$.

Again, we can see that for any figure of merit which depends only on $q(B|b = b_0)$, the assumptions of corollary 83 are satisfied and therefore to achieve the optimal estimation, it suffices to consider measurement operators inside the algebra $\mathcal{A}^{\otimes n}$. It follows that it suffices to consider measurements that are nontrivial on the left qubits only. In other words, one can essentially ignore the right qubits. Note that deciding about the value of b is also equivalent to deciding whether the reduced state of the right qubits is $(V|0\rangle)^{\otimes n}$ or $(\mathbb{I}/2)^{\otimes n}$. It follows that the n right qubits do contain some information about the value of b, however, our results imply that once one has the information contained in the left qubits, the information contained in the right qubits is redundant.

10.2.3 Conclusion

Given that the class of estimation problems for which our results apply is very large, they represent a dramatic expansion, relative to previously known results, in the scope of prob-

lems for which we can easily determine the optimal measurement. Furthermore, in previous results where independent measurements on each copy were shown to be optimal, such as Ref. [67], the reasoning was rather *ad hoc*. It was not clear what feature of the estimation problem implied the sufficiency of such measurements. By contrast, our approach follows a clear methodology – we are determining the consequences of the gauge symmetries of the estimation problem. Our results establish a sufficient condition for the optimality of independent measurements, i.e. the lack of any need for adaptive or entangled measurements. It is that the set of single-copy observables that are needed to define the estimation problem form a *commutative* set. In a slogan, *the commutativity of the observables defining the estimation problem imply the adequacy of independent measurements.*

10.3 Proof of theorem 79 and theorem 81

To prove theorem 79 we first prove the following lemma which holds for any arbitrary subgroup of the unitary group.

Lemma 84 *(**From symmetry of the problem to symmetry of the measurement**) In the scenario described in section 10.2, assume the prior p and the vector of parameters $\vec{\mathfrak{s}}$ are invariant under a subgroup H of U(d) which has the (normalized) Haar measure $d\mu$. Then for any measurement described by a POVM $M : \sigma(\Omega) \to End((\mathbb{C}^d)^{\otimes n})$, the measurement described by*

$$\tilde{M} \equiv \mathcal{T}_{\boldsymbol{Q}(H)}(M) = \int_H d\mu(V)\ V^{\otimes n} M V^{\dagger \otimes n}$$

is as informative as M about $\vec{\mathfrak{s}}$, that is,

$$q_M\left(B|\vec{S} \in \vec{\Delta}\right) = q_{\tilde{M}}\left(B|\vec{S} \in \vec{\Delta}\right) \tag{10.8}$$

for all $B \in \sigma(\Omega)$ and all l-dimensional intervals $\vec{\Delta} \subseteq \mathbb{R}^l$ which are assigned nonzero probability.

Proof. First note that for any $B \in \sigma(\Omega)$

$$q_M(B|\rho) = \mathrm{tr}\left(\rho^{\otimes n} M(B)\right)$$

and

$$q_{\tilde{M}}(B|\rho) = \mathrm{tr}\left(\rho^{\otimes n}[\int_H d\mu(V)\ V^{\otimes n} M(B) V^{\dagger \otimes n}]\right)$$

Therefore, by the cyclic property of the trace,

$$q_{\tilde{M}}(B|\rho) = \int_H d\mu(V)\ q_M(B|V\rho V^\dagger) \tag{10.9}$$

On the other hand,

$$q_M\left(B|\vec{S}\in\vec{\Delta}\right) = \frac{1}{\Pr(\vec{S}\in\vec{\Delta})}\int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \ q_M(B|\rho) \tag{10.10}$$

and similarly

$$q_{\tilde{M}}\left(B|\vec{S}\in\vec{\Delta}\right) = \frac{1}{\Pr(\vec{S}\in\vec{\Delta})}\int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \ q_{\tilde{M}}(B|\rho) \tag{10.11}$$

where $\Pr(\vec{S}\in\vec{\Delta})$ is defined as

$$\Pr(\vec{S}\in\vec{\Delta}) \equiv \int_{\vec{\mathfrak{s}}(\rho)\in\vec{\Delta}} \mathrm{d}\rho\ p(\rho). \tag{10.12}$$

But

$$\begin{aligned}
&\int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \ q_{\tilde{M}}(B|\rho)\\
&= \int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \int_H d\mu(V)\ q_M(B|V\rho V^\dagger)\\
&= \int_H d\mu(V)\int_{\vec{\mathfrak{s}}(V\rho V^\dagger)\in\vec{\Delta}} d\rho\ p(V\rho V^\dagger)\ q_M(B|V\rho V^\dagger)\\
&= \int_H d\mu(V)\int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \ q_M(B|\rho)\\
&= \int_{\vec{S}\in\vec{\Delta}} d\rho\ p(\rho)\ \ q_M(B|\rho)
\end{aligned}$$

where to get the second line we use Eq.(10.9), to get the third line we use the invariance of p and $\vec{\mathfrak{s}}$ under G, to get the fourth line we use the fact that the measure $d\rho$ is invariant under unitary transformations and to get the last line we use the fact that the Haar measure of H is normalized. This completes the proof. ■

Proof. (**Theorem** 79)

According to the first condition in theorem 79, the prior p and the parameters $\vec{\mathfrak{s}}$ are invariant under the gauge group $G_{\mathcal{A}}$. So we can use lemma 84 for the symmetry group $G_{\mathcal{A}}$. This implies that for any given POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ and

$$\tilde{M} \equiv \mathcal{T}_{\mathbf{Q}(G_{\mathcal{A}})}(M) = \int_{G_{\mathcal{A}}} d\mu(V)\ V^{\otimes n} M {V^\dagger}^{\otimes n} \tag{10.13}$$

it holds that

$$q_{\tilde{M}}\left(B|\vec{S}\in\vec{\Delta}\right)=q_{M}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.14}$$

for all $B\in\sigma(\Omega)$ and all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability. Now according to assumption 3 of theorem 79, the prior p is nonzero only for pure states. So for all states in $\{\rho^{\otimes n}:\rho\in\mathrm{supp}(p)\}$, i.e. the states Alice is sending to Bob, the support of the state is restricted to the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$. Since, by assumption 2, the channel is assumed to be the identity map, Bob receives the same state. Therefore all states that Bob receives are restricted to the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$. By virtue of corollary 78, this together with the fact that the measurement $\tilde{M}$ has global symmetry imply $\forall B\in\sigma(\Omega)$ and $\forall\rho\in\mathrm{supp}(p)$

$$\mathrm{tr}\left(\tilde{M}(B)\rho^{\otimes n}\right)=\mathrm{tr}\left(\mathcal{L}_{+}(\tilde{M}(B))\rho^{\otimes n}\right)$$

Define $M'\equiv\mathcal{L}_{+}(\tilde{M})$ where $\mathcal{L}_{+}$ is the superoperator defined in Eq.(8.10) of theorem 76. Then the above equality implies that

$$q_{\tilde{M}}\left(B|\vec{S}\in\vec{\Delta}\right)=q_{M'}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.15}$$

for all $B\in\sigma(\Omega)$ and all $\vec{\Delta}$ which are assigned nonzero probability. This together with Eq.(10.14) implies that for arbitrary POVM M

$$q_{M}\left(B|\vec{S}\in\vec{\Delta}\right)=q_{M'}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.16}$$

for all $B\in\sigma(\Omega)$ and all $\vec{\Delta}$ which are assigned nonzero probability.

Finally, using the fact that Π_{+} commutes with $V^{\otimes n}$ for arbitrary $V\in\mathrm{U}(d)$ we can easily see that

$$\mathcal{L}_{+}(\tilde{M})=\mathcal{L}_{+}(M),$$

so that

$$M'=\mathcal{L}_{+}(M).$$

From theorem 76, we know that the image of $\mathcal{L}_{+}$ is in $\mathcal{A}^{\otimes n}$ and therefore so is $M'(B)$ for arbitrary $B\in\sigma(\Omega)$. ■

Proof. (**Theorem 81**)

We first prove the special case of theorem 81 where assumptions 1, 2' and 3 hold. In other words, we first prove the theorem for the case of general channels which satisfy the

assumptions of theorem 81 but for the special case where the prior is still nonzero only on pure states. Then we extend the result to the case of general priors which satisfy the assumption 3'.

(i) Generalization to non-identity channels, pure state priors:

The idea is to convert the estimation problem with channel $\mathcal{E}$ to another estimation problem with the identity channel and then apply the result of theorem 79 to this new estimation problem.

For any estimation problem described by the parameters $\vec{\mathfrak{s}}$, prior p, and the channel $\mathcal{E}$, we consider the two following scenarios:

- Scenario (a) in which Alice prepares n copies of the state ρ according to the probability density $p(\rho)$ and sends them through the channel $\mathcal{E}$ and then Bob performs a measurement described by POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$, and
- Scenario (b) in which Alice prepares n copies of the state ρ according to the probability density $p(\rho)$ but then sends them through the identity channel and Bob performs the measurement described by POVM $\mathcal{E}^\dagger(M)$ on the systems.

The definitions of these two scenarios immediately imply

$$q^{(a)}_M\left(B|\vec{S}\in\vec{\Delta}\right) = q^{(b)}_{\mathcal{E}^\dagger(M)}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.17}$$

where the left and right hand sides describe the conditional for the scenarios (a) and (b) respectively. This is true because in the scenario (a) the probability of event $B \in \sigma(\Omega)$ given that Alice has chosen state ρ is $\mathrm{tr}\left(M(B)\mathcal{E}(\rho^{\otimes n})\right)$. On the other hand, in the scenario (b), the probability of event $B \in \sigma(\Omega)$ given that the state chosen by Alice is ρ is $\mathrm{tr}\left(\mathcal{E}^\dagger(M(B))\rho^{\otimes n}\right)$. But since

$$\mathrm{tr}\left(M(B)\mathcal{E}(\rho^{\otimes n})\right) = \mathrm{tr}\left(\mathcal{E}^\dagger(M(B))\rho^{\otimes n}\right)$$

for all $\rho \in \mathrm{supp}(p)$ and $B \in \sigma(\Omega)$, Eq.(10.17) follows.

Now in the scenario (b), where the channel is the identity map, we can apply theorem 79. Note that the assumptions of this theorem are satisfied for the gauge group $G_{\mathcal{A}}$. This implies

$$q^{(b)}_{\mathcal{L}_+(\mathcal{E}^\dagger(M))}\left(B|\vec{S}\in\vec{\Delta}\right) = q^{(b)}_{\mathcal{E}^\dagger(M)}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.18}$$

Since the channel $\mathcal{E}$ is noiseless on $\mathcal{A}^{\otimes n}$ (assumption 2') then all elements of $\mathcal{A}^{\otimes n}$ are fixed points of $\mathcal{E}^\dagger$. (The fact that $\mathcal{E}$ is noiseless on $\mathcal{A}^{\otimes n}$ implies that for any operators

$R_1 \in \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ and $R_2 \in \mathcal{A}^{\otimes n}$ it holds that $\mathrm{tr}\,(R_2\mathcal{E}(R_1)) = \mathrm{tr}\,(R_2R_1)$. But this implies that $\mathrm{tr}\left(\mathcal{E}^\dagger(R_2)R_1\right) = \mathrm{tr}\,(R_2R_1)$ which proves the claim.)

Then since elements of $\mathcal{A}^{\otimes n}$ are fixed points of $\mathcal{E}^\dagger$ and since the image of $\mathcal{L}_+$ is in $\mathcal{A}^{\otimes n}$ we conclude that

$$\mathcal{E}^\dagger \circ \mathcal{L}_+ = \mathcal{L}_+$$

Putting this into Eq.(10.18) we find

$$q^{(b)}_{\mathcal{E}^\dagger\circ\mathcal{L}_+\circ\mathcal{E}^\dagger(M)}\left(B|\vec{S}\in\vec{\Delta}\right) = q^{(b)}_{\mathcal{E}^\dagger(M)}\left(B|\vec{S}\in\vec{\Delta}\right)$$

Now for the conditionals on each side of this equality, we use Eq.(10.17) to find the measurement in the scenario (a) that yields the same conditional. We infer that

$$q^{(a)}_{\mathcal{L}_+\circ\mathcal{E}^\dagger(M)}\left(B|\vec{S}\in\vec{\Delta}\right) = q^{(a)}_{M}\left(B|\vec{S}\in\vec{\Delta}\right), \tag{10.19}$$

and this holds for arbitrary $\rho \in \mathrm{supp}(p)$ and event $B \in \sigma(\Omega)$ and arbitrary POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. This completes the proof of the special case of the theorem where the prior p is nonzero only for pure states. Note that in this particular case one can choose

$$M' \equiv \mathcal{L}_+ \circ \mathcal{E}^\dagger(M).$$

(ii) Generalization to mixed state prior:

According to assumption 1 the prior p is invariant under $G_\mathcal{A}$ and according to assumption 3', it can be realized by first sampling a pure state from $\tilde{p}$ and then applying channel $\mathcal{N}$ to the state where $\mathcal{N}$ is both $G_\mathcal{A}$ covariant and noiseless on $\mathcal{A}$. Then one can easily see that the prior $\tilde{p}$ can always be chosen to be invariant under $G_\mathcal{A}$. In other words, for any given prior $\tilde{p}$ which satisfies the above properties there exists a prior p' defined as

$$p'(\cdot) \equiv \int_{G_\mathcal{A}} d\mu(V)\ \tilde{p}(V\cdot V^\dagger) \tag{10.20}$$

which also satisfies these properties, i.e. p' is nonzero only on pure states and furthermore one can realize the prior p by sampling a pure state from p' and then applying the quantum channel $\mathcal{N}$ to the state. In addition to these properties, definition 10.20 guarantees that p' is also invariant under $G_\mathcal{A}$.

Now consider the estimation problem which is specified by the parameters $\vec{\mathfrak{s}}$, the prior p and the channel $\mathcal{E}$ which satisfy all the assumptions of theorem 81. We call this *estimation problem (a)*. Now define *estimation problem (b)* via the following modifications of problem (a):

1. We change the prior p to p' defined in Eq. (10.20).

2. We change the parameters $\vec{\mathfrak{s}}$ to $\vec{\mathfrak{s}}'$ where

$$\vec{\mathfrak{s}}'(\cdot) \equiv \vec{\mathfrak{s}}\,(\mathcal{N}(\cdot)) \tag{10.21}$$

   and so naturally replace the random variables $\vec{S}$ induced by parameters $\vec{\mathfrak{s}}$ to the random variables $\vec{S}'$ induced by parameters $\vec{\mathfrak{s}}'$.

3. We change the channel $\mathcal{E}$ in the problem (a) to the channel

$$\mathcal{E}' \equiv \mathcal{E} \circ \mathcal{N}^{\otimes n}. \tag{10.22}$$

For any POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ let

$$q_M^{(a)}\left(B|\vec{S} \in \vec{\Delta}\right)$$

be the conditional that in problem (a) an event $B \in \sigma(\Omega)$ happens given $\vec{S} \in \vec{\Delta}$ and similarly

$$q_M^{(b)}\left(B|\vec{S}' \in \vec{\Delta}\right)$$

be the conditional that in problem (b) an event $B \in \sigma(\Omega)$ happens given $\vec{S}' \in \vec{\Delta}$.

Now one can easily see that by the manner in which they are defined, the parameters $\mathfrak{s}'$, prior p' and channel $\mathcal{E}'$ of problem (b) satisfy all the assumptions of the theorem.

On the other hand, since p' is nonzero only for pure states then in the case of problem (b) we can use the result of part (i) of this proof, Eq. (10.19), which implies that for any POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$

$$q_M^{(b)}\left(B|\vec{S}' \in \vec{\Delta}\right) = q_{\mathcal{L}_+ \circ \mathcal{E}'^{\dagger}(M)}^{(b)}\left(B|\vec{S}' \in \vec{\Delta}\right) \tag{10.23}$$

for all $B \in \sigma(\Omega)$ and for all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability.

Then it can be shown that for any POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$ it holds that

$$q_M^{(a)}\left(B|\vec{S} \in \vec{\Delta}\right) = q_M^{(b)}\left(B|\vec{S}' \in \vec{\Delta}\right) \tag{10.24}$$

for all $B \in \sigma(\Omega)$ and for all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability. We present the proof of this equality at the end. Now this equality allows us

to transform the conditionals for problem (a) to the conditionals for the problem (b). Applying Eq. (10.24) to both sides of Eq.(10.23), we get

$$q_M^{(a)}\left(B|\vec{S}\in\vec{\Delta}\right)=q_{\mathcal{L}_+\circ\mathcal{E}'^\dagger(M)}^{(a)}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.25}$$

Recall that the problem (a) is the original problem in the statement of theorem. So, defining

$$M'\equiv\mathcal{L}_+\circ\mathcal{E}'^\dagger(M)=\mathcal{L}_+\circ\mathcal{N}^{\dagger\otimes n}\circ\mathcal{E}^\dagger(M)$$

we conclude that in the original problem for arbitrary POVM M, for arbitrary $B\in\sigma(\Omega)$ and for arbitrary $\vec{\Delta}$, it holds that

$$q_M\left(B|\vec{S}\in\vec{\Delta}\right)=q_{M'}\left(B|\vec{S}\in\vec{\Delta}\right) \tag{10.26}$$

where for all $B\in\sigma(\Omega)$, $M'(B)$ is in $\mathcal{A}^{\otimes n}$ as it is claimed in the theorem.

So it remains only to prove that Eq.(10.24) holds. Let $\vec{\Delta}\subseteq\mathbb{R}^l$, and define probability measures

$$\begin{aligned}\Pr^{(a)}\left(\vec{S}\in\vec{\Delta}\right)&\equiv\int_{\vec{\mathfrak{s}}(\rho)\in\vec{\Delta}}d\rho\;p(\rho)\qquad\text{and,}\\ \Pr^{(b)}\left(\vec{S}'\in\vec{\Delta}\right)&\equiv\int_{\vec{\mathfrak{s}}'(\rho)\in\vec{\Delta}}d\rho\;p'(\rho).\end{aligned}$$

Note that

$$\begin{aligned}q_M^{(a)}(B|\vec{S}\in\vec{\Delta})&\equiv\frac{\int_{\vec{S}\in\vec{\Delta}}d\rho p(\rho)\;q_M^{(a)}(B|\rho)}{\Pr^{(a)}\left(\vec{S}\in\vec{\Delta}\right)}\qquad\text{and,}\\ q_M^{(b)}(B|\vec{S}'\in\vec{\Delta})&\equiv\frac{\int_{\vec{S}'\in\vec{\Delta}}d\rho p'(\rho)\;q_M^{(b)}(B|\rho)}{\Pr^{(b)}\left(\vec{S}'\in\vec{\Delta}\right)}\end{aligned}$$

Now using the definition $\mathfrak{s}'(\cdot)\equiv\mathfrak{s}(\mathcal{N}(\cdot))$ from Eq. (10.21), we get

$$\begin{aligned}\Pr^{(b)}\left(\vec{S}'\in\vec{\Delta}\right)&=\int_{\vec{\mathfrak{s}}(\mathcal{N}(\rho))\in\vec{\Delta}}d\rho\;p'(\rho)\\ &=\int_{\vec{\mathfrak{s}}(\rho)\in\vec{\Delta}}d\rho\;p(\rho)\\ &=\Pr^{(a)}\left(\vec{S}\in\vec{\Delta}\right)\end{aligned} \tag{10.27}$$

where to get the second line we have used the fact that by sampling a pure state from p' and applying the channel $\mathcal{N}$ to it realizes the prior p. Using exactly the same argument for

$$q_M^{(b)}(B|\rho) = \mathrm{tr}\left(\mathcal{E}'(\rho^{\otimes n})M(B)\right) \qquad \text{and}$$
$$q_M^{(a)}(B|\rho) = \mathrm{tr}\left(\mathcal{E}(\rho^{\otimes n})M(B)\right)$$

and the definition $\mathcal{E}' \equiv \mathcal{E} \circ \mathcal{N}^{\otimes n}$, Eq. (10.22), we can prove that

$$\int_{\vec{S}\in\vec{\Delta}} d\rho\; p(\rho)\; q_M^{(a)}(B|\rho) = \int_{\vec{S}'\in\vec{\Delta}} d\rho\; p'(\rho)\; q_M^{(b)}(B|\rho) \tag{10.28}$$

Eqs. (10.28) and (10.27) together imply Eq.(10.24). This completes the proof. ■

Chapter 11

Single-copy estimation problems for bipartite systems

Previously in this thesis, the distinction between global and local symmetries was relative to the partitioning of the total system into n copies of the system of interest. However, one can also consider estimation problems where the estimator gets only a single copy of the system of interest, and the distinction between global and local symmetries is relative to the partitioning of the system of interest into its components. This case can be significantly different because the components of the system of interest need not correspond to copies of a single state. Indeed, they could even be entangled.

In particular, we consider the case where the system has only *two* components. This case allows us to obtain particularly strong constraints on the optimal measurement because the permutation group on two systems has only irreducible representations over the symmetric and antisymmetric subspaces and our duality only permits an inference from global symmetry to local symmetry within the symmetric and antisymmetric subspaces (as shown by the counterexample from section 8.3.1).

11.1 General framework

We begin with some notation. The canonical representation of the permutation group on the pair is $\mathbf{P}(\mathcal{S}_2) \equiv \{\mathbb{I}_{d\times d}, \text{Swap}\}$, where $\mathbb{I}_{d\times d}$ is the identity operator on $(\mathbb{C}^d)^{\otimes 2}$ and Swap is the unitary which exchanges the state of the two systems, i.e. $\text{Swap}(|\psi\rangle|\phi\rangle) = |\phi\rangle|\psi\rangle$.

Under $\mathbf{P}(\mathcal{S}_2)$, the space $(\mathbb{C}^d)^{\otimes 2}$ decomposes as

$$(\mathbb{C}^d)^{\otimes 2} \cong [(\mathbb{C}^d)^{\otimes 2}]_+ \oplus [(\mathbb{C}^d)^{\otimes 2}]_- \tag{11.1}$$

Also, for any subgroup $H \subseteq \mathrm{U}(d)$, the collective representation of H on the pair of systems is denoted by $\mathbf{Q}(G_{\mathcal{A}}) \equiv \{V^{\otimes 2} : V \in G_{\mathcal{A}}\}$.

We are now in a position to state our result.

Scenario: Suppose that Alice randomly chooses an unknown state ρ from the density operators in $\mathrm{End}\left((\mathbb{C}^d)^{\otimes 2}\right)$ according to some probability density p and sends a single system in the state ρ to Bob. Here, the density p is defined relative to $d\rho$ a reference measure on the space of mixed states which is invariant under unitary transformations. Let $\vec{\mathfrak{s}}(\cdot) = \left(\mathfrak{s}^{(1)}(\cdot), \cdots, \mathfrak{s}^{(l)}(\cdot)\right)$ be an arbitrary set of functions where $\mathfrak{s}^{(i)} : \mathrm{supp}(p) \to \mathbb{R}$, and let $\vec{S}$ be the random variables defined as $\vec{S} \equiv \vec{\mathfrak{s}}(\rho)$ where ρ is the random state Alice chooses. We refer to $\vec{\mathfrak{s}}$ as the *parameters*.

Recalling our earlier definitions, Eqs. (10.4) and (10.5), of what it means for a prior p and a vector of parameters $\vec{\mathfrak{s}}$ to have a symmetry, we can state our result as follows:

Theorem 85 *Let $\mathcal{A} \subseteq End(\mathbb{C}^d)$ be a von Neumann algebra with the gauge group $G_{\mathcal{A}}$. Assume that the prior p and the vector of parameters $\vec{\mathfrak{s}}$*

1. *have $\boldsymbol{Q}(G_{\mathcal{A}})$ as a symmetry;*
2. *have $\boldsymbol{P}(\mathcal{S}_2)$ as a symmetry.*

Then for any given measurement with POVM $M : \sigma(\Omega) \to End((\mathbb{C}^d)^{\otimes 2})$, there is another measurement whose POVM is of the form

$$M' \equiv \Pi_+ M_+ \Pi_+ + \Pi_- M_- \Pi_-$$

where $M_\pm : \sigma(\Omega) \to \mathcal{A}^{\otimes 2}$ are POVMs, such that M' is as informative about $\vec{S}$ as M is, i.e.,

$$q_M\left(B|\vec{S} \in \vec{\Delta}\right) = q_{M'}\left(B|\vec{S} \in \vec{\Delta}\right) \tag{11.2}$$

for all $B \in \sigma(\Omega)$ and all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability.

The proof is provided at the end of this section. Note that unlike theorems 79 and 81, the prior is not presumed to have support only on the pure states nor to be a gauge distortion of one that does.

Remark 86 *The measurement M' described in the above theorem can be implemented as follows: first perform the measurement which projects onto the symmetric/anti-symmetric subspace (the projective measurement described by projectors $\{\Pi_+, \Pi_-\}$) and then, depending on the outcome of this measurement, perform either measurement M_+ or M_- where both have local symmetry with respect to $G_{\mathcal{A}}$. The outcome of measurement M' is the outcome of whichever of these measurements was performed.*

11.1.1 Example

Suppose that the prior over the pair of systems has support only on product states $\rho_1 \otimes \rho_2$ where $\rho_1, \rho_2 \in \mathrm{End}(\mathbb{C}^d)$ and that it corresponds to choosing ρ_1 and ρ_2 independently according to a prior p_0, so that the joint prior has the form $p(\rho_1 \otimes \rho_2) = p_0(\rho_1)p_0(\rho_2)$. Assume further that $p_0(\rho)$ only depends on the eigenvalues of ρ, so that $p_0(\cdot) = p_0\left(V(\cdot)V^\dagger\right)$ for arbitrary $V \in \mathrm{U}(d)$, i.e., p_0 has $\mathrm{U}(d)$ as a symmetry. It follows that the prior p on the pair has $\mathbf{Q}(\mathrm{U}(d))$ as a symmetry, and consequently it also has $\mathbf{Q}(H)$ as a symmetry for any subgroup H of $\mathrm{U}(d)$. Moreover, the prior p is invariant under permutations, i.e. it has $\mathbf{P}(\mathcal{S}_2)$ as a symmetry.

The goal is to estimate the parameter $\mathfrak{s}(\rho_1 \otimes \rho_2) = |\mathrm{tr}\,(A\rho_1) - \mathrm{tr}\,(A\rho_2)\,|$ for some observable A. Let $\mathcal{A}$ denote the algebra generated by $\{\mathbb{I}_d, A \in \mathrm{End}(\mathbb{C}^d)\}$ and let $G_{\mathcal{A}}$ denote the associated gauge group. It is clear that $\mathfrak{s}$ has $\mathbf{Q}(G_{\mathcal{A}})$ as a symmetry. Furthermore, $\mathfrak{s}$ is invariant under a swap of the pair of systems and therefore has $\mathbf{P}(\mathcal{S}_2)$ as a symmetry as well. The parameter $\mathfrak{s}$ therefore satisfies the assumptions of the above theorem for the gauge group $G_{\mathcal{A}}$. Furthermore, because $G_{\mathcal{A}}$ is a subgroup of $\mathrm{U}(d)$, the prior p satisfies the assumptions of the above theorem as well.

So, for any figure of merit that can be defined as a functional acting on $q_M\,(B|S = s_0)$, the optimal estimation strategy corresponds to a POVM M' of the form described in the theorem. In our example, such a measurement has a particularly simple form. First, note that because the two POVMs M_+ and M_- have local symmetry with respect to $G_{\mathcal{A}}$ and because $\mathcal{A}$ is commutative, using proposition 77, we can conclude that M_+ and M_- can both be realized by measuring a Hermitian generator of $\mathcal{A}$ (e.g. the operator A) individually on each system and performing a classical processing of the outcome. This means that in the case of this example, the POVM M' described in the theorem can be realized by (i) performing the measurement which projects the state into the symmetric and anti-symmetric subspaces, (ii) measuring the observable A individually on each system and (iii) generating the outcome by a classical processing of the outcomes of these measurements. So for all such M's, the measurements are fixed and the part which is different is just the classical processing.

The same result holds for any other parameter which is invariant with respect to the exchange of the pair of systems and can be expressed in terms of an operator A, such as $\mathfrak{s}(\rho_1 \otimes \rho_2) = \mathrm{tr}\,(A\rho_1) + \mathrm{tr}\,(A\rho_2)$ or more complicated parameters such as $\mathfrak{s}(\rho_1 \otimes \rho_2) = \mathrm{tr}\left(A\rho_1^k\rho_2^k\right) + \mathrm{tr}\left(A\rho_2^k\rho_1^k\right)$ for some integer k.

11.1.2 Proof of theorem 85

Proof. (Theorem 85) We need to apply lemma 84 in its special case where $n = 1$ and the Hilbert space of a single copy (which was denoted by $\mathbb{C}^d$ in the statement of lemma) is $\mathbb{C}^d \otimes \mathbb{C}^d$. The symmetry of the problem, denoted by $H \subseteq \mathrm{U}(d^2)$, is the group generated by $\mathbf{Q}(G_{\mathcal{A}})$ and $\mathbf{P}(\mathcal{S}_2)$ together. Then lemma 84 implies that for any POVM $M : \sigma(\Omega) \to \mathrm{End}(\mathbb{C}^d \otimes \mathbb{C}^d)$ there is a POVM

$$\tilde{M} \equiv \mathcal{T}_H(M) = \int_H d\mu(V)\ VMV^\dagger$$

such that

$$q_{\tilde{M}}\left(B|\vec{S} \in \vec{\Delta}\right) = q_M\left(B|\vec{S} \in \vec{\Delta}\right)$$

for all $B \in \sigma(\Omega)$ and all l-dimensional intervals $\vec{\Delta}$ which are assigned nonzero probability. Now the above definition implies that $\tilde{M}$ is invariant under permutation, i.e. $\tilde{M} = \mathrm{Swap}[\tilde{M}]\mathrm{Swap}$. This implies that

$$\tilde{M} = \Pi_+\tilde{M}\Pi_+ + \Pi_-\tilde{M}\Pi_-.$$

$\tilde{M}$ also has global symmetry with respect to the gauge group $G_{\mathcal{A}}$, i.e. it commutes with $\mathbf{Q}(G_{\mathcal{A}})$. Now corollary 78 implies that for states whose supports are restricted to the symmetric/anti-symmetric subspaces a measurement with global symmetry with respect to gauge group G_A can be simulated by a measurement whose POVM has local symmetry (and so its POVM elements are in $\mathcal{A} \otimes \mathcal{A}$). Therefore there exists POVMs M_+ and M_- where $M_\pm : \sigma(\Omega) \to \mathcal{A} \otimes \mathcal{A}$ such that

$$\Pi_+M_+\Pi_+ = \Pi_+\tilde{M}\Pi_+ \quad \text{and} \quad \Pi_-M_-\Pi_- = \Pi_-\tilde{M}\Pi_-$$

An example of $M_\pm$ is $\mathcal{L}_\pm(\tilde{M})$. Also since $\Pi_\pm\mathcal{L}_\pm(\tilde{M})\Pi_\pm = \Pi_\pm\mathcal{L}_\pm(M)\Pi_\pm$, it follows that $\mathcal{L}_\pm(M)$ is also an example of $M_\pm$. This completes the proof. ■

Chapter 12

Agreement between independent observers

In this chapter, we show that the generalization of Schur-Weyl duality we introduced in chapter 8 has a very intuitive physical interpretation if one considers a particular problem concerning two independent observers using different conventions to describe quantum systems. This discussion also reveals the motivation for calling the specific subgroups of U(d) for which this generalization hold *gauge groups*.

Consider two observers, Alice and Bob, who are both trying to describe states and observables of the same physical system. Assume each observer uses his/her own personal convention to associate states and observables with operators in the Hilbert space $\mathcal{H}$ of the system, and assume that each observer is not aware of the other's convention.

In this chapter we are interested in answering the following two questions:

1. Assuming Alice and Bob agree on the description of a given set of physical states and observables, what are the set of all states and observable for which we can be sure that Alice and Bob have the same description? We call this set the *set of agreement*.

2. Suppose these two observers are trying to describe the states and observables defined on n-copies of this system and they use the same conventions for describing each one of these n copies. Then what is the set of agreement in this case?

Question (i) is answered in section 12.1 and question (ii) is answered in section 12.2. The answer to question (i) is a straightforward application of Wigner's theorem.[1] It is the

[1] See the footnote at page 12.

solution to question (ii) that will make use of the generalization of Schur-Weyl duality.

Note: In all the previous chapters we have used $\mathrm{Alg}\{B_i\}$ to denote the *complex* associative algebra generated by the set of operators $\{B_i\}$. Unlike the rest of this thesis, in this chapter we need to consider both the *real* associative algebras and the *complex* associative algebras generated by a set of operators $\{B_i\}$. So, to distinguish these two cases we denote the former by $\mathrm{Alg}^{\mathbb{R}}\{B_i\}$ and the latter by $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$.

12.1 The set of agreement for a single copy of the system

We begin by formalizing the notion that Alice and Bob use different conventions. A state which Alice describes by a density operator ρ, Bob describes by the density operator $f_s(\rho)$, where f_s is a bijection from the space of density operators of this physical system to itself. Furthermore, an observable which is described by the operator B with respect to Alice's convention is described by the operator $f_o(B)$ relative to Bob's convention where f_o is a bijection from the space of observables to itself. So, in general, the relation between Alice and Bob's conventions is described by a pair of bijections (f_s, f_o). However, Alice and Bob are describing the *same* physical states and observables, therefore using any of these two conventions to find an observable quantity, such as the expectation value of an observable for a given state, they should get the same results. In other words, for all observables B and all sates ρ we should have

$$\mathrm{tr}(\rho B) = \mathrm{tr}(f_s(\rho) f_o(B)) \tag{12.1}$$

This consistency condition is very powerful and can highly restricts the possible forms of the two bijections f_o and f_s. In particular, one can show that $f_s(\cdot) = f_o(\cdot)$ and so we denote both by the map f. Also, one can argue that f should map pure states to pure states and then using Wigner's theorem one can show that $f(\cdot) = V(\cdot)V^\dagger$ for some unitary or anti-unitary V.

Now suppose Alice and Bob somehow agree on the description of a set of operators (observables and states) $\{B_i\}$ such that

$$\forall i : f(B_i) = B_i. \tag{12.2}$$

Suppose V is the unitary or anti-unitary which relates Alice's and Bob's conventions to each other such that $f(\cdot) = V(\cdot)V^\dagger$. Then Eq. (12.2) implies that $\forall i : VB_iV^\dagger = B_i$ and

therefore the unitary or anti-unitary V satisfies $\forall i : [V, B_i] = 0$. Based on this observation we can prove the following

Proposition 87 (Single-copy set of agreement) *Suppose Alice and Bob use different conventions to describe states and observables of a system with Hilbert space $\mathcal{H}$. Given the fact that the only thing they know about the relation between their conventions is that they agree on the description of states/observables $\{B_i \in End(\mathcal{H})\}$, then the set of agreement in $End(\mathcal{H})$ is exactly equal to all states/observables which are in*

1. *$Alg^{\mathbb{C}}\{B_i\}$ if there does not exist an anti-unitary V such that $\forall B_i : [V, B_i] = 0$.*
2. *$Alg^{\mathbb{R}}\{B_i\}$ if there exists an anti-unitary V such that $\forall B_i : [V, B_i] = 0$.*

Proof. Suppose there does not exist any anti-unitary V which satisfies $\forall B_i : [V, B_i] = 0$. Then we know that the relation between the conventions of the two parties is described by a unitary V for which $\forall B_i : [V, B_i] = 0$. Then one can easily see that for any operator B in the *complex* associative algebra generated by $\{B_i\}$, denoted by $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$, we have

$$f(B) = VBV^\dagger = B \tag{12.3}$$

So any state/observable in this algebra is in the set of agreement. Now we show that there does not exist any operator outside $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$ for which the two observers can be sure that they have the same description of it. This can be seen by noting that for any given operator $B^\perp \notin \mathrm{Alg}^{\mathbb{C}}\{B_i\}$ there is a unitary V^* which commutes with all $\{B_i\}$ but does not commute with $B^\perp$[2]. So if the relation between their two conventions were described by V^*, Alice and Bob could have the same description of $\{B_i\}$, but they would disagree about the description of $B^\perp$. This argument can be made for any operator outside of $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$. This completes the proof of item 1.

In the following we prove item 2 of the proposition. Here, the assumption is that there exists an anti-unitary which commutes with all $\{B_i\}$. Therefore, the fact that Alice and Bob agree on the description of the set $\{B_i\}$ alone is not sufficient to determine whether their relation is described by a unitary or an anti-unitary. But still from item 1 we can infer that the set of agreement should be a subset of $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$ and any observable/state outside $\mathrm{Alg}^{\mathbb{C}}\{B_i\}$ may have different descriptions in the two conventions.

Assume V is an arbitrary anti-unitary for which $\forall B_i : [V, B_i] = 0$. Then one can easily see that for any operator B in $\mathrm{Alg}^{\mathbb{R}}\{B_i\}$ the *real* associative algebra generated by $\{B_i\}$ it holds that

$$f(B) = VBV^\dagger = B \tag{12.4}$$

[2]This can be easily shown for example by decomposing the algebra into irreducible algebras.

So if the relation is described by an unknown anti-unitary which commutes with all $\{B_i\}$ then all states/observables inside $\text{Alg}^{\mathbb{R}}\{B_i\}$ should be in the set of agreement.

Now since $\text{Alg}^{\mathbb{R}}\{B_i\} \subseteq \text{Alg}^{\mathbb{C}}\{B_i\}$, even if the two observers do not know whether their conventions are related via a unitary or an anti-unitary they can still be sure that they agree on the description of all states/observables in $\text{Alg}^{\mathbb{R}}\{B_i\}$. In the following we prove that in this situation, where the two observers do not know whether their conventions are related via a unitary or an anti-unitary, there is no state/observable outside $\text{Alg}^{\mathbb{R}}\{B_i\}$ for which the two observers can be sure that they have the same description of it.

First recall that the set of agreement is a subset of $\text{Alg}^{\mathbb{C}}\{B_i\}$. From the above discussion we also know that any state/observable in $\text{Alg}^{\mathbb{R}}\{B_i\}$ is in the set of agreement. Now we argue that there is no state/observable in $\text{Alg}^{\mathbb{C}}\{B_i\}\backslash\text{Alg}^{\mathbb{R}}\{B_i\}$ in the set of agreement. To see this we note that an arbitrary element of $\text{Alg}^{\mathbb{C}}\{B_i\}$ can be written as $C_1 + iC_2$ where $C_{1,2} \in \text{Alg}^{\mathbb{R}}\{B_i\}$. Now if there exists an anti-unitary V such that $\forall i: \ [V, B_i] = 0$ then it also leaves C_1 and C_2 invariant but it transform $C_1 + iC_2$ to $C_1 - iC_2$. So if there exists such an anti-unitary then Alice and Bob cannot be sure whether they have the same description of any state or observable which is in $\text{Alg}^{\mathbb{C}}\{B_i\}\backslash\text{Alg}^{\mathbb{R}}\{B_i\}$. This completes the proof. ■

In retrospect, it was reasonable to expect that if two parties agree on $\{B_i\}$ then they agree on all elements of $\text{Alg}^{\mathbb{C}}\{B_i\}$ on the grounds that there are few other natural choices for the solution to the problem. And this is indeed the correct answer in the case that their conventions are assumed to be related by a unitary. However, this is an unnatural assumption. Their conventions might well be related by an anti-unitary and if there exists an anti-unitary that commutes with all elements of $\{B_i\}$, then the correct answer is $\text{Alg}^{\mathbb{R}}\{B_i\}$. So the result is not completely intuitive.

Example 88 *Suppose Alice and Bob agree on the description of the set of observables* $\{\mathbb{I}, \sigma_x, \sigma_y\}$ *where the system is a qubit. Then, they will also agree on the description of any observable in* $Alg^{\mathbb{R}}\{B_i\}$ *which is equal to the set of* $\{r_0\mathbb{I} + r_x\sigma_x + r_y\sigma_y : r_{0,x,y} \in \mathbb{R}\}$. *Note that* $i\sigma_z$ *is also in* $Alg^{\mathbb{R}}\{B_i\}$ *but it is not a hermitian operator and so is not an observable. On the other hand, since* $Alg^{\mathbb{R}}\{B_i\}$ *is a real algebra this does not imply that* σ_z *is also in the algebra. However,* $Alg^{\mathbb{C}}\{B_i\}$ *includes all qubit observables and in particular* σ_z *but Alice and Bob do not necessarily agree on the description of this observable. In other words, there is an anti-unitary which leaves* σ_x, σ_y *invariant but it transforms* σ_z *to* $-\sigma_z$.

Note that if $\text{Alg}^{\mathbb{C}}\{B_i\} = \text{Alg}^{\mathbb{R}}\{B_i\}$ then there exists no anti-unitary which commutes with all elements of $\{B_i\}$ but the inverse does not hold, i.e. $\text{Alg}^{\mathbb{C}}\{B_i\} \neq \text{Alg}^{\mathbb{R}}\{B_i\}$ does not imply that there exists an anti-unitary which commutes with all elements of $\{B_i\}$. This is shown in the following example.

Example 89 *We modify the example above in the following way: The system is described by a four dimensional Hilbert space which we will think of as* $\mathbb{C}^2 \oplus \mathbb{C}^2$*. Suppose they agree on the description of the following six operators*

$$\{\mathbb{I}_2 \oplus \mathbb{I}_2, \sigma_x \oplus \mathbb{I}_2, \sigma_y \oplus \mathbb{I}_2, \mathbb{I}_2 \oplus \sigma_x, \mathbb{I}_2 \oplus \sigma_y, \mathbb{I}_2 \oplus \sigma_z\}$$

where $\mathbb{I}_2$ *is the identity operator on* $\mathbb{C}^2$*. Then in this case, although* $Alg^{\mathbb{C}}\{B_i\} \neq Alg^{\mathbb{R}}\{B_i\}$*, there is no anti-unitary commuting with all* $\{B_i\}$*: If an anti-unitary* V *leaves* $\mathbb{I}_2 \oplus \sigma_x$ *and* $\mathbb{I}_2 \oplus \sigma_y$ *invariant it cannot leave* $\mathbb{I}_2 \oplus \sigma_z$ *invariant, because*

$$V(I \oplus \sigma_z)V^\dagger = V(-i)(\mathbb{I}_2 \oplus \sigma_x)(\mathbb{I}_2 \oplus \sigma_y)V^\dagger = -\mathbb{I}_2 \oplus \sigma_z.$$

So, since there is no anti-unitary which leaves all $\{B_i\}$ *invariant then proposition 87 implies that two observers agree on the description of all states/observable in* $Alg^{\mathbb{C}}\{B_i\}$ *and in particular they agree on the description of* $\sigma_z \oplus \mathbb{I}_2$ *though it is not in* $Alg^{\mathbb{R}}\{B_i\}$*.*

As we have seen in the above, in the case where we know that the relation between Alice's and Bob's conventions is described by a unitary, and not an anti-unitary, the set of agreement is exactly equal to all states and observables in $\mathcal{B} = \mathrm{Alg}^{\mathbb{C}}\{B_i\}$. Then, to specify the set of agreement one should somehow specify the algebra $\mathcal{B}$. Clearly this can be done by specifying a set of generators of the algebra, say the set $\{B_i\}$. Alternatively, one can specify $G_{\mathcal{B}}$, the set of unitaries that commute with the algebra (or, equivalently, that commute with a set of generators of the algebra). Note that this set of unitaries forms a gauge group, i.e. it is equal to the centralizer of its centralizer in the group of all unitaries. We call it the *gauge group of the set of agreement*. One can think of these unitaries as all possible unitaries that can relate Bob's convention to Alice's convention while leaving all states/observables B_i invariant, i.e. satisfying Eq. (12.2). This observation leads to a natural interpretation of the generalization of Schur-Weyl duality as we shall see in Sec. 12.2.

This discussion also reveals the motivation for calling the group $G_{\mathcal{B}}$ a *gauge group*. It is because such a group describes the possible transformations that leave the physically relevant set of observables invariant (in this case, the single-system observables that Alice and Bob agree upon), and such transformations are typically called gauge transformations by physicists.

12.2 The set of agreement for multiple copies of the system

Now consider the states and observables defined on $\mathcal{H}^{\otimes n}$, that is, n copies of the system of interest. By the same arguments provided earlier, Alice's and Bob's conventions on this composite system must be related by a bijection $f^{(n)}(\cdot) = V^{(n)}(\cdot)V^{(n)\dagger}$ where $V^{(n)}$ is a unitary or an anti-unitary. We shall make an assumption about Alice and Bob's conventions on the n-copy system, namely, that for every $A \in \text{End}(\mathcal{H})$, there exists an $A' \in \text{End}(\mathcal{H})$ such that

$$\forall m \in \{0, \ldots, n-1\}: \quad f^{(n)}\left(I^{\otimes m} \otimes A \otimes I^{\otimes(n-m-1)}\right) = I^{\otimes m} \otimes A' \otimes I^{\otimes(n-m-1)} \tag{12.5}$$

This assumption means that Alice and Bob agree on which degrees of freedom in the composite system correspond to the subsystems of interest, that is, they agree on how to partition the composite system into n copies. Furthermore, the fact that $\forall m \in \{0, \ldots, n-1\}$ the same operator A' is assigned to the operator A means that the relation between Alice's and Bob's conventions is the same for each of the n copies. In other words, if the subsystems have the same description in the convention of one party, then they also have the same description in the convention of the other.[3] It follows from these two assumptions that $f^{(n)}(\cdot) = f^{\otimes n}(\cdot)$ for some single-copy f, or equivalently, that $V^{(n)} = V^{\otimes n}$ for some single-copy V that is either unitary or anti-unitary.

Now consider the situation where two observers agree on the description of a set of observables $\{B_i \in \text{End}(\mathcal{H})\}$ defined on the subsystems (note that $\{B_i\}$ are operators acting on $\mathcal{H}$ and not on $\mathcal{H}^{\otimes n}$). Then the question is: under this situation what is the set of agreement, i.e. the set of all states/observables defined on the n subsystems which we can be sure the two parties have the same descriptions of them?

To answer this question, first note that since both observers have the same description of the observables $\{B_i\}$ then the possible unitary (anti-unitaries) which can relate their description of the states of subsystems are unitaries (anti-unitaries) which commute with all $\{B_i\}$. This implies that the set of agreement is the set of states/observables which are invariant under $V^{\otimes n}$ for arbitrary unitary or anti-unitary V which commutes with all $\{B_i\}$. Assume for a moment that we know that the relation between the two conventions is described by a unitary (and not an anti-unitary). So the unitary V which relates the convention for single copy systems is in $G_{\mathcal{B}}$, the gauge group of the algebra $\mathcal{B} = \text{Alg}^{\mathbb{C}}\{B_i\}$.

[3] Were the relation between conventions to be different for different copies, then all we could say about $f^{(n)}$ would be that $f^{(n)}(A^{\otimes n}) = A'_1 \otimes A'_2 \otimes \cdots \otimes A'_n$ for some $A'_1, A'_2, \ldots, A'_n \in \text{End}(\mathcal{H})$.

Now theorem 71 or equivalently corollary 72 can be used to find the set of agreement for the multipartite system. Any state/observable which is invariant under $V^{\otimes n}$ for all $V \in G_{\mathcal{B}}$ is by definition in the commutant of the complex algebra generated by $\mathbf{Q}(G_{\mathcal{B}})$. But by corollary 72, this is just the the complex associative algebra generated by $\langle \mathcal{B}^{\otimes n}, \mathbf{P}(\mathcal{S}_n) \rangle$.

So in this case, where we know the conventions are related via a unitary, the set of agreement is equal to $\mathrm{Alg}^{\mathbb{C}}\{\mathbf{P}(\mathcal{S}_n), B_{i_1} \otimes \cdots \otimes B_{i_n} : B_{i_k} \in \{B_i\}\}$. Now using a similar argument to the one we used in the case of $n = 1$, one can show that if we do not know whether the relation is via a unitary or an anti-unitary then the set of agreement is the *real* associative algebra generated by $\{B_{i_1} \otimes \cdots \otimes B_{i_n} : B_{i_k} \in \{B_i\}\}$ and the elements of the permutation group $\mathbf{P}(\mathcal{S}_n)$. So to summarize we have proven that

Proposition 90 (Multi-copy set of agreement) *Suppose Alice and Bob use different conventions to describe states/observables on n copies of a system with the Hilbert space $\mathcal{H}$ (so the total Hilbert spaces is $\mathcal{H}^{\otimes n}$). Furthermore, assume each party uses the same convention for describing the states/observables of all these n systems (i.e. Eq.(12.5) holds). Finally, assume Alice and Bob know that they agree on the description of states/observables $\{B_i \in End(\mathcal{H})\}$ on a single system. Given that these assumptions are all they know about the relation between their conventions, the set of agreement defined on n copies of this system is exactly equal to all states/observables which are in*

1. *$Alg^{\mathbb{C}}\{\boldsymbol{P}(\mathcal{S}_n), B_{i_1} \otimes \cdots \otimes B_{i_n} : B_{i_k} \in \{B_i\}\}$ if there does not exist an anti-unitary V such that $\forall B_i : [V, B_i] = 0$.*
2. *$Alg^{\mathbb{R}}\{\boldsymbol{P}(\mathcal{S}_n), B_{i_1} \otimes \cdots \otimes B_{i_n} : B_{i_k} \in \{B_i\}\}$ if there exists an anti-unitary V such that $\forall B_i : [V, B_i] = 0$.*

Ignoring the extra complexity introduced by the possibility of anti-unitaries which can relate two conventions, this result gives us an intuitive understanding of the generalization of Schur-Weyl duality: If two parties agree on the description of states/observables $\{B_i\}$ on a single system then they also agree on the description of the n-fold tensor product of these operators, i.e. $\{B_{i_1} \otimes \cdots \otimes B_{i_n} : B_{i_k} \in \{B_i\}\}$. Furthermore, since they agree on how to partition the composite system into n copies, i.e. Eq.(12.5) holds, they also agree on the description of all permutations $\mathbf{P}(\mathcal{S}_n)$. Now intuitively, one expect that any state or observable that Alice and Bob can agree on its description should be in the algebra formed by these operators. There does not exist any other natural candidate. Trying to prove this intuition will naturally lead us to the generalization of Schur-Weyl duality.

Conclusion (Part II)

In part II of this thesis we introduced the notion of gauge groups and provided a simple characterization of them. We saw that any gauge group can be thought as the set of all unitaries which describe a change of reference frame or convention under which the description of a certain set of observables remain unchanged. This is in fact the main motivation for the name of gauge groups.

We proved some nice properties of the tensor product representations of gauge groups and, based on these properties, we introduced a new example of dual reductive pairs on the space $\left(\mathbb{C}^d\right)^{\otimes n}$. More precisely, for any gauge group $G \subseteq U(d)$ we constructed two subgroups of $\mathrm{GL}(d^n)$ such that the span of each is equal to the algebra formed by the commutants of the other. The standard Schur-Weyl duality is the specific case of these new dual reductive pairs where the gauge group is the unitary group U(d).

We also proved that a stronger form of this duality holds in the symmetric and anti-symmetric subspaces of $\left(\mathbb{C}^d\right)^{\otimes n}$. Furthermore, by virtue of a counterexample, we showed that this stronger form of duality does not exist in the subspaces corresponding to the other irreps of the permutation group $\mathcal{S}_n$.

This stronger form of duality implies that for any operator acting on $\left(\mathbb{C}^d\right)^{\otimes n}$ with global symmetry with respect to a gauge group $G \subseteq U(d)$ there exists an operator which i) has local symmetry with respect to G and ii) its restriction to the symmetric (anti-symmetric) subspace is exactly equal to the original operator. We found a completely positive, unital super-operator which realizes this map from operators with global symmetry to operators with local symmetry.

Applying this result to Hamiltonians or measurements with global symmetry with respect to a gauge group can have interesting implications in quantum information theory. In particular, we showed that if a measurement on n qudits has global symmetry with respect to a gauge group $G \subseteq U(d)$ then there exists a measurement with local symmetry with respect to that gauge group which has exactly the same statistics for all states of n

qudits whose support are restricted to the symmetric (anti-symmetric) subspace of $(\mathbb{C}^d)^{\otimes n}$.

As we explained, the importance of this result is that the local symmetry of measurements can put strong constraints on the amount of entanglement and interactions which are required to implement them. In particular, we showed that if a measurement on n qudits has local symmetry with respect to the gauge group of a commutative algebra of operators $\mathcal{A} \subset \mathrm{End}(\mathbb{C}^d)$ then the measurement can be realized by measuring observables which generate $\mathcal{A}$ on each single qudit separately and then performing a classical processing on the outcomes of all these measurements to generate the outcome of the original measurement on n qudits.

We used this result to study a particular family of quantum estimation problems in which one is given n copies of a qudit state where the state is chosen according to some known prior and the goal is to find information about the state of this qudit. For example, the goal is to estimate the expectation value of a certain set of observables for the state of qudit. The performance of a particular estimation procedure is evaluated via a figure of merit such as the mutual information or the mean squared error.

We introduced a framework for describing the figures of merit. The point of this specific way of describing figures of merit is to clarify which parameters of state they depend on which, in turn, clarifies the symmetries of the figure of merit. For instance, from this point of view, the following figures of merit depend on the same parameter and so have the same symmetries: i) the mutual information between the actual value of the expectation value of an observable and its estimated value and ii) the mean squared error of this estimation.

Then we showed that, if the prior is nonzero only for pure states, then the optimal measurement for this estimation problem can be chosen to have local symmetry with respect to the gauge symmetry of the estimation problem, i.e. the gauge group which describes transformations under which the prior, the parameters to be estimated and the figure of merit remain unchanged.

We also demonstrate several other generalizations of the basic multi-copy estimation problem – to cases which include mixed states and to cases where the channel between the source and the estimator can be noisy – such that our results still have nontrivial consequences for the optimal measurement.

Given that the class of estimation problems for which our results apply is very large, they represent a dramatic expansion, relative to previously known results, in the scope of problems for which we can easily determine the optimal measurement. Furthermore, in previous results where independent measurements on each copy were shown to be optimal, such as Ref. [67], the reasoning was rather *ad hoc*. It was not clear what feature of the estimation problem implied the sufficiency of such measurements. By contrast, our approach

follows a clear methodology – we are determining the consequences of the gauge symmetries of the estimation problem. Our results establish a sufficient condition for the optimality of independent measurements, i.e. the lack of any need for adaptive or entangled measurements. It is that the set of single-copy observables that are needed to define the estimation problem form a *commutative* set. In a slogan, *the commutativity of the observables defining the estimation problem imply the adequacy of independent measurements.*

We also demonstrated that our result about promoting global symmetry of measurements to local symmetry has applications for a different type of estimation problems where the estimator gets only a single copy of the state of a system formed form two qudits. In the particular case of a system formed from *two* qudits the permutation group has only irreducible representations corresponding to the symmetric and antisymmetric subspaces. But in both of these subspaces the strong form duality hold. This implies a very strong constraint on the form of optimal measurement.

Appendix A

Appendices of part I

A.1 Input-output Hilbert spaces

In general the input and output Hilbert space of a time evolution are not the same ($\mathcal{H}_{\text{in}} \neq \mathcal{H}_{\text{out}}$). This can happen especially in the case of open system time evolutions. However, we can always assume that the input and output spaces are two different sectors of a larger Hilbert space ($\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$) and extend the time evolution to a time evolution which acts on this larger Hilbert space. Therefore without loss of generality we can restrict our attention to the cases where the input and output Hilbert spaces are the same.

On the other hand, when the spaces are equipped with a representation of a symmetry group and the time evolution is covariant we may also care about the symmetries of the extended time evolution and therefore this process of embedding spaces in a larger space is less trivial. Suppose there is a representation of group G on the input and output Hilbert spaces given by $\{U_{\text{in}}(g) : g \in G\}$ and $\{U_{\text{out}}(g) : g \in G\}$. Suppose the time evolution is G-covariant i.e. $\mathcal{E} \circ \mathcal{U}_{\text{in}}(g) = \mathcal{U}_{\text{out}}(g) \circ \mathcal{E}$ for all $g \in G$. In the following we will show that it is always possible to extend this time evolution to a time evolution on $\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$ such that this extended time evolution respects the natural representation of G on $\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$ given by $\{U_{\text{in}}(g) \oplus U_{\text{out}}(g) : g \in G\}$. Therefore without loss of generality we can always restrict our attention to the G-covariant time evolutions whose input and output Hilbert spaces are the same. In particular when we ask whether there exists a G-covariant time evolution which maps ρ to σ we can always assume ρ and σ live in two sectors of the same Hilbert space.

A.1.1 General G-covariant Channels

Suppose $\mathcal{E}$ is a channel (completely positive-trace preserving linear map) from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$ which is G-covariant i.e. for all $g \in G$ we get $U_{\text{out}}(g)\mathcal{E}[\cdot]U_{\text{out}}^{\dagger}(g) = \mathcal{E}(U_{\text{in}}(g)[\cdot]U_{\text{in}}^{\dagger}(g))$. Then we can always extend this channel to $\tilde{\mathcal{E}}$ a G-covariant channel from $\mathcal{B}(\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}})$ to itself by defining

$$\tilde{\mathcal{E}} \equiv \mathcal{E}(\Pi_{\text{in}}[\cdot]\Pi_{\text{in}}) + \frac{I_{\mathcal{H}_{\text{in}}\oplus\mathcal{H}_{\text{out}}}}{d_{\text{in}} + d_{\text{out}}}\text{tr}(\Pi_{\text{out}}[\cdot]\Pi_{\text{out}}) \tag{A.1}$$

where $I_{\mathcal{H}_{\text{in}}\oplus\mathcal{H}_{\text{out}}}/(d_{\text{in}} + d_{\text{out}})$ is the totally mixed state on $\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$. Clearly by this definition $\tilde{\mathcal{E}}$ is completely positive and trace preserving and so a valid channel and moreover it is G-covariant. Furthermore the restriction of $\tilde{\mathcal{E}}$ to $\mathcal{H}_{\text{in}}$ i.e. $\tilde{\mathcal{E}}(\Pi_{\text{in}}[\cdot]\Pi_{\text{in}})$ is equal to $\mathcal{E}(\cdot)$.

On the other hand, if there is a G-covariant channel $\mathcal{B}(\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}})$ to itself which maps all operators in $\mathcal{B}(\mathcal{H}_{\text{in}})$ to operators in $\mathcal{B}(\mathcal{H}_{\text{out}})$ then clearly by restricting its input to $\mathcal{B}(\mathcal{H}_{\text{in}})$ we get a valid G-covariant channel from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to operators in $\mathcal{B}(\mathcal{H}_{\text{out}})$.

Finally consider the situation where there is a G-covariant channel $\mathcal{E}$ from $\mathcal{B}(\mathcal{H})$ to itself which maps ρ_i to σ_i for a set of i's. Assume the representation of group G on the Hilbert space is $\{U(g) : g \in G\}$. Define Π_{in} and Π_{out} to be respectively the span of the supports of all operators $\{U(g)\rho_i U^{\dagger}(g)\}$ and $\{U(g)\sigma_i U^{\dagger}(g)\}$. It is clear from this definition that both Π_{in} and Π_{out} commute with all $\{U(g) : g \in G\}$. Therefore the subspace associated to these projectors $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ have a natural representation of the group G given by $\{\Pi_{\text{in}}U(g)\Pi_{\text{in}}\}$ and $\{\Pi_{\text{out}}U(g)\Pi_{\text{out}}\}$. Now $\tilde{\mathcal{E}} \equiv \mathcal{E}(\Pi_{\text{in}}[\cdot]\Pi_{\text{in}})$ is a new G-covariant quantum channel which maps states from $\mathcal{B}(\mathcal{H}_{\text{in}})$ to $\mathcal{B}(\mathcal{H}_{\text{out}})$ and $\tilde{\mathcal{E}}(\rho_i) = \sigma_i$.

A.1.2 G-invariant unitaries and G-invariant isometries

Basically we can repeat all of those observations for equivalence of a G-invariant unitary, where the input and output are the same Hilbert spaces, and a G-invariant isometry where the input and output Hilbert spaces are different.

For example if there exists a G-invariant unitary on $\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$ which unitarily maps the subspace $\mathcal{H}_{\text{in}}$ to (a subspace) of $\mathcal{H}_{\text{out}}$ then clearly there exists a G-invariant isometry V from H_{in} to $\mathcal{H}_{\text{out}}$ such that $\forall g \in G : \; VU_{\text{in}}(g) = U_{\text{out}}(g)V$ and $V^{\dagger}V = I_{\text{in}}$ where I_{in} is the identity on $\mathcal{H}_{\text{in}}$.

The only property which is less trivial in the case of unitary-isometry equivalences is the the following: Suppose V is an isometry from H_{in} to H_{out} which is G-invariant i.e.

$\forall g \in G : VU_{\rm in}(g) = U_{\rm out}(g)V$. Then there exits a unitary V_{ext} on $\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out}$ such that $\forall g :\in G : V_{ext}(U_{\rm in}(g) \oplus U_{\rm out}(g)) = (U_{\rm in}(g) \oplus U_{\rm out}(g))V_{ext}$ and moreover $V = \Pi_{\rm out} V_{ext} \Pi_{\rm in}$ where $\Pi_{in/out}$ is the projector to $\mathcal{H}_{in/out}$. This is shown by the following lemma

Lemma 91 *Suppose W maps the subspace of the support of the projector Π unitarily to another subspace such that $\Pi W^\dagger W \Pi = \Pi$ (in other words, $W\Pi$ is an isometry). Then if $\forall g \in G : [W\Pi, U(g)] = 0$ there exits a unitary W_{G-inv} such that $\forall g \in G : [W_{G-inv}, U(g)] = 0$ and $W_{G-inv}\Pi = W\Pi$.*

Proof. $W\Pi$ commutes with all $U(g)$ and so does $\Pi W^\dagger$. Therefore $\Pi = \Pi W^\dagger W \Pi$ also commutes with all $U(g)$. Now we consider the decomposition of $U(g)$ to the irreps.

$$U(g) = \bigoplus_\mu U_\mu(g) \otimes I_{\mathcal{N}_\mu} \tag{A.2}$$

Since Π commutes with all $\{U(g) : g \in G\}$ it has a simple form in this basis:

$$\Pi = \bigoplus_\mu I_\mu \otimes \Pi^{(\mu)} \tag{A.3}$$

where $\Pi^2 = \Pi$ implies ${\Pi^{(\mu)}}^2 = \Pi^{(\mu)}$ and so all $\Pi^{(\mu)}$'s are projectors (Note that for some μ, Π_μ might be zero.). $W\Pi$ also commutes with all $\{U(g)\}$. Since $W\Pi = (W\Pi)\Pi$ we conclude that the decomposition of $W\Pi$ should be in the following form

$$W\Pi = \bigoplus_\mu I_\mu \otimes (W^{(\mu)}\Pi^{(\mu)}) \tag{A.4}$$

$\Pi W^\dagger W \Pi = \Pi$ implies that $\Pi^{(\mu)} {W^{(\mu)}}^\dagger W^{(\mu)} \Pi^{(\mu)} = \Pi^{(\mu)}$. Therefore $W^{(\mu)}\Pi^{(\mu)}$ unitarily acts on on the subspace of the support of $\Pi^{(\mu)}$. Now we can always find a unitary $\tilde{W}^{(\mu)}$ on this subsystem such that $\tilde{W}^{(\mu)}\Pi^{(\mu)} = W^{(\mu)}\Pi^{(\mu)}$. Finally define the unitary $\tilde{W}$ as

$$W_{G-inv} = \bigoplus_\mu I_\mu \otimes \tilde{W}^{(\mu)} \tag{A.5}$$

Clearly it commutes with all $\{U(g)\}$ and $\tilde{W}\Pi = W\Pi$. ■

A.2 Proof of proposition 41

Suppose we are restricted to use rotationally invariant Hamiltonians and we can prepare states in rotationally invariant states. Therefore any measurement we can realize is rotationally invariant, i.e. its POVM commutes with the representation of rotation. Under this restriction we cannot distinguish two orthogonal spin-half states $|\uparrow\rangle_{\hat{n}}$ and $|\downarrow\rangle_{\hat{n}}$.

Now suppose we are given a spin-j system in state ρ and we can use it as a quantum reference frame to distinguish two states $|\uparrow\rangle_{\hat{n}}$ and $|\downarrow\rangle_{\hat{n}}$ where these states are given with equal probability. Hereafter we drop the direction $\hat{n}$. So, we are basically trying to distinguish states

$$\rho \otimes |\uparrow\rangle\langle\uparrow| \quad \text{and} \quad \rho \otimes |\downarrow\rangle\langle\downarrow|$$

using measurements which have rotational symmetry. But this problem is equivalent to the problem of distinguishing two states

$$\mathcal{G}\left(\rho \otimes |\uparrow\rangle\langle\uparrow|\right) \quad \text{and} \quad \mathcal{G}\left(\rho \otimes |\downarrow\rangle\langle\downarrow|\right)$$

using arbitrary measurement, where $\mathcal{G}$ is uniform twirling over all rotations.

From Helstrom's theorem we know that the maximum probability of success which we can obtain using a quantum reference frame ρ is

$$p_{\text{succ}}(\rho) \equiv \frac{1}{2} + \frac{\|\mathcal{G}\left(\rho \otimes |\uparrow\rangle\langle\uparrow|\right) - \mathcal{G}\left(\rho \otimes |\downarrow\rangle\langle\downarrow|\right)\|}{4} \tag{A.6}$$

To calculate this probability of success we first note that $\mathcal{G}(\rho \otimes |\uparrow\rangle\langle\uparrow|)$ and $\mathcal{G}(\rho \otimes |\downarrow\rangle\langle\downarrow|)$ have very simple forms. We can easily see that

$$\mathcal{G}(\rho \otimes |\uparrow\rangle\langle\uparrow|) = p_{j+1/2}\frac{\Pi_{j+1/2}}{2j+2} + p_{j-1/2}\frac{\Pi_{j-1/2}}{2j} \tag{A.7}$$

and

$$\mathcal{G}(\rho \otimes |\downarrow\rangle\langle\downarrow|) = q_{j+1/2}\frac{\Pi_{j+1/2}}{2j+2} + q_{j-1/2}\frac{\Pi_{j-1/2}}{2j} \tag{A.8}$$

where $\Pi_{j\pm1/2}$ is the projector to the subspace corresponding to irrep $j \pm 1/2$ and $p_{j+1/2}$, $p_{j-1/2}$, $q_{j+1/2}$, $q_{j-1/2}$ are all positive numbers which satisfy

$$p_{j+1/2} + p_{j-1/2} = 1 \quad \text{and} \quad q_{j+1/2} + q_{j-1/2} = 1 \tag{A.9}$$

Then we find

$$\begin{aligned}\|\mathcal{G}\left(\rho\otimes|\uparrow\rangle\langle\uparrow|\right)-\mathcal{G}\left(\rho\otimes|\downarrow\rangle\langle\downarrow|\right)\| &= |p_{j+1/2}-q_{j+1/2}|+|p_{j-1/2}-q_{j-1/2}| \\ &= 2|p_{j+1/2}-q_{j+1/2}| \end{aligned} \tag{A.10}$$

In the following we calculate $|p_{j+1/2}-q_{j+1/2}|$ and to do this we consider the expectation value of $L^2_{\rm tot}$, the total angular momentum of quantum reference frame and spin-half system for state $\mathcal{G}(\rho\otimes|\uparrow\rangle\langle\uparrow|)$ and for state $\mathcal{G}(\rho\otimes|\downarrow\rangle\langle\downarrow|)$. First, notice that $L^2_{\rm tot}$, is invariant under rotations and so for any state τ

$$\mathrm{tr}(L^2_{\rm tot}\tau)=\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\tau)\right) \tag{A.11}$$

So

$$\begin{aligned}\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\uparrow\rangle\langle\uparrow|)\right) &= \mathrm{tr}\left(L^2_{\rm tot}(\rho\otimes|\uparrow\rangle\langle\uparrow|)\right) \\ &= p_{j+1/2}(j+1/2)(j+3/2)+p_{j-1/2}(j-1/2)(j+1/2)\end{aligned}$$

and

$$\begin{aligned}\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\downarrow\rangle\langle\downarrow|)\right) &= \mathrm{tr}(L^2_{\rm tot}(\rho\otimes|\downarrow\rangle\langle\downarrow|)) \\ &= q_{j+1/2}(j+1/2)(j+3/2)+q_{j-1/2}(j-1/2)(j+1/2)\end{aligned}$$

Therefore we get

$$\left|\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\uparrow\rangle\langle\uparrow|)\right)-\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\downarrow\rangle\langle\downarrow|)\right)\right|=(2j+1)|p_{j+1/2}-q_{j+1/2}|$$

where we have used Eqs.(A.9).

On the other hand, total angular momentum $L^2_{\rm tot}$ is equal to

$$L^2_{\rm tot}=L^2+S^2+2\overrightarrow{S}.\overrightarrow{L}_{\rm RF} \tag{A.12}$$

where $\overrightarrow{L}$ and $\overrightarrow{S}$ are respectively the vector of angular momentum of the quantum reference frame and the spin-half system.

Using this equality we can calculate the difference of expectation value of $L^2_{\rm tot}$ for $\mathcal{G}(\rho\otimes|\uparrow\rangle\langle\uparrow|)$ and $\mathcal{G}(\rho\otimes|\downarrow\rangle\langle\downarrow|)$. It turns out that

$$\begin{aligned}\left|\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\uparrow\rangle\langle\uparrow|)\right)-\mathrm{tr}\left(L^2_{\rm tot}\mathcal{G}(\rho\otimes|\downarrow\rangle\langle\downarrow|)\right)\right| &= 2\left|\mathrm{tr}(\overrightarrow{L}.\overrightarrow{S}\,[\rho\otimes|\uparrow\rangle\langle\uparrow|-\rho\otimes|\downarrow\rangle\langle\downarrow|])\right| \\ &= 4\left|\mathrm{tr}(\overrightarrow{L}.\overrightarrow{S}\,[\rho\otimes S_z])\right| \\ &= 4\left|\mathrm{tr}(\overrightarrow{L}.\overrightarrow{S}\,[\rho\otimes S_z])\right| \\ &= 2\left|\mathrm{tr}(L_z\rho)\right|\end{aligned}$$

where we have used $S_z = 1/2(|\uparrow\rangle\langle\uparrow| - |\downarrow\rangle\langle\downarrow|)$, $\mathrm{tr}(S_z S_{x,y}) = 0$ and $\mathrm{tr}(S_z^2) = 1/2$. Comparing with Eq.(**??**) we find

$$|p_{j+1/2} - q_{j+1/2}| = \frac{2\,|\mathrm{tr}(L_z\rho)|}{2j+1} \tag{A.13}$$

This together with Eq.(A.10) and Eq.(A.6) implies

$$p_{\mathrm{succ}}(\rho) = \frac{1}{2}\left[1 + \frac{|\mathrm{tr}(\rho L_z)|}{j+1/2}\right] \tag{A.14}$$

This completes the proof of proposition 41.

A.3 Characteristic functions and pairwise distinguishability

In this section we discuss about the interpretation of the amplitude of characteristic function of state $\{|\psi\rangle\}$ in terms of the pairwise distinguishability of states in the set $\{U(g)|\psi\rangle : g \in G\}$.

First, note that any measure of the distinguishability of a pair of pure states, $|\alpha_1\rangle$ and $|\alpha_2\rangle$, depends only on the absolute value of their inner product, $|\langle\alpha_1|\alpha_2\rangle|$. This is a consequence of the fact that for two pairs of states, $\{|\alpha_1\rangle\langle\alpha_1|, |\alpha_2\rangle\langle\alpha_2|\}$ and $\{|\beta_1\rangle\langle\beta_1|, |\beta_2\rangle\langle\beta_2|\}$, the condition $|\langle\alpha_1|\alpha_2\rangle| = |\langle\beta_1|\beta_2\rangle|$ implies that it is possible, via a unitary dynamics, to reversibly interconvert between the two pairs, which in turn implies (on the grounds that no processing can increase the distinguishability of a pair of states) that they have the same distinguishability. Moreover using the same type of argument we can easily see that any measure of distinguishability should be monotonically nonincreasing in this overlap. Therefore, for any pair of states $U(g_1)|\psi\rangle$ and $U(g_2)|\psi\rangle$, the distinguishability is specified by $|\langle\psi|U^\dagger(g_1)U(g_2)|\psi\rangle| = |\chi_\psi(g_1^{-1}g_2)|$.

At first glance, therefore, one might think that the Gram matrix for any set of pure states merely encodes the distinguishability of every pair of these states, and therefore, that the characteristic function of a state merely encodes the pairwise distinguishability of the state and every group-transformed version thereof. This is not the case however. Although it is true that if two (covariant) sets are reversibly interconvertible [i.e. they have the same Gram matrix (characteristic function)], then every pair from the first has the same distinguishability as the corresponding pair from the second, the opposite implication fails.

In other words, the information content of the set (in particular its entropy for different probability measures) is not specified by the pairwise distinguishabilities of its elements.

This phenomenon is highlighted by the results of Jozsa and Schlienz [57]. Also, a particularly nice example is provided by a result of Gisin and Popescu concerning the optimal state of two spin-half systems to use for sending a direction in space [59]. Define $|\uparrow_{\hat{n}}\rangle$ and $|\downarrow_{\hat{n}}\rangle$ to be the eigenstates of spin along the $+\hat{n}$ direction, that is, $\hat{n}\cdot\vec{\sigma}|\uparrow_{\hat{n}}\rangle = |\uparrow_{\hat{n}}\rangle$ and $\hat{n}\cdot\vec{\sigma}|\downarrow_{\hat{n}}\rangle = -|\downarrow_{\hat{n}}\rangle$. Then it is shown in [59] that the state $\{|\uparrow_{\hat{n}}\rangle|\downarrow_{\hat{n}}\rangle\}$ is better than $\{|\uparrow_{\hat{n}}\rangle|\uparrow_{\hat{n}}\rangle\}$ for this task when the figure of merit is the fidelity of the estimated direction with the actual sent direction. In other words, they showed that the with respect to this figure of merit the encoding $\{\Omega \to (U(\Omega)\otimes U(\Omega))|\uparrow_{\hat{z}}\rangle|\downarrow_{\hat{z}}\rangle, \Omega \in SO(3)\}$ provides more information about $\Omega\hat{z}$ than the encoding $\{\Omega \to (U(\Omega)\otimes U(\Omega))|\uparrow_{\hat{z}}\rangle|\uparrow_{\hat{z}}\rangle, \Omega \in SO(3)\}$. On the other hand, one can easily check that the amplitudes of the characteristic functions for the two sets, which encode the pairwise distinguishability of elements of the sets, are exactly the same. This follows from the fact that

$$|\chi_{\uparrow\downarrow}(\Omega)| = |\ \langle\uparrow_{\hat{z}}|\langle\downarrow_{\hat{z}}|\left[U(\Omega)\otimes U(\Omega)\right]|\uparrow_{\hat{z}}\rangle|\downarrow_{\hat{z}}\rangle\ | = |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle| \times |\langle\downarrow_{\hat{z}}|U(\Omega)|\downarrow_{\hat{z}}\rangle|$$

and

$$|\chi_{\uparrow\uparrow}(\Omega)| = |\langle\uparrow_{\hat{z}}|\langle\uparrow_{\hat{z}}|\left[U(\Omega)\otimes U(\Omega)\right]|\uparrow_{\hat{z}}\rangle|\uparrow_{\hat{z}}\rangle| = |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle| \times |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle|$$

and the fact that for arbitrary rotation Ω we have $|\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle| = |\langle\downarrow_{\hat{z}}|U(\Omega)|\downarrow_{\hat{z}}\rangle|$.

The insufficiency of the pairwise overlaps within a set of states for specifying the information contained in the set implies that the relevant global properties of the set are encoded in the phases of the components of the Gram matrix, or, in the case of the covariant set of pure states, in the phase of the characteristic function.

One may think that the insufficiency of pairwise distinguishabilities for specifying the content of a set is a quantum phenomenon which does not happen in the classical world. But this is not the case: A simple example (attributed to Peter Shor in Ref. [57]) illustrates the point. Consider a discrete sample space with four elements, and the following two sets of probability distributions: $\{(1/2,1/2,0,0),(1/2,0,1/2,0),(0,1/2,1/2,0)\}$ and $\{(1/2,1/2,0,0),(1/2,0,1/2,0),(0,1/2,0,1/2)\}$. The three distributions in each case are illustrated by the "sausages" in Fig. A.1. It is clear that the pairwise overlaps are the same for the two sets but there are not reversibly interconvertible.

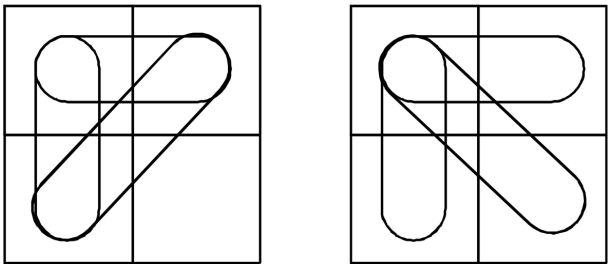

Figure A.1: Example of two ensembles of classical probability distributions that have different information content, but for which the pairwise distinguishability are the same.

A.4 Comparison of classical and quantum characteristic functions

The characteristic function of a quantum state can be understood as a generalization of the characteristic function of a probability distribution. In fact, this generalization was the first motivation for introducing the notion of a characteristic function for a quantum state by Gu [62]. We first review some properties of classical characteristic functions and then we talk about their analogues in the case of quantum states and non-Abelian groups. We also review positive definiteness as the main criterion for a complex function over the group to be the characteristic function of a valid quantum state. Almost all the materials of this appendix are borrowed from [62, 63, 64].

A.4.1 Review of classical characteristic functions

For a real random variable x with the distribution function $F(x)$ the characteristic function is defined as the expectation value of the random variable e^{itx} i.e.

$$f_x(t) = \int dF(x) e^{itx} \tag{A.15}$$

The distribution function is uniquely determined by its characteristic function. Moreover if the probability density exists then it will be equal to the inverse Fourier transform of the characteristic function. One particularly useful property of the characteristic function is the multiplicative property according to which the characteristic function of the sum of two independent random variables is equal to the product of their characteristic functions.

$$f_{x+y}(t) = f_x(t) f_y(t) \tag{A.16}$$

There exists a remarkably simple proof of the central limit theorem using this multiplicative property of characteristic functions.

The derivative of characteristic functions at the origin determines the moments of the random variable.

$$\langle x^n \rangle = i^{-n} \frac{d^n}{dt^n} f_x(t) \mid_{t=0} \tag{A.17}$$

Sometimes it is more favourable to use *cumulants* of the random variable instead where the n-th order cumulant is defined as the n-th order derivative of the logarithm of the characteristic function at the point 0, multiplied by i^{-n}.

$$\kappa^{(n)} \equiv i^{-n} \frac{d^n}{dt^n} \log(f_x(t)) \mid_{t=0} \tag{A.18}$$

The first and second cumulants are mean and variance of the random variable. By this definition, it turns out that cumulants of a sum of independent random variables is equal to the sum of the cumulants of the individual terms for all orders of cumulants.

The set of all classical characteristic functions is determined by Bochner's theorem, according to which a complex function $f(t)$ is the characteristic function of a random variable if and only if 1) $f(0) = 1$, 2) $f(t)$ is continuous at the origin, and 3) it is *positive definite*. Recall that a function $f(t)$ is positive definite if for any integer n and for any string of real numbers $t_1, ..., t_n$ the matrix $a_{i,j} \equiv f(t_i - t_j)$ is a positive definite matrix. Positive definiteness of a function guarantees that the inverse Fourier transform of this function is positive for all values of the random variable, which is clearly a necessary condition for a function to be a probability density.

For more discussion about the properties of characteristic functions of probability distributions, see e.g. [61].

A.4.2 Quantum characteristic functions

As the characteristic function of a probability distribution determines all of its statistical properties, the characteristic function of a quantum state over the group G uniquely specifies all the statistical properties of observables in the algebra of observables which generates the projective unitary representation of G. For example suppose L is the representation of a generator of the Lie group G then we have

$$\mathrm{tr}(\rho L^k) = i^{-k} \frac{\partial^k}{\partial \theta^k} \chi_\rho(e^{i\theta L}) \mid_{\theta=0} \tag{A.19}$$

In particular the first derivative ($k = 1$) determines the expectation value of the generator.This is just property 7 of characteristic functions from Section 6.2.2.

Similarly we can define *cumulants* of the observable L, where the n-th order cumulant is defined as the n-th order derivative of the logarithm of the characteristic function at the identity element multiplied by i^{-n}.

$$\kappa_L^{(n)} \equiv i^{-k} \frac{\partial^k}{\partial \theta^k} \log[\chi_\rho(e^{i\theta L})] \mid_{\theta=0} \tag{A.20}$$

The first and second cumulants are mean and variance of the observable. By this definition, it turns out that the cumulants of the tensor product of two states is equal to the sum of the cumulants of the individual states for all orders of cumulants.

In the rest of this appendix, we are interested to find the generalization of Bochner's theorem i.e. the set of necessary and sufficient conditions for $\phi(g)$ a complex function over group to be the characteristic function of some quantum state. We see that such a generalization can be found via both non-commutative Fourier transform and the Gelfand-Naimark-Segal (GNS) construction theorem. As in the rest of the paper, we focus on the finite groups and compact Lie groups.

As the first necessary condition we note that $\text{tr}(\rho) = 1$ implies that $\chi(e) = 1$ (where e is the identity of group). We call the functions which satisfy this condition *normalized* functions. In the case of compact Lie groups $\phi(g)$ should also be a continuous function. We also need a condition on $\phi(g)$ equivalent to the positivity of density operators. As we just saw in the case of probability distributions the condition of positivity of probabilities is equivalent to the positive definiteness of characteristic function of the probability distribution. Similarly it turns out that the relevant condition on $\phi(g)$ to be the characteristic function of a positive operator is the natural generalization of positive definiteness for the functions defined on the group:

Definition 92 *A complex function $\phi(g)$ on a group G is positive definite if for all choices $m \in \mathbb{N}$, $g_1, ...g_m \in G$ and $\alpha_1, ...\alpha_m \in \mathbb{C}$*

$$\sum_{i,j=1}^{m} \bar{\alpha}_i \alpha_j \phi(g_i^{-1} g_j) \geq 0 \tag{A.21}$$

For the case of compact Lie groups where the function should also be continuous we can express the condition as

Definition 93 *A continuous function $\phi(g)$ on a group G with the Haar measure dg is called positive definite if it satisfies*

$$\int\int dgdh\ \bar{f}(g)\phi(g^{-1}h)f(h) \geq\ 0. \tag{A.22}$$

for any $f \in L^1(G)$.

Now using the Fourier transform, one can easily prove a theorem similar to the Bochner's theorem [62, 63]:

Theorem 94 *A complex function $\phi(g)$ on the finite or compact Lie group G is the characteristic function of a quantum state in a finite dmensional Hilbert space iff $\phi(e) = 1$, $\phi(g)$ is positive definite and continuous (in the case of Lie groups).*

Proof. We present the proof assuming that the group G is a compact Lie group (The same argument works for a finite group by replacing integrals with summation.). We use the inverse Fourier transform. Suppose $B^{(\mu)} \equiv d_\mu \int dg U^{(\mu)}(g^{-1})\phi(g)$. Then the set of operators $\{B^{(\mu)}\}$ is the reduction onto irreps of a valid quantum state iff (1) $\sum_\mu \mathrm{tr}(B^{(\mu)}) = 1$ and (2) all operators $\{B^{(\mu)}\}$ are positive definite. The first condition expresses the fact that the trace of the state is one and is guaranteed by $\phi(e) = 1$. On the other hand, $B^{(\mu)}$ is positive iff $\mathrm{tr}(FF^\dagger B^{(\mu)}) \geq 0$ for all operators F acting on $\mathcal{M}_\mu$ (the subsystem on which U^μ acts irreducibly). Note that $\mathrm{tr}(FF^\dagger B^{(\mu)})$ is equal to the Fourier transform of the operator $FF^\dagger B^{(\mu)}$ at point e. So using the convolution property of characteristic functions, Eq.(6.31), we get

$$\mathrm{tr}(FF^\dagger B^{(\mu)}) = d_\mu^2 \int\int dh_1 dh_2 f(h_1)\overline{f(h_2)}\phi(h_1^{-1}h_2) \tag{A.23}$$

So if $\phi(g)$ is positive definite and therefore satisfies Eq.(A.22) then all $B^{(\mu)}$'s are positive. We can prove the other direction of the theorem similarly. ■

Therefore the set of normalized positive definite functions (also continuous in the case of Lie groups) are exactly the set of characteristic functions of states.

We can also get this result using a more fundamental theorem in the representation theory of C^* algebras, called the GNS construction after Gel'fand, Naimark and Segal. A specific form of this theorem states

Theorem 95 (GNS construction) *With every (continuous) positive definite function $\phi(g)$ we can associate a Hilbert space $\mathcal{H}$, a unitary representation $\{U(g) : g \in G\}$ of G in $\mathcal{H}$ and a vector ψ, cyclic for $\{U(g) : g \in G\}$, such that*

$$\phi(g) = \langle\psi| U(g) |\psi\rangle \tag{A.24}$$

Moreover the representation $\{U(g)\}$ is unique up to a unitary equivalence.

Note that a vector $|\xi\rangle$ is cyclic for the representation $\{U(g) : g \in G\}$ on the space $\mathcal{H}$ if the span of vectors $\{U(g)|\xi\rangle : \ g \in G\}$ is a dense subset of the space $\mathcal{H}$.

Therefore the GNS construction theorem guarantees that for any given (continuous) normalized positive definite function there exists a corresponding pure cyclic state with that characteristic function. Note that for any arbitrary mixed or pure state there exists a pure state which is cyclic (for the representation on its Hilbert space) with exactly the same characteristic function. So the set of all (continuous) normalized, positive definite function is exactly the same as the set of all characteristic functions of states.

A.5 More on the approximate notion of unitary G-equivalence

In this section we prove theorem 54 and present some other versions of this result.

Using the standard bounds between fidelity and trace distance of two operators [17] we can express this result in terms of trace distance of the reductions. For future applications here we present the condition which guarantees the existence of a G-invariant unitary for transforming states to each other in terms of trace distance of reductions.

Corollary 96 *Suppose $\{F_1^{(\mu)}\}$ and $\{F_2^{(\mu)}\}$ are respectively the reductions onto irreps of states $\psi_1, \psi_2 \in \mathcal{H}$. Then there exists a G-invariant unitary V acting on $\mathcal{H}$ such that*

$$|\langle\psi_2|V|\psi_1\rangle| \geq 1 - \frac{1}{2}\sum_{\mu} \|F_1^{(\mu)} - F_2^{(\mu)}\| \tag{A.25}$$

In the following we present a similar bound in terms of the distance between characteristic functions of states $\chi_{\psi_{1,2}}(g)$ and another bound in terms of the distance between

the components of characteristic functions $\{\chi^{(\mu)}_{\psi_{1,2}}(g)\}$ where the μ component of $\chi_{\psi_{1,2}}(g)$ is defined as

$$\begin{aligned}\chi^{(\mu)}_{\psi_{1,2}}(g) &\equiv \mathrm{tr}(U^{(\mu)}(g)F^{(\mu)}_{1,2}) \\ &= d_\mu \ \mathrm{tr}(U^{(\mu)}(g)\int dh U^{(\mu)}(h^{-1})\chi_{\psi_{1,2}}(h)) \\ &= d_\mu \ \left(\varphi_\mu * \chi_{\psi_{1,2}}\right)(g)\end{aligned}$$

where $\varphi_\mu(g) = \mathrm{tr}(U^{(\mu)}(g))$ is the character of irrep μ and $*$ (convolution) is defined in Eq.(6.32).

Corollary 97 *Suppose χ_{ψ_1} and χ_{ψ_2} are respectively the characteristic functions of states ψ_1 and ψ_2. Then there exists a G-invariant unitary V such that*

$$|\langle\psi_2|V|\psi_1\rangle| \geq 1 - \frac{1}{2}(\sum_\mu d_\mu^2)\int dg|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)| \tag{A.26}$$

and

$$|\langle\psi_2|V|\psi_1\rangle| \geq 1 - \frac{1}{2}\sum_\mu d_\mu^2\left(\int dg\ |\chi^{(\mu)}_{\psi_1}(g) - \chi^{(\mu)}_{\psi_2}(g)|\right) \tag{A.27}$$

where the summation is over all irreps in which ψ_1 and ψ_2 have nonzero components.

To prove theorem 54, we first recall a well-known theorem by Uhlmann (see e.g. [18]).

Theorem 98 ***(Uhlmann)*** *Suppose A_1 and A_2 are two positive operators on $\mathcal{H}$. Also suppose $\mathcal{H}'$ is a space large enough such that $\mathcal{H}\otimes\mathcal{H}'$ admits purification of both A_1 and A_2. Suppose for $k \in \{1,2\}$ that $|\alpha_k\rangle$ is a purification of A_k on $\mathcal{H}\otimes\mathcal{H}'$, i.e. $tr_{\mathcal{H}'}(|\alpha_k\rangle\langle\alpha_k|) = A_k$. In this case,*

$$Fid(A_1, A_2) \equiv \|\sqrt{A_1}\sqrt{A_2}\| \tag{A.28}$$

$$= \max\{|\langle\alpha_1|\alpha_2\rangle|, tr_{\mathcal{H}'}(|\alpha_2\rangle\langle\alpha_2|) = A_2\} \tag{A.29}$$

Proof. (theorem 54 and remark 55)

Suppose $\mathcal{M}_\mu \otimes \mathcal{N}_\mu$ is the subspace associated to irrep μ in $\mathcal{H}_1 \oplus \mathcal{H}_2$ and Π_μ is the projective operator to this subspace. Define

$$|\psi^{(\mu)}_{1,2}\rangle \equiv \Pi_\mu|\psi_{1,2}\rangle \tag{A.30}$$

Suppose V is an arbitrary G-invariant unitary. Define $|\widetilde{\psi}\rangle \equiv V|\psi_1\rangle$ and $|\widetilde{\psi}^{(\mu)}\rangle \equiv \Pi_\mu V|\psi_1\rangle$ then

$$|\langle\psi_2|V|\psi_1\rangle| = |\sum_\mu \langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle| \leq \sum_\mu |\langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle| \tag{A.31}$$

Then we have

$$F_{1,2}^{(\mu)} = \mathrm{tr}_{\mathcal{N}_\mu}(|\psi_{1,2}^{(\mu)}\rangle\langle\psi_{1,2}^{(\mu)}|) \tag{A.32}$$

where $F_1^{(\mu)}$ and $F_2^{(\mu)}$ are both operators acting on $\mathcal{M}_\mu$.

The fact that V is G-invariant implies that $|\widetilde{\psi}\rangle$ and $|\psi_1\rangle$ have the same reductions onto irreps, i.e., for all μ

$$\mathrm{tr}_{\mathcal{N}_\mu}(|\widetilde{\psi}^{(\mu)}\rangle\langle\widetilde{\psi}^{(\mu)}|) = \mathrm{tr}_{\mathcal{N}_\mu}(|\psi_1^{(\mu)}\rangle\langle\psi_1^{(\mu)}|) = F_1^{(\mu)} \tag{A.33}$$

Since $|\widetilde{\psi}^{(\mu)}\rangle$ and $|\psi_2^{(\mu)}\rangle$ are purifications of $F_1^{(\mu)}$ and $F_2^{(\mu)}$ according to the Uhlmann's theorem

$$|\langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle| \leq \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \tag{A.34}$$

This inequality together with the inequality (A.31) implies the bound (6.16).

Now we prove this bound is achievable. According to the Uhlmann's theorem there exists a purification of $F_1^{(\mu)}$ shown by $|\phi^{(\mu)}\rangle$ such that

$$\mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) = |\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle| \tag{A.35}$$

But all purifications of $F_1^{(\mu)}$ can be transformed to each other by unitaries acting on $\mathcal{N}_\mu$ (and acting trivially on $\mathcal{M}_\mu$). So there exists a unitary $V^{(\mu)}$ acting on $\mathcal{N}_\mu$ such that $I \otimes V^{(\mu)}|\psi_1^{(\mu)}\rangle = |\phi^{(\mu)}\rangle$. Now define

$$V \equiv \bigoplus_\mu e^{i\theta_\mu} I \otimes V^{(\mu)} \tag{A.36}$$

where $\{e^{i\theta_\mu}\}$ are chosen such that all the numbers $\{e^{i\theta_\mu}\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle\}$ have the same phases. Note that with this definition V is a G-invariant unitary. Then we get

$$|\langle\psi_2|V|\psi_1\rangle| = |\sum_\mu e^{i\theta_\mu}\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle| = \sum_\mu |\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle| \tag{A.37}$$

where the second equality holds because we have chosen $\{e^{i\theta_\mu}\}$ such that all $\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle$ have the same phases. Therefore for this G-invariant unitary we have

$$|\langle\psi_2|V|\psi_1\rangle| = \sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \tag{A.38}$$

This complete the proof of theorem 54. To prove remark 55 we use Eq. (A.35)

$$\begin{aligned}\sum_{\mu} \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) &= \sum_{\mu} |\langle \psi_2^{(\mu)} | \phi^{(\mu)} \rangle| \\ &\leq \sum_{\mu} \sqrt{\langle \psi_2^{(\mu)} | \psi_2^{(\mu)} \rangle} \sqrt{\langle \phi^{(\mu)} | \phi^{(\mu)} \rangle} \\ &\leq \sqrt{\sum_{\mu} \langle \psi_2^{(\mu)} | \psi_2^{(\mu)} \rangle} \sqrt{\sum_{\mu} \langle \phi^{(\mu)} | \phi^{(\mu)} \rangle} = 1\end{aligned}$$

where the both inequalities are implied by the Cauchy-Schwarz inequality and the last equality is implied by the normalization of states. Now we note that the last inequality holds as an equality iff $\forall \mu : \ \langle \psi_2^{(\mu)} | \psi_2^{(\mu)} \rangle = k \langle \phi^{(\mu)} | \phi^{(\mu)} \rangle$ for some constant k. But the normalization of states implies that $\forall \mu : \langle \psi_2^{(\mu)} | \psi_2^{(\mu)} \rangle = \langle \phi^{(\mu)} | \phi^{(\mu)} \rangle = 1$. Furthermore, the first inequality holds as an equality if and only if for each μ there is a constant c_μ such that $|\psi_2^{(\mu)}\rangle = c_\mu |\phi^{(\mu)}\rangle$. These two observations together imply that $\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \leq 1$ and the equality holds only if

$$\forall \mu : \ |\psi_2^{(\mu)}\rangle\langle\psi_2^{(\mu)}| = |\phi^{(\mu)}\rangle\langle\phi^{(\mu)}| \tag{A.39}$$

But $|\psi_2^{(\mu)}$ is a purification of $F_2^{(\mu)}$ and $|\phi^{(\mu)}\rangle$ is a purification of $F_1^{(\mu)}$. So the above equality implies that

$$\forall \mu : \ F_1^{(\mu)} = F_2^{(\mu)} \tag{A.40}$$

This completes the proof of the remark 55. ■

To prove corollary 96, we begin by recalling some facts about the trace distance. For density operators ρ_1 and ρ_2 it is well known that $\|\rho_1 - \rho_2\| \geq 2(1 - \mathrm{Fid}(\rho_1, \rho_2))$ [17, 18]. Using the same argument it can be easily seen that for general positive operators A_1 and A_2, we have the following lemma

Lemma 99 *Suppose A_1 and A_2 are two positive operators. Then*

$$\|A_1 - A_2\| \geq tr(A_1) + tr(A_2) - 2Fid(A_1, A_2) \tag{A.41}$$

We now provide the proof.

Proof. (corollary 96)

According to lemma 99,

$$\mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \geq \frac{1}{2} \left(\mathrm{tr}(F_1^{(\mu)}) + \mathrm{tr}(F_2^{(\mu)}) - \|F_1^{(\mu)} - F_2^{(\mu)}\| \right) \tag{A.42}$$

which implies

$$\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \geq \frac{1}{2}\left(\sum_\mu \mathrm{tr}(F_1^{(\mu)}) + \sum_\mu \mathrm{tr}(F_2^{(\mu)}) - \sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\|\right)$$
$$= 1 - \frac{1}{2}\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\|$$

where we have used the fact that the sum of the trace of the elements of the reduction onto the irreps is one. Combining this bound with theorem 54 we obtain the desired result. ■

Proof. (corollary 97)

According to the Fourier transform Eq. (6.27)

$$F_{1,2}^{(\mu)} = d_\mu \int dg\ U^{(\mu)}(g^{-1})\chi_{\psi_{1,2}}(g) \tag{A.43}$$

Therefore

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| = d_\mu \left\| \left| \int dg\ U^{(\mu)}(g^{-1})\left[\chi_{\psi_1}(g) - \chi_{\psi_2}(g)\right] \right| \right\|$$
$$\leq d_\mu \int dg\ \|U^{(\mu)}(g^{-1})\|\,|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)|$$

Since $U^{(\mu)}(g^{-1})$ is a unitary acting on a d_μ dimensional space then $\|U^{(\mu)}(g^{-1})\| = d_\mu$. So we get

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| \leq d_\mu^2 \int dg\,|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)| \tag{A.44}$$

Therefore we get

$$\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\| \leq \left(\sum_\mu d_\mu^2\right) \int dg|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)| \tag{A.45}$$

where the summation is over all irreps in which ψ_1 and ψ_2 have nonzero components.

The second bound on $\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\|$ is obtained as follows.

Recalling the definition of the μ component of $\chi_{\psi_{1,2}}(g)$, the orthonormality of matrix elements of different irreps implies

$$F_{1,2}^{(\mu)} = d_\mu \int dg\ U^{(\mu)}(g^{-1})\chi_{\psi_{1,2}}^{(\mu)}(g) \tag{A.46}$$

Therefore

$$\begin{aligned}\|F_1^{(\mu)} - F_2^{(\mu)}\| &= d_\mu \| \int dg\ U^{(\mu)}(g^{-1}) \left[\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right] \| \\ &\leq d_\mu \int dg\ \|U^{(\mu)}(g^{-1})\| \left|\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right|\end{aligned}$$

Since $U^{(\mu)}(g^{-1})$ is a unitary acting on a d_μ dimensional space then $\|U^{(\mu)}(g^{-1})\| = d_\mu$. So we get

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| \leq d_\mu^2 \int dg \left|\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right| \tag{A.47}$$

Therefore we get

$$\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\| \leq \sum_\mu d_\mu^2 \int dg\ |\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)| \tag{A.48}$$

where the summation is over all irrep μ in which $F_1^{(\mu)}$ or $F_2^{(\mu)}$ are nonzero. ■

Appendix B

Appendix of part II

B.1 Cost function

Here, we present the average cost function as an example of common figures of merit and we show that it can be accommodated within the framework we introduced in chapter 10.

Suppose that $\mathfrak{s}(\rho)$ is a parameter to be estimated. As described earlier, any estimation scheme, consisting of a choice of measurement and a post-processing of its outcome, can be described by a POVM $M : \sigma(\Omega) \to \mathrm{End}((\mathbb{C}^d)^{\otimes n})$. In this case, the outcome space Ω must correspond to the range of $\mathfrak{s}$. In the following we use the differential notation $M(\mathrm{d}S_{\mathrm{est}})$ to show POVM so that for any interval $\Delta \subseteq \mathbb{R}$

$$M(\Delta) = \int_{\Delta} M(\mathrm{d}S_{\mathrm{est}}) \tag{B.1}$$

Therefore, using the strategy M the conditional probability of outcomes for state ρ will be

$$q_M(\mathrm{d}S_{\mathrm{est}}|\rho) = \mathrm{tr}(M(\mathrm{d}S_{\mathrm{est}})\rho). \tag{B.2}$$

Now suppose that the performance of the estimation scheme will be judged by a cost function (we follow Ref. [10]). The most basic case would be a function of the form $C(S_{\mathrm{est}}, \mathfrak{s}(\rho))$, which represents the cost of estimating S_{est} when the true value of the parameters is $\mathfrak{s}(\rho)$.

The average cost of the estimation strategy M for the state ρ is

$$\overline{C}_M(\rho) \equiv \int C(S_{\mathrm{est}}, \mathfrak{s}(\rho)) \;\; q_M(dS_{\mathrm{est}}|\rho) \tag{B.3}$$

and the expected cost of the estimation strategy M given the prior density p is

$$\langle C \rangle_M \equiv \int d\rho \; p(\rho) \; \overline{C}_M(\rho). \tag{B.4}$$

Therefore,

$$\langle C \rangle_M = \int d\rho \; p(\rho) \int C(S_{\text{est}}, \mathfrak{s}(\rho)) \;\; q_M(dS_{\text{est}}|\rho) = \int \int p(S) \; C(S_{\text{est}}, S) \;\; q_M(dS_{\text{est}}|dS)$$

where S is the random variable defined by the function $\mathfrak{s}$ acting on the random state ρ and $p(S)$ is the density of random variable S relative to dS. So this figure of merit is clearly a functional of $q_M(dS_{\text{est}}|dS)$ and hence the condition of corollary 83 applies. It follows that if the problem has gauge symmetry $G_{\mathcal{A}}$ and satisfies the assumptions of theorem 81 (or theorem 79), then the optimal estimation can be achieved with POVMs restricted to $\mathcal{A}^{\otimes n}$.

References

[1] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. 79, 555 (2007).

[2] I. Marvian, and R.W. Spekkens, quant-ph/1104.0018.

[3] I. Marvian, and R. W. Spekkens, quant-ph/1105.1816.

[4] I. Marvian, and R. W. Spekkens, quant-ph/1112.0638.

[5] I. Marvian, and R. B. Mann, Phys. Rev. A 78, 022304 (2008), quant-ph/0802.0870.

[6] G. Gour, I. Marvian, and R. W. Spekkens, Phys. Rev. A 80, 012307 (2009), quant-ph/0901.0943v2.

[7] J. Preskill, J. Mod. Opt. 47, 127 (2000), quant-ph/9904022.

[8] H. Goldstein, *Classical Mechanics*, 2nd ed. (Reading, MA: Addison-Wesley Publishing, 1980).

[9] E. P. Wigner, *Group Theory* (Academic Press Inc., New York, 1959), pp. 233-236.

[10] G. Chiribella, *Optimal estimation of quantum signals in the presence of symmetry*, (PhD thesis, University of Pavia, Pavia, Italy, 2006), http://www.qubit.it/educational/thesis/ThesisRevised.pdf.

[11] J. F. Cornwell, *Group theory in physics: An introduction*, (Academic Press, 1997).

[12] A. O. Barut and R. Raczka, *Theory of Group Representations and Applications*, (World Scientific, 1986).

[13] R. Goodman, and N. R. Wallach. *Representations and Invariants of the Classical Groups*, (Cambridge University Press, 1998).

[14] V. Giovannetti, S. Lloyd, and L. Maccone, Science 306, 1330 (2004).

[15] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).

[16] G. Gour, and R. W. Spekkens, New J. Phys. 10, 033023 (2008), quant-ph/0711.0043v2.

[17] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[18] John Watrous's lecture notes:
http://www.cs.uwaterloo.ca/~watrous/lecture-notes.html.

[19] John Preskill's lecture notes:
http://www.theory.caltech.edu/~preskill/ph229/.

[20] Chiribella, Marvian, and Spekkens, in preparation.

[21] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (Edizioni della Normale, 2011).

[22] J. A. Vaccaro, F. Anselmi, H. M. Wiseman, and K. Jacobs, Phys. Rev. A 77, 032114 (2008).

[23] N. Schuch, F. Verstraete, and J. I. Cirac, Phys. Rev. A 70, 042310 (2004), quant-ph/0404079.

[24] N. Schuch, F. Verstraete, and J. I. Cirac, Phys. Rev. Lett. 92, 087904 (2004), quant-ph/0310124.

[25] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, New J. Phys. 8, 58 (2006), quant-ph/0602069.

[26] M. Skotiniotis, and G. Gour, quant/ph-1202.3163.

[27] B. Toloui, G. Gour, and B. C. Sanders, Phys. Rev. A 84, 022322 (2011), quant-ph/1104.1144.

[28] G. Vidal, and R. F. Werner, Phys. Rev. A 65, 032314 (2002), quant-ph/0102117.

[29] M. B. Plenio, Phys. Rev. Lett. 95, 090503 (2005), quant-ph/0505071v2.

[30] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A 69, 052326 (2004), quant-ph/0310088.

[31] E. P. Wigner, and M. M. Yanase, Proc. Nat. Acad. Sci. USA 49, 910 (1963).

[32] A. Connes, and E. Stormer, J. Funct. Anal. 28, 187 (1978).

[33] E. H. Lieb, Advances in Math. 11, 267 (1973).

[34] A. Wehrl, Rev. of Mod. Phys. 50, 221 (1978).

[35] E. H. Lieb, and M. B. Ruskai, J. of Math. Phys. 14, 1938 (1973).

[36] E. H. Lieb, and M. B. Ruskai, Phys. Rev. Lett. 30, 434 (1973).

[37] S. Luo, Phys. Rev. Lett. 91, 180403 (2003).

[38] K. Yanagi, S. Furuichi, and K. Kuriyama, IEEE Trans. on Inf. Th. 51, 4401, (2005), quant-ph/0501152.

[39] K. Yanagi, J. of Math. Anal. and App. 365, (2010), quant-ph/1003.3907.

[40] S. Luo, and Q. Zhang, IEEE Trans. on Inf. Th. 50, 1778 (2004).

[41] S. Luo, and Q. Zhang, IEEE Trans. on Inf. Th. 51, 4432 (2005).

[42] S. Luo, and Q. Zhang, J. of Stat. Phys. 114, 1557, (2004).

[43] H. Kosaki, Int. J. of Math. 16, 629 (2005).

[44] M. Hayashi, *Quantum Information: An Introduction*, (Springer 2006).

[45] J. Emerson, R. Alicki, and K. Zyczkowski, J. Opt. B: Quantum and Semiclassical optics, Opt. 7, S347 (2005), quant-ph/0503243.

[46] J. Emerson, M. Silva, O. Moussa, C. A. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, Science 317, 1893 (2007).

[47] J.J. Sakurai, *Modern Quantum Mechanics*, (Addison-Wesley Publishing, 1994).

[48] M. Keyl, and R. F. Werner, J. Math. Phys. **40**, 3283 (1999), quant-ph/9807010v1.

[49] M. Ahmadi, D. Jennings, and T. Rudolph, Phys. Rev. A 82, 032320 (2010), quant-ph/1005.0798.

[50] D. Poulin, and J. Yard, New J. Phys 9, 156 (2007), quant-ph/0612126.

[51] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, New J. Phys. 8, 58 (2006), quant-ph/0602069.

[52] S. D. Bartlett, T. Rudolph, B. C. Sanders, and P. S. Turner, J. Mod. Opt. 54, 2211 (2007), quant-ph/0607107.

[53] J. C. Boileau, L. Sheridan, M. Laforest, and S. D. Bartlett, J. Math. Phys. 49, 032105 (2008), quant-ph/0709.0142.

[54] Y. Aharonov, and T. Kaufherr, Phys. Rev. D 30, 368 (1984).

[55] Y. Aharonov, T. Kaufherr, S. Popescu, and B. Reznik, Phys. Rev. Lett. 80, 2023 (1998).

[56] M. A. Nielsen, Phys. Rev. Lett. 83, 436 (1999), quant-ph/9811053.

[57] R. Jozsa, and J. Schlienz, Phys. Rev. A 62, 012301-1 (1999), quant-ph/9911009v1.

[58] K. Davidson, *C*-algebras by example, Fields Institute Monographs*, (Amer. Math. Soc., Providence, 1996).

[59] N. Gisin and S. Popescu, Phys. Rev. Lett. 83, 432 (1999), quant-ph/9901072v1.

[60] D. Jonathan, M. Plenio, Phys. Rev. Lett. 83, 3566(1999).

[61] B.V. Gnedenko, *The theory of probability*, (Chelsa, New York, 1962).

[62] Y. Gu, Phys. Rev. A 32, 1310 (1985).

[63] J. K. Korbicz, M. Lewenstein, Phys. Rev. A 74, 022318 (2006), quant-ph/0601189.

[64] J. K. Korbicz, J. Wehr, M. Lewenstein, Com. Math. Phys. 281, 753 (2008), quant-ph/0705.2965.

[65] I. Marvian, and R. W. Spekkens, Under preparation.

[66] A. Harrow, *Applications of coherent classical communication and the Schur transform to quantum information theory*, (PhD thesis, MIT, 2005), quant-ph/0512255.

[67] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A 73, 062322 (2006).

[68] P. Zanardi, and M. Rasetti, Phys. Rev. Lett. 79, 3306 (1997);

[69] P. Zanardi, Phys. Rev. A 63, 012301 (2000).

[70] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. 84, 2525 (2000)

[71] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A 63, 042307 (2001).

[72] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. Lett. 91, 027901 (2003).

[73] K. Zyczkowski, and H. J. Sommers, J. Phys. A 34, 7111 (2001), quant-ph/0012101.

[74] C. W. Helstrom, *Quantum detection and estimation theory*, (Academic press,1976).

[75] M. Keyl, and R. F. Werner, Phys. Rev. A 64, 052311 (2001).

[76] C. M. Caves, Phys. Rev. D 26, 1817 (1982).

[77] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. 92, 067902 (2004).