PAPER • OPEN ACCESS

The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations

To cite this article: Iman Marvian and Robert W Spekkens 2013 *New J. Phys.* **15** 033001

New Journal of Physics
The open access journal for physics

The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations

Iman Marvian[1,2,3] **and Robert W Spekkens**[1]

[1] Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada
[2] Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
E-mail: imarvian@gmail.com

New Journal of Physics **15** (2013) 033001 (52pp)
Received 31 October 2012
Published 1 March 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/3/033001

Abstract. If a system undergoes symmetric dynamics, then the final state of the system 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. It follows that for the purpose of understanding the consequences of symmetries of dynamics, in particular, complicated and open-system dynamics, it is useful to introduce the notion of a state's *asymmetry properties*, which includes the type and measure of its asymmetry. We demonstrate and exploit the fact that the asymmetry properties of a state can also be understood in terms of information-theoretic concepts, for instance in terms of the state's ability to encode information about an element of the symmetry group. We show that the asymmetry properties of a pure state ψ relative to the symmetry group G are completely 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. For a symmetry described by a compact Lie group G, we show that two pure states can be reversibly interconverted one to the other by symmetric operations if and only if their characteristic functions are equal up to a one-dimensional representation of the group. Characteristic functions also allow us

[3] Author to whom any correspondence should be addressed.

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.

Contents

1. Introduction

Symmetry arguments are ubiquitous in physics. 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. One of the best known examples of such a result is Noether's theorem, according to which a differentiable symmetry of the Hamiltonian or action entails a conservation law (see e.g. [1]). But there are innumerable results of this sort; symmetry arguments have broad applicability across many fields of physics.

We are interested in determining all the consequences of a symmetry of the dynamics in quantum theory. To find these consequences we ask the following question: given two quantum states, ρ and σ, does there exist a time evolution with the given symmetry such that under this time evolution the first state evolves to the second? Suppose, for instance, that the symmetry under consideration is rotational symmetry. Clearly, rotationally-invariant time evolutions cannot take a rotationally-symmetric state to one that breaks the rotational symmetry. So to answer these types of questions we need to know the extent to which each of the two states breaks the rotational symmetry. It is intuitively clear that there are many different ways in which a quantum state may be asymmetric. For instance, consider a spin-1/2 particle with spin in the $\hat{z}$ direction and another with spin in the $\hat{x}$ direction. Neither is invariant under the full rotation group, but because they point in different directions, they break the rotational symmetry differently. Furthermore, it is intuitively clear that asymmetry must be quantifiable. For instance, the precision with which one can specify a direction in space, a measure of rotational asymmetry, varies with the quantum state one uses to do so.

We will say that two states have exactly the same *asymmetry properties* (with respect to a given symmetry group) if there exists a symmetric time evolution which transforms the first state to the second and a symmetric time evolution which transforms the second state to the first. Thus, the symmetric operations define equivalence classes of states and the asymmetry properties of a state are precisely those that are necessary and sufficient to determine its equivalence class. If the symmetry in question is associated with a representation of the group G, we call the equivalence relation *G-equivalence*. We will consider G-equivalence classes of pure states for the case of arbitrary compact Lie groups and finite groups.

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. However, one can also take an *information-theoretic* perspective on how to define the asymmetry properties of a state. 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.

To understand better the information-theoretic point of view, consider the following scenario: suppose Alice wants to inform Bob about a randomly chosen direction in space. She can prepare a quantum system specifying the direction and send it to Bob. For example, to send a direction in a plane she may prepare a number of photons polarized in that direction. Clearly to transmit more information about this direction, Alice should prepare the quantum system in a state which sharply specifies the chosen direction. Such a state should break the rotational symmetry as much as possible. Again the relevant property of the state which determines its

quality as a pointer can be called its asymmetry. This example suggests that the information-theoretic point of view should be relevant for the study of asymmetry.

We will show that these two approaches to the notion of asymmetry, the constrained-dynamical and the information-theoretic, provide equivalent characterizations of asymmetry. It follows that one can exploit the machinery of information theory for the study of asymmetry and for finding the consequences of symmetry of the dynamics. In this paper, 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.

In the above scenario the quantum system which is sent to Bob to transfer information about direction is called a *quantum reference frame* (see [2] for a review of this topic). The theory of quantum reference frames deals with the problem of using quantum systems to transfer information, such as a direction in space, which is *unspeakable*, i.e. cannot be transferred by sending a sequence of 0's and 1's if two agents do not have access to some shared background reference frame. In other words, unspeakable information can only be encoded in particular degrees of freedom. For example, information about a direction in space cannot be encoded in degrees of freedom that transform trivially under rotations.

Therefore this example suggests that the study of asymmetry is not only useful to learn about the consequences of symmetries of dynamics but it is also useful for the study of quantum reference frames. The relevant property of the state which specifies how well it can act as a quantum reference frame is the asymmetry of the state. Indeed, in previous work, the asymmetry has been called the *frameness* of the state [3, 4]. Therefore all the results about the manipulation of reference frames and their frameness are in fact results about the asymmetry of states. In particular Gour and Spekkens [3] present a systematic study of the manipulation of pure state asymmetry for groups $U(1)$ and Z_2 and also presents some partial results for the case of $SO(3)$. In the present paper, using a different approach based on characterizing the equivalence classes of asymmetries of pure states, we are able to generalize the results in [3] significantly and to extend their scope from a few particular groups to arbitrary compact Lie groups and finite groups.

The main focus of this paper is to characterize the asymmetry of pure states. Another interesting aspect of asymmetry which has been studied previously is the problem of finding *measures of asymmetry* or *asymmetry monotones* [13–15]. An asymmetry monotone is a function from states to real numbers which quantifies the amount of asymmetry of a state relative to a given symmetry group. This notion is mainly inspired by the notion of entanglement monotones in entanglement theory[4].

1.1. 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 must 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 that 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.

[4] Also, earlier related work has considered state-interconversion in the context of bipartite systems where two distant parties are under a $U(1)$-superselection rule motivated by a particle number conservation law [11, 12].

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). 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 [5]. 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 [5]. 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 [6]. 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 this paper, we will show that all the asymmetry properties of a pure state ψ relative to the group G and the 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.

We then proceed to find the complete set of selection rules for pure states under deterministic and stochastic single-copy operations, that is, the necessary and sufficient conditions under which one pure state can be converted to another by a G-covariant operation either deterministically or non-deterministically. These results are the analogues within the resource theory of asymmetry of, respectively, Nielsen's theorem [6] and Vidal's theorem in entanglement theory. Finally, we consider the case of catalysis of asymmetry transformations, wherein a state with asymmetry can be used to assist in the conversion but must be returned intact at the end of the protocol. We show that a finite catalyst is useless in the case of compact connected Lie groups, while in the case of a finite group, there exists for any state interconversion problem a finite catalyst that makes it possible.

1.2. Outline

We now summarize the structure of the paper. In section 2 we review some elementary concepts. We also formally define G-equivalence classes of states. Appendix A includes a short review of projective unitary representations and appendix B includes a discussion about the situations

where the input and output Hilbert space of a time evolution are different. In section 3, we introduce the idea of two dual points of view to asymmetry, constrained-dynamical and information-theoretic. We also show how these two dual points of view arise naturally in the study of quantum reference frames. In section 4, we define the notion of *unitary G-equivalence*, another equivalence relation over states that is slightly stronger than G-equivalence. Using the constrained-dynamical and information-theoretic perspectives, we find two different ways to characterize the unitary G-equivalence classes of states: the characteristic function and the reduction to the irreducible projective unitary representations (irreps). Section 4.3 extends these considerations to the case of *approximate* unitary G-equivalence, in which one state should be transformed to a state that is close to (but not necessarily exactly equal to) a second. The proofs for this section are presented in appendix E.

In section 5, we show that the two different characterizations of the unitary G-equivalence classes are in fact two different representations of the same object, the reduction of the state to the associative algebra and that these representations can be transformed one to the other via Fourier and inverse Fourier transforms. We further outline several nice mathematical properties of the characteristic function of a state, properties which make it particularly useful for the study of the asymmetry of pure states. We also show, in appendix C, that both the amplitude and the phase of the characteristic function are important for specifying the asymmetry of a state, while in appendix D we explain more about characteristic functions and their connection with the classical characteristic function of probability distributions.

In section 6, we present our main result, the characterization of the G-equivalence classes. Specifically, we show that for compact Lie groups, the G-equivalence class of a state is uniquely specified by its characteristic function up to a one-dimensional (1D) representation of the group. In the important case of semi-simple Lie groups, we show that it is uniquely specified by the characteristic function alone.

Finally, the results on single-copy transformations are presented in the three short sections: deterministic transformations in section 7, state-to-ensemble transformations and stochastic transformations in section 9, and catalysis in section 8. We end with a general discussion.

2. 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[5] by Wigner [7] 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 operator $V\rho V^\dagger$ for some unitary or anti-unitary operator V. In this paper 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

$$U(g_2 g_1)\rho U^\dagger(g_2 g_1) = U(g_2)(U(g_1)\rho U^\dagger(g_1))U^\dagger(g_2). \tag{1}$$

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

$$U(g_2 g_1) = \omega(g_2, g_1)U(g_2)U(g_1), \tag{2}$$

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 a *(non-projective) unitary representation*. We provide a short list of some useful properties of projective unitary representations of compact Lie groups and finite groups in appendix A. For a helpful review of this topic we refer to chapter 2 of Giulio Chiribella's thesis [8].

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

$$\mathcal{U}_g(X) = U(g)XU^\dagger(g). \tag{3}$$

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 representations of $SO(3)$ describe systems with different physical properties.

For most symmetries, such as the fundamental symmetries of space–time, the representation of the symmetry on a composite system is the *collective representation*: if the projective unitary representations of a symmetry transformation $g \in G$ on systems with 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 paper we always assume that the representation of the symmetry on the joint system is the collective representation.

[5] **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 states 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.*

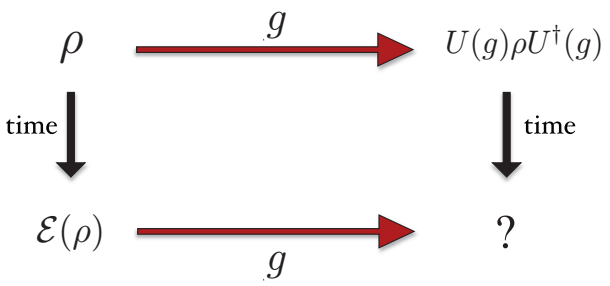

Figure 1. A time evolution is called G-covariant if the above transformations commute for all group elements $g \in G$.

2.1. 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 1. *The symmetry subgroup of a state ρ relative to the group G, denoted* $\mathrm{Sym}_G(\rho)$*, is the subgroup of G under which ρ is invariant,*

$$\mathrm{Sym}_G(\rho) \equiv \{g \in G : \mathcal{U}_g[\rho] = \rho\}. \tag{4}$$

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 non-trivial 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.

$$\forall g \in G : \mathcal{U}_g(\rho) = \rho, \tag{5}$$

then we say that the state is *G-invariant*[6].

2.2. 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 (figure 1)[7]. We will sometimes refer to an operation that is G-covariant as a *symmetric* operation. (It is important not to confuse symmetry transformations, which correspond to a particular group action, with symmetric 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.

[6] 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.

[7] 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.

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

$$\forall g \in G, \quad \forall \rho : VU(g)\rho U^\dagger(g)V^\dagger = U(g)V\rho V^\dagger U^\dagger(g), \tag{6}$$

or equivalently,

$$\forall g \in G : \ [\mathcal{V}, \mathcal{U}_g] = 0, \tag{7}$$

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

$$\forall g \in G : \ VU(g) = U(g)V\omega(g), \tag{8}$$

where $\omega(g)$ is a phase factor that can easily be shown to be a 1D representation of the group. In the case of finite-dimensional Hilbert spaces (which is the case under consideration in this paper), 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) [9].

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

$$\forall g \in G : \ [V, U(g)] = 0. \tag{9}$$

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*[8], 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).

[8] 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 $\mathcal{B}(\mathcal{H}_{\text{out}}) \otimes \mathcal{B}(\mathcal{K})$.

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

Definition 2. (G-covariant operation). *The quantum operation $\mathcal{E}$ is said to be G-covariant if*

$$\forall g \in G: \ \mathcal{E}(U_{\rm in}(g)(\cdot)U_{\rm in}^{\dagger}(g)) = U_{\rm out}(g)\mathcal{E}(\cdot)U_{\rm out}^{\dagger}(g), \tag{10}$$

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

If the input and output spaces are equivalent then the condition of G-covariance can be expressed as

$$\forall g \in G: \ \mathcal{E}\left(U(g)(\cdot)U^{\dagger}(g)\right) = U(g)\mathcal{E}(\cdot)U^{\dagger}(g), \tag{11}$$

or equivalently,

$$\forall g \in G: \ [\mathcal{E}, \mathcal{U}_g] = 0, \tag{12}$$

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

As we demonstrate in appendix B, any G-covariant operation for which the input and output Hilbert spaces are different can always be modeled by one wherein the input and 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, $\mathcal{H}_{\rm in} \bigoplus \mathcal{H}_{\rm out}$, and any operation from $\mathcal{B}(\mathcal{H}_{\rm in})$ to $\mathcal{B}(\mathcal{H}_{\rm out})$ that is G-covariant relative to the representations $\{U_{\rm in}(g)\}$ and $\{U_{\rm out}(g)\}$ can always be extended to an operation on $\mathcal{B}(\mathcal{H}_{\rm in} \bigoplus \mathcal{H}_{\rm out})$ that is G-covariant relative to the representation $\{U_{\rm in}(g) \bigoplus U_{\rm out}(g)\}$.

Similarly, any G-invariant isometry (a reversible operation where the input and output Hilbert spaces may differ) can always be modeled by a G-invariant unitary (where the input and output Hilbert spaces are the same). Again, this is shown in appendix B. It follows that without loss of generality, we can restrict our attention in the rest of this paper 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

$$\mathcal{K} \equiv \int_K \mathrm{d}k \, \mathcal{U}_k, \tag{13}$$

where K is a subgroup of G and $\mathrm{d}k$ is the uniform measure over K. We refer to this as the *uniform twirling over K*.[9] 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 $gKg^{-1} \equiv \left\{gkg^{-1} : k \in K\right\}$. It follows that

$$\forall g \in G: \ \mathcal{U}_g \circ \mathcal{K} \circ \mathcal{U}_{g^{-1}} = \int_K \mathrm{d}k \, \mathcal{U}_{gkg^{-1}} = \mathcal{K}, \tag{14}$$

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

[9] 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.

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.) Here by *proper* subsystem we mean a subsystem which is closed under the action of the symmetry transformations, i.e. under this action any vector in that subsystem is mapped to a vector in the same subsystem.

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. This is sometimes called the Stinespring dilation theorem for G-covariant channels and was first proved in [17].[10] This result provides an operational prescription for realizing every such operation.

In the theory of asymmetry 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 $\rho \xrightarrow{G\text{-cov}} \sigma$ to denote 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 1. *If ρ transforms to σ by a G-covariant quantum operation ($\rho \xrightarrow{G\text{-cov}} \sigma$), then* $\mathrm{Sym}_G(\rho) \subseteq \mathrm{Sym}_G(\sigma)$.

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. This proposition highlights a simple example of restrictions one can put on the final states of a possibly open system dynamics based on the initial state of the system and symmetry of dynamics. For instance, it implies that under rotationally-covariant time evolutions, a spin pointing along $\hat{z}$ cannot evolve to one pointing along $\hat{x}$ because the first state is invariant under the group of rotations around $\hat{z}$ while the second one is not. This result can be understood as a cognate of Curie's principle, which states that symmetric causes cannot have asymmetric effects [18]. Also, note that this proposition suggests a simple characterization of the asymmetry of states relative to a group G by characterizing the largest subgroup of G which leaves each state invariant. Indeed, this simple characterization is very useful, for example, in condensed matter theory. However, finding a more fine-grained characterization of asymmetry of states can also be useful, for example, to study the consequences of symmetry of an open system dynamics.

On the other hand, for any arbitrary pair of G-invariant states ρ and σ there always exist G-covariant channels which transform one to the other. A trivial instance of these G-covariant

[10] A different proof of this is provided in [10].

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

$$\mathcal{E}_\sigma(X) = \mathrm{tr}(X)\sigma. \tag{15}$$

Finding the necessary and sufficient condition to determine for any given pair of states ρ and σ whether $\rho \xrightarrow{G-\mathrm{cov}} \sigma$ or not, turns out to be a hard problem and is still open. However, in this paper, we will answer this question for the special case where both ρ and σ are pure states. In the rest of this section we present two physical examples of channels which are covariant with respect to the group $U(1)$, the group formed by all phases $\{e^{i\theta} : \theta \in (0, 2\pi]\}$.

2.3. 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.

2.3.1. 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 $\{|m\rangle : m \in \{-j, -j+1, \ldots, j\}\}$, 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 $L_z|m\rangle = m|m\rangle$ (taking $\hbar = 1$). Note that in the case of half-integer spins the representation $e^{i\theta} \to e^{i\theta L_z}$ is a projective 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 non-trivial symmetry subgroup because it is invariant under a π phase shift. Meanwhile, all the elements of the basis $\{|m\rangle : m \in \{-j, -j+1, \ldots, j\}\}$ 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 $\{|m\rangle : m \in \{-j, -j+1, \ldots, j\}\}$ basis.

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

$$V_{U(1)\text{-inv}} = \sum_{m=-j}^{j} e^{i\beta_m} |m\rangle\langle m|. \tag{16}$$

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 covariant under rotations around $\hat{z}$, i.e.

$$\forall \theta \in (0, 2\pi]: \ \mathcal{E}(\mathrm{e}^{\mathrm{i}\theta L_z} \rho \, \mathrm{e}^{-\mathrm{i}\theta L_z}) = \mathrm{e}^{\mathrm{i}\theta L_z} \mathcal{E}(\rho) \mathrm{e}^{-\mathrm{i}\theta L_z}. \tag{17}$$

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 $(|m-1\rangle + |m\rangle)/\sqrt{2}$.

2.3.2. Phase-covariant channels in quantum optics. Another physical example of $U(1)$-covariant quantum operations comes from quantum optics (for more discussion see [2]). 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 non-negative integer and α labels possible degeneracies. Then the operator which shifts this oscillator in its cycle by phase θ is $\exp(\mathrm{i}\theta N)$. For example, this operator transforms the coherent state $|\gamma\rangle$ to $|\mathrm{e}^{\mathrm{i}\theta}\gamma\rangle$.

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

$$\forall \theta \in (0, 2\pi]: \ \mathcal{E}(\mathrm{e}^{\mathrm{i}\theta N} \rho \, \mathrm{e}^{-\mathrm{i}\theta N}) = \mathrm{e}^{\mathrm{i}\theta N} \mathcal{E}(\rho) \mathrm{e}^{-\mathrm{i}\theta N}. \tag{18}$$

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 $\mathrm{e}^{\mathrm{i}N\theta}|\psi\rangle = \mathrm{e}^{-\mathrm{i}\theta}|\psi\rangle$; 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 non-negative does not have any impact on the set of operations one can implement—all $U(1)$-covariant operations are still physically accessible [10]. 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[11]. For the rest of this paper, we will assume that all G-covariant operations are physically accessible (including in the quantum optics examples).

[11] This follows from the constructive proof of Stinespring dilations of G-covariant channels presented in [10].

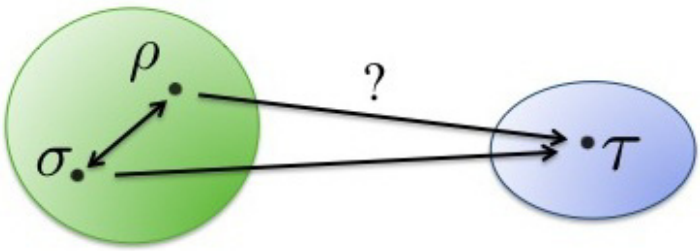

Figure 2. A depiction of two G-equivalence classes in the space of all states. Because both $\rho \xrightarrow{G\text{-cov}} \sigma$ and $\sigma \xrightarrow{G\text{-cov}} \rho$ are possible, ρ and σ are in the same class. It follows that if $\rho \xrightarrow{G\text{-cov}} \tau$ then $\sigma \xrightarrow{G\text{-cov}} \tau$.

3. 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 section we formally define the notion of asymmetry of a state and demonstrate that the asymmetry properties of a state can be understood in terms of information-theoretic concepts.

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 3 (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*

$$\forall g \in G:\ [\mathcal{E}, \mathcal{U}_g] = 0 \quad \text{and} \quad \mathcal{E}[\rho] = \sigma, \tag{19}$$

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

$$\forall g \in G:\ [\mathcal{F}, \mathcal{U}_g] = 0, \quad \text{and} \quad \mathcal{F}[\sigma] = \rho. \tag{20}$$

(Using the notation we introduced in section 2.2, ρ and σ are G-equivalent iff $\rho \xrightarrow{G\text{-cov}} \sigma$ and $\sigma \xrightarrow{G\text{-cov}} \rho$, see figure 2.)

A complete specification of the G-asymmetry properties of a state is achieved by specifying its G-equivalence class. So, for example specifying the 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 1, if ρ can be transformed to σ by a G-covariant quantum operation ($\rho \xrightarrow{G\text{-cov}} \sigma$), then $\mathrm{Sym}_G(\rho) \subseteq \mathrm{Sym}_G(\sigma)$ where $\mathrm{Sym}_G(\rho)$ is the subgroup of G which leaves ρ invariant (see definition 1). So if ρ and σ are G-equivalent, i.e. $\rho \xrightarrow{G\text{-cov}} \sigma$ and $\sigma \xrightarrow{G\text{-cov}} \rho$, then $\mathrm{Sym}_G(\rho) = \mathrm{Sym}_G(\sigma)$.

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 non-zero 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, dynamical concepts provide a useful framework for describing asymmetry. In the next section we show that information-theoretic concepts are also useful for the study of asymmetry.

3.1. Information-theoretic point of view to asymmetry

In this section we introduce another perspective to the notion of asymmetry of states which we call the *information-theoretic* perspective[12]. 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 suggests 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

[12] Recently, a similar information-theoretic argument has been used in [16] to study the duality between the particle and wave natures of quantum systems from the point of view of symmetry and asymmetry.

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 interconvertibility 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 1. *The following statements are equivalent:*

(A) There exists a G-covariant quantum operation $\mathcal{E}_{G\text{-cov}}$ (as defined in equation (11)) 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.

$$\forall g \in G : \ \mathcal{E}(\mathcal{U}_g[\rho]) = \mathcal{U}_g[\sigma]. \tag{21}$$

For pure states, we have

Lemma 2. *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.

$$\forall g \in G : \ VU(g)|\psi\rangle = U(g)|\phi\rangle. \tag{22}$$

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 such that each state in the former set is mapped to its corresponding state in the latter set under this dynamics.

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. This technique has many other applications in the study of asymmetry. For instance, the information-theoretic approach is used in [10] to quantify the amount of asymmetry of states. In this paper 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 of lemma 1. Condition (A) can be seen to imply (B) by taking $\mathcal{E} = \mathcal{E}_{G\text{-cov}}$. To show the reverse, note that (B) implies the existence of a quantum operation $\mathcal{E}$ which satisfies equation (21). Now we can define

$$\mathcal{E}' \equiv \int \mathrm{d}g\, \mathcal{U}_g^\dagger \circ \mathcal{E} \circ \mathcal{U}_g. \tag{23}$$

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

Proof of lemma 2. Condition (A) can be seen to imply (B) by taking $V = V_{G\text{-inv}}$. In the following we prove that (B) also implies (A). Assume there exists a unitary V such that $\forall g \in G$,

$$VU(g)|\psi\rangle = U(g)|\phi\rangle. \tag{24}$$

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

$$\forall g \in G: \; VU(g)\Pi = U(g)V\Pi. \tag{25}$$

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

$$\forall g \in G: \; [V\Pi, U(g)] = 0. \tag{26}$$

The operator $V\Pi$ unitarily maps a subspace of the Hilbert space to another subspace and it commutes with all $\{U(g)\}$. Using lemma B.1 we conclude that this G-invaraint isometry can always be extended to a G-invariant unitary $V_{G\text{-inv}}$ such that $V_{G\text{-inv}}\Pi = V\Pi$ and therefore

$$V_{G\text{-inv}}U(g)|\psi\rangle = V\Pi U(g)|\psi\rangle = U(g)|\phi\rangle. \tag{27}$$

□

3.2. 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 [2] 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.

3.2.1. 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 $\int \mathrm{d}g\, \mathcal{U}_g \circ\ \mathcal{E} \circ \mathcal{U}_g^{\dagger}$. 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.

3.2.2. 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 $\forall g \in G:\ \ \mathcal{E}[\mathcal{U}_g[\rho]] = \mathcal{U}_g[\sigma]$. In other words, from this perspective the interconversion task can be achieved only if every element of the set $\{\mathcal{U}_g[\rho] : g \in G\}$ can be mapped to the corresponding element of $\{\mathcal{U}_g[\sigma] :\ g \in G\}$ by the same 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.

4. Unitary *G*-equivalence

In the previous section 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 4 (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*

$$V_{G\text{-inv}}|\psi\rangle = |\phi\rangle. \tag{28}$$

Recall the two alternative points of view to the notion of asymmetry introduced in the previous section, 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 interconvertibility of the orbits defined by the two states. The equivalence of these two definitions follows trivially from lemma 2.

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, we will show that for semi-simple connected compact Lie groups the unitary G-equivalence classes are the same as the G-equivalence classes.

4.1. The constrained-dynamical characterization: equality of the reductions onto irreducible projective unitary representations (irreps)

We here find a characterization of the unitary G-equivalence classes within the constrained-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 irreps. This suggests the following decomposition of the Hilbert space [2]:

$$\mathcal{H} = \bigoplus_{\mu} \mathcal{M}_\mu \otimes \mathcal{N}_\mu, \tag{29}$$

where μ labels the irreps and $\mathcal{N}_\mu$ is the subsystem associated to the copies of representation μ (the dimension of $\mathcal{N}_\mu$ is equal to the multiplicity of the irrep μ in this representation). Then $U(g)$ can be written as

$$U(g) = \bigoplus_{\mu} U_\mu(g) \otimes \mathbb{I}_{\mathcal{N}_\mu}, \tag{30}$$

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 1. *Two pure states $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if and only if*

$$\forall \mu:\ \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\psi\rangle\langle\psi|\Pi_\mu) = \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\phi\rangle\langle\phi|\Pi_\mu). \tag{31}$$

Proof. First, we find a simple characterization of G-invariant unitaries. It is shown in appendix A that any operator that commutes with all unitaries $U(g)$ has the form of equation (A.3), which implies that any G-invariant unitary is of the form [2],

$$V_{G\text{-inv}} = \bigoplus_{\mu} \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}, \tag{32}$$

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 $V_{G\text{-inv}}$. Then given equation (32), it follows that for all μ,

$$\Pi_\mu|\phi\rangle = \Pi_\mu V_{G\text{-inv}}|\psi\rangle = \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}\Pi_\mu|\psi\rangle. \tag{33}$$

Equation (31) then follows from the cyclic property of the trace and the unitarity of $V_{\mathcal{N}_\mu}$.

Now we prove the converse. If equation (31) 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 $\mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\psi\rangle\langle\psi|\Pi_\mu) = \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu|\phi\rangle\langle\phi|\Pi_\mu)$. 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

$$\mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}\Pi_\mu|\psi\rangle = \Pi_\mu|\phi\rangle \tag{34}$$

(see e.g. [5]). By defining

$$V \equiv \bigoplus_\mu \mathbb{I}_{\mathcal{M}_\mu} \otimes V_{\mathcal{N}_\mu}, \tag{35}$$

we can easily see that V is a G-invariant unitary and moreover $V|\psi\rangle = |\phi\rangle$. This completes the proof. □

For an arbitrary state ρ we call the set of operators $\{\mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu\rho\Pi_\mu)\}$, 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 section 5.1, this is not true for general mixed states.

Example 1. *Recall the quantum optics example studied in section 2.3.2 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*

$$U(\theta) \equiv e^{iN\theta} = \sum_n e^{in\theta} \sum_\alpha |n,\alpha\rangle\langle n,\alpha|, \tag{36}$$

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 1D. 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

$$p_\psi(n) \equiv \langle\psi|\Pi_n|\psi\rangle = \sum_\alpha |\psi_{n,\alpha}|^2, \tag{37}$$

where Π_n is the projector to the eigen-subspace corresponding to the eigenvalue n of N. That is, the reduction onto irreps is the probability distribution over the spectrum of the number operator induced by $|\psi\rangle$. Consequently, two pure states are unitarily $U(1)$-equivalent if and only if they define the same probability distribution over number.

4.2. 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 5 (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*

$$\chi_\rho(g) \equiv \mathrm{tr}\,(\rho U(g))\,. \tag{38}$$

Specifically, we have

Theorem 2. *Two pure states $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if and only if their characteristic functions are equal,*

$$\forall g \in G : \ \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle. \tag{39}$$

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 interconvertibility of sets of pure states. We express the condition for such interconvertibility as a lemma, after recalling the definition of the Gram matrix of a set of states.

Definition 6 (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 3. *There exists a unitary operator V which transforms each member of $\{|\psi_\theta\rangle\}$ to its corresponding member in $\{|\phi_\theta\rangle\}$, 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.*

$$\forall\theta,\theta' : \ \langle\psi_\theta|\psi_{\theta'}\rangle = \langle\phi_\theta|\phi_{\theta'}\rangle.$$

A simple proof of this lemma is provided in the footnote[13].
It is now straightforward to prove theorem 2.

Proof of theorem 2. By definition 4, $|\psi\rangle$ and $|\phi\rangle$ are unitarily G-equivalent if there exists a unitary transformation $V_{G\text{-inv}}$ which takes $|\psi\rangle$ to $|\phi\rangle$. By lemma 2 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 3, 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

$$[X_\phi]_{g_1,g_2} = \langle\phi|U^\dagger(g_1)U(g_2)|\phi\rangle = \omega(g_1^{-1},g_2)\langle\phi|U(g_1^{-1}g_2)|\phi\rangle,$$

[13] The necessity of the equality of the Gram matrices is trivial. Sufficiency is proven as follows. Suppose we use a subset $\{|\psi_{\theta_1}\rangle, |\psi_{\theta_2}\rangle, \ldots\}$ 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.

where we have used 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. Equality of the Gram matrices is equivalent to

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle, \tag{40}$$

and this is simply the statement that the characteristic functions of ψ and ϕ are equal. □

Example 2. *In example 1 we found the characterization of unitary equivalence classes based on 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 non-negative integer eigenvalues. Here, we use the result of lemma 3 to find another characterization of these unitary equivalence classes in terms of characteristic functions of states. In this case, for arbitrary state $|\psi\rangle = \sum_{n,\alpha} \psi_{n,\alpha}|n, \alpha\rangle$, the characteristic function is given by the expectation value of the phase shift operator, i.e.*

$$\chi_\psi(\phi) \equiv \langle\psi|\exp(i\phi N)|\psi\rangle = \sum_n p_\psi(n)e^{in\phi}, \tag{41}$$

where $p_\psi(n) = \sum_\alpha |\psi_{n,\alpha}|^2$ is the reduction onto irreps.

It follows that 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 or for finite groups (which might be non-Abelian) and in these cases as well, it describes the relation between the reduction onto irreps and the characteristic function, as will be shown in section 5.

4.3. 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 in some sense (or equivalently their characteristic functions are close) then there exists a G-invariant unitary which transforms ψ to a state close to ϕ (see appendix E for a discussion about the relevant notion of distance in this context).

Recall that the fidelity of two positive operators A_1 and A_2 is defined as

$$\mathrm{Fid}(A_1, A_2) \equiv \|\sqrt{A_1}\sqrt{A_2}\| = \mathrm{tr}\left(\sqrt{\sqrt{A_1}A_2\sqrt{A_1}}\right), \tag{42}$$

where $\|\cdot\|$ denotes the trace norm.

Theorem 3. *Suppose $\{F_1^{(\mu)}\}$ and $\{F_2^{(\mu)}\}$ are respectively the reductions onto irreps of ψ_1 and ψ_2, two arbitrary pure states in the same Hilbert space. Then for any G-invariant unitary V acting on this space*

$$|\langle\psi_2|V|\psi_1\rangle| \leqslant \sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}). \tag{43}$$

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 1. For $\{F_1^{(\mu)}\}$ and $\{F_2^{(\mu)}\}$ the reductions of an arbitrary pair of states it holds that $\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \leqslant 1$ and the equality holds iff $\forall \mu : F_1^{(\mu)} = F_2^{(\mu)}$. So theorem 3 is a special case of theorem 3.

We present the proof of theorem 3 as well as some other versions of it and the proof of remark 1 in appendix E.

Example 3. *Recall our quantum optics example where the set of all phase shifts forms a representation of the group $U(1)$ (see example 1). Let p_ψ and p_ϕ be the probability distributions over integers which describe the reductions onto irreps of the states ψ and ϕ respectively. Then theorem 3 implies that for any $U(1)$-invariant unitary V,*

$$|\langle\psi|V|\phi\rangle| \leqslant \sum_n \sqrt{p_\psi(n)\, p_\phi(n)} \tag{44}$$

and furthermore there exists a $U(1)$-invariant unitary for which the equality holds.

5. What are the reduction onto irreps and the characteristic function?

We have found two different characterizations of the unitary G-equivalence class 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 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 section.

In appendices C and D we present more discussions about the meaning of characteristic functions of states. In appendix C 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 D 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.

5.1. 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, etc) 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 $\mathrm{Alg}\{O_i\}$. 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 the expectation values of all the operators in $\mathrm{Alg}\{O_i\}$ under the state ρ. The object that contains all and only this information is called the reduction of the state to the associative algebra, denoted $\rho|_{\mathrm{Alg}\{O_i\}}$.

$\mathrm{Alg}\{O_i\}$, considered as a finite-dimensional C^*-algebra, has a unique decomposition (up to unitary equivalence) of the form

$$\bigoplus_J \mathfrak{M}_{m_J} \otimes \mathbb{I}_{n_J}, \tag{45}$$

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 $\mathbb{C}^{n_J}$ [20]. This means that any element A of the algebra can be written as

$$A = \bigoplus_J A^{(J)} \otimes \mathbb{I}_{n_J}, \tag{46}$$

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 $A \in \mathrm{Alg}\{O_i\}$, 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:

$$\mathcal{H} = \bigoplus_J \mathcal{M}_J \otimes \mathcal{N}_J, \tag{47}$$

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

$$\rho^{(J)} \equiv \mathrm{tr}_{\mathcal{N}_J}(\Pi_J \rho \Pi_J). \tag{48}$$

Then for any arbitrary observable A in the algebra we have

$$\mathrm{tr}(A\rho) = \sum_J \mathrm{tr}(A^{(J)} \rho^{(J)}) \tag{49}$$

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 $\rho|_{\mathrm{Alg}\{O_i\}}$.

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.

Decomposition of this algebra in the form of equation (45) in fact coincides with the decomposition of the unitary projective representation $\{U(g) : g \in G\}$ to irreps

$$U(g) \cong \bigoplus_{\mu} U^{(\mu)}(g) \otimes \mathbb{I}_{N_\mu}, \tag{50}$$

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 equation (45). Each irrep index μ appearing in the decomposition of $\{U(g) : g \in G\}$ corresponds to one J in equation (45) 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 equation (48)) is simply the reduction onto the irreps of the state ρ, the generalization to mixed states of the notion defined in the section 4.1, 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 4.2.

To summarize, we have

Remark 2. 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 $\mathrm{Alg}\{U(g) : g \in G\}$ can be represented either in terms of the *reduction onto irreps* of ρ, defined as

$$\{\rho^{(\mu)} \equiv \mathrm{tr}_{\mathcal{N}_\mu}(\Pi_\mu \rho \Pi_\mu)\} \tag{51}$$

(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

$$\chi_\rho(g) \equiv \mathrm{tr}(\rho U(g)). \tag{52}$$

Finally, we note that the relationship between these two representations is the Fourier transform over the group.

Proposition 2. *The characteristic function and reduction onto irreps can be computed one from the other via*

$$\chi_\rho(g) = \sum_\mu \mathrm{tr}(\rho^{(\mu)} U^{(\mu)}(g)) \tag{53}$$

and

$$\rho^{(\mu)} = d_\mu \int \mathrm{d}g\, \chi_\rho(g^{-1}) U^{(\mu)}(g). \tag{54}$$

Proof. The expression for $\chi_\rho(g)$ in terms of $\{\rho^{(\mu)}\}$, equation (53), follows directly from equations (50) and (52). 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. [21]):

$$\int_G \mathrm{d}g\, U^{(\mu)}_{i,j}(g)\overline{U}^{(\nu)}_{k,l}(g) = \frac{\delta_{\mu,\nu}\delta_{i,k}\delta_{j,l}}{d_\mu}, \tag{55}$$

where $\{U^\mu_{i,j}\}$ are the matrix elements of $U^\mu(g)$, $\mathrm{d}g$ is the unique Haar measure on the group, bar denotes the 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 imply that this expansion has a simple form as

$$A^{(\mu)} = d_\mu \int \mathrm{d}g\, U^\mu(g)\,\mathrm{tr}(A^{(\mu)}U^\mu(g^{-1})). \tag{56}$$

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 $\nu \neq \mu$

$$\int \mathrm{d}g\, U^\nu(g)\mathrm{tr}(A^{(\mu)}U^\mu(g^{-1})) = 0 \quad (\nu \neq \mu). \tag{57}$$

Using these orthogonality relations, we obtain equation (54). □

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 section 4.2) 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 $\chi(\theta) = 1/2(1 + \exp(\mathrm{i}\theta))$.

We close this section by mentioning another consequence of the orthogonality relations equation (55) 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

$$\chi_{AB} = d_\mu\, \chi_A * \chi_B, \tag{58}$$

where $*$ is the convolution of two functions[14]

$$f_1 * f_2(g) \equiv \int \mathrm{d}h f_1(gh^{-1}) f_2(h). \tag{59}$$

In particular, since $\mathrm{tr}(AB) = \chi_{AB}(e)$ (where e is the identity of the group) the above formula can be used to find $\mathrm{tr}(AB)$ in terms of the characteristic functions of A and B. Using equation (58) we get

$$\begin{aligned}\mathrm{tr}(AB) = \chi_{AB}(e) &= d_\mu\, [\chi_A * \chi_B](e) \\ &= d_\mu \int \mathrm{d}h\ \chi_A(h)\chi_B(h^{-1}).\end{aligned}$$

5.2. *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 D. Here we simply summarize some useful properties of characteristic functions.

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 D) and normalized (i.e. $\phi(e) = 1$ where e is the identity of the 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,

   $$\chi_{\mathcal{V}_{G\text{-inv}}[\rho]}(g) = \chi_\rho(g),$$

   where $\mathcal{V}_{G\text{-inv}}[\cdot] = V_{G\text{-inv}}(\cdot)V_{G\text{-inv}}^\dagger$ and $[V_{G\text{-inv}}, U(g)] = 0$ for all $g \in G$.
3. Characteristic functions multiply under tensor product,

   $$\chi_{\rho\otimes\sigma}(g) = \chi_\rho(g)\chi_\sigma(g). \tag{60}$$

4. $|\chi_\rho(g)| \leqslant 1$ for all $g \in G$ and $\chi_\rho(e) = 1$ where e is the identity of the 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 1D representation of the group.
7. Suppose L is the representation of a generator of a Lie group on the Hilbert space of a system such that $\{\mathrm{e}^{\mathrm{i}\theta L} : \theta \in (0, 2\pi]\}$ is the representation of a $U(1)$-subgroup of the group. Then we can find all moments of L using the characteristic function

   $$\mathrm{tr}(\rho L^k) = \mathrm{i}^{-k} \frac{\partial^k}{\partial\theta^k} \chi_\rho(\mathrm{e}^{\mathrm{i}\theta L})\ |_{\theta=0}\ . \tag{61}$$

   (Note that by $\chi_\rho(\mathrm{e}^{\mathrm{i}\theta L})$ we really mean $\chi_\rho(g)$ for the group element $g \in G$ which is represented by $\mathrm{e}^{\mathrm{i}\theta L}$.)

[14] Note that for non-Abelian groups $f_1 * f_2$ is not necessarily equal to $f_2 * f_1$.

Proof. Item 1 is proven in appendix D.2. All the rest of these properties can simply be proved by using the definition of the characteristic function, $\chi_\rho(g) = \mathrm{tr}(\rho U(g))$, 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

$$\chi_{\rho\otimes\sigma}(g) = \mathrm{tr}\left(\rho \otimes \sigma U_A(g) \otimes U_B(g)\right) = \mathrm{tr}\left(\rho U_A(g)\right) \mathrm{tr}\left(\sigma U_B(g)\right) = \chi_\rho(g)\chi_\sigma(g).$$

To prove item 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 $U(g_s)|\psi\rangle = \mathrm{e}^{\mathrm{i}\theta}|\psi\rangle$ 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 item 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 $U(g)|\nu\rangle = \mathrm{e}^{\mathrm{i}\theta(g)}|\nu\rangle$ for some phase $\mathrm{e}^{\mathrm{i}\theta(g)}$. It is then clear that $\chi_\rho(g) = \mathrm{e}^{\mathrm{i}\theta(g)}$ and is a 1D representations 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–Gordan 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.

6. *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 compact connected Lie groups, the conditions under which two pure states are G-equivalent can also be stated simply in terms of their characteristic functions, as is shown presently.

Theorem 4. *For G a compact connected 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 1D representation of G, $\mathrm{e}^{\mathrm{i}\Theta(g)}$, such that*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \mathrm{e}^{\mathrm{i}\Theta(g)}\langle\phi|U(g)|\phi\rangle. \tag{62}$$

Since semi-simple compact Lie groups do not have any non-trivial 1D representation, the above theorem implies

Corollary 1. *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.*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle. \tag{63}$$

The above theorem applies only to compact connected Lie groups. By putting a restriction on the states we can prove a similar theorem which applies to both compact Lie groups and finite groups

Theorem 5. *Two pure states $|\psi\rangle$ and $|\phi\rangle$ for which $\langle\psi|U(g)|\psi\rangle$ and $\langle\phi|U(g)|\phi\rangle$ are non-zero 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 1D representation of G, $e^{i\Theta(g)}$, such that*

$$\forall g \in G: \quad \langle\psi|U(g)|\psi\rangle = e^{i\Theta(g)}\langle\phi|U(g)|\phi\rangle. \tag{64}$$

Proof of theorems 4 and 5. The main tool we use in this proof is the Stinespring dilation theorem for G-covariant channels discussed in the preliminaries (see [10] and [17]). According to this result any G-covariant channel can be implemented by preparing an environment in a G-invariant state and coupling it to the system with a G-invariant unitary.

First we prove that equation (62) 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 the environment with characteristic function $e^{i\Theta(g)}$ where by assumption $e^{i\Theta(g)}$ is a 1D representation of the group (such states always exist by virtue of property 1 of characteristic functions listed in section 5.2). Then according to equation (62) and property 3 of characteristic functions (listed in section 5.2), 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 2 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 is clearly 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 1D 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 2 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, that if $|\psi\rangle$ and $|\phi\rangle$ are G-equivalent, then equation (62) follows. By assumption, there exists a G-covariant operation from $|\psi\rangle$ to $|\phi\rangle$ and vice versa. It then follows from the Stinespring dilation theorem that there exists a G-invariant unitary V and a G-invariant pure state $|\eta_1\rangle$ such that

$$V|\psi\rangle|\eta_1\rangle = |\phi\rangle|\eta_2\rangle \tag{65}$$

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

$$V'V|\psi\rangle|\eta_1\rangle|\eta_1'\rangle = |\psi\rangle|\eta_2\rangle|\eta_2'\rangle. \tag{66}$$

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.

$$\chi_\psi \chi_{\eta_1} \chi_{\eta_1'} = \chi_\psi \chi_{\eta_2} \chi_{\eta_2'}. \tag{67}$$

Since $|\eta_1\rangle$ and $|\eta_1'\rangle$ are both G-invariant states the amplitudes of their characteristic functions are always one and so

$$|\chi_\psi| = |\chi_\psi||\chi_{\eta_2}\chi_{\eta_2'}|. \tag{68}$$

Now suppose G is a connected compact Lie group. Then for any state ψ in a finite-dimensional Hilbert space carrying a projective unitary representation of G, $|\chi_\psi|$ is 1 at the identity and is non-vanishing for a neighborhood around the identity in any direction. This implies that $|\chi_{\eta_2}\chi_{\eta_2'}|$ has value 1 for a neighborhood around the identity in any direction. By the analyticity, over the group, of the characteristic functions induced by vectors in a finite-dimensional Hilbert space, 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 equation (65) implies that

$$\chi_\psi(g) = \chi_\phi(g)\mathrm{e}^{\mathrm{i}[\Theta_2(g)-\Theta_1(g)]}, \tag{69}$$

where $\mathrm{e}^{\mathrm{i}\Theta_1(g)}$ and $\mathrm{e}^{\mathrm{i}\Theta_2(g)}$ are respectively the characteristic functions of $|\eta_1\rangle$ and $|\eta_2\rangle$. Finally, because $\mathrm{e}^{\mathrm{i}\Theta_1(g)}$ and $\mathrm{e}^{\mathrm{i}\Theta_2(g)}$ are 1D representations of G, it follows that $\mathrm{e}^{\mathrm{i}[\Theta_2(g)-\Theta_1(g)]}$ is as well. This completes the proof of theorem 4.

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 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 non-zero 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 5. □

Example 4. *Recall our quantum optics example where the set of all phase shifts forms a representation of group $U(1)$ (see example 1). 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 over integers p_ψ and p_ϕ are the reductions onto the irreps of ψ and ϕ respectively, so that the characteristic functions are the Fourier transforms of these. Theorem 4 implies that ψ and ϕ are $U(1)$-equivalent if and only if there exists an integer Δ such that $\sum_n p_\psi(n)\mathrm{e}^{\mathrm{i}n\theta} = \mathrm{e}^{\mathrm{i}\Delta\theta}\sum_n p_\phi(n)\mathrm{e}^{\mathrm{i}n\theta}$, or equivalently, using the Fourier transform, such that*

$$p_\psi(n) = p_\phi(n+\Delta), \tag{70}$$

which is precisely the condition found in [3]. 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 $\chi_\psi(\theta) = \mathrm{e}^{\mathrm{i}2\theta}\chi_\phi(\theta)$ 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 an invariant state $|\eta_1\rangle$ (a non-resource) 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-resources). 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.

7. Deterministic transformations

In this section we find the necessary and sufficient condition to determine whether a pure state ψ can be transformed to a pure state 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 6. *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 the group G such that $\chi_\psi(g) = \chi_\phi(g) f(g)$ for all $g \in G$.*

Note that if χ_ϕ is non-zero 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 D.2 one can test positive definiteness of $f(g)$ by verifying that the set of operators defining its Fourier transform are all positive.

Proof of theorem 6. As in the proof of theorems 4 and 5, the main tool we use in this proof is the Stinespring dilation theorem discussed in the preliminaries (see [10] and [17]). By this result we know that the transformation can be achieved 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, we require

$$\chi_\psi(g)\mathrm{e}^{\mathrm{i}\Theta(g)} = \chi_\varphi(g)\chi_\nu(g), \tag{71}$$

where $\mathrm{e}^{\mathrm{i}\Theta(g)}$ is a 1D 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 $\chi_\psi(g) = \chi_\varphi(g)\left[\chi_\nu(g)\mathrm{e}^{-\mathrm{i}\Theta(g)}\right]$. Since $\chi_\nu(g)$ and $\mathrm{e}^{-\mathrm{i}\Theta(g)}$ are both positive definite, so is their product (see appendix D). This proves one direction of the theorem. To prove the other direction, suppose there exists 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 4 and 5) 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 imply that there exist normalized positive definite functions f_1 and f_2 such that $\chi_\psi(g) = \chi_\phi(g) f_1(g)$ and $\chi_\phi(g) = \chi_\psi(g) f_2(g)$. Substituting the second equation into the first, we have

$$\chi_\psi(g) = \chi_\psi(g) f_1(g) f_2(g), \tag{72}$$

and so if $\chi_\psi(g)$ is non-zero for all group elements it follows that $\forall g \in G : f_1(g) f_2(g) = 1$. Given that $\forall g \in G : |f_1(g)|, |f_2(g)| \leqslant 1$ (because the absolute value of a positive definite function at any g is always less than or equal to its absolute value at e and $f_1(e), f_2(e) = 1$ by virtue of equation (72)), we infer that $\forall g \in G : |f_1(g)|, |f_2(g)| = 1$. It follows therefore that f_1 and f_2 are 1D representations of the group, which is the content of theorem 5. One can prove theorem 4 similarly for the case of connected compact Lie groups.

In the following we present two examples, corresponding to the groups $U(1)$ and Z_N.

7.1. *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 1). According to theorem 6 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

$$\chi_\psi(\theta) = f(\theta) \chi_\phi(\theta). \tag{73}$$

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 probability distributions over integers p_ψ and p_ϕ are the Fourier transforms of χ_ψ and χ_ϕ respectively. Then the Fourier transform of equation (73) yields

$$p_\psi(n) = \sum_k p_\phi(n-k) q(k). \tag{74}$$

So the $U(1)$-covariant transformation from ψ to ϕ exists iff there exists a probability distribution q over integers which satisfies the above equality. This is indeed the condition for deterministic interconversion in the $U(1)$ case found in [3].

7.2. *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 $\{0, \ldots, N-1\}$ where the group action is addition modulo N. We use this isomorphism to denote the group elements. These groups are clearly Abelian and so all of their irreps are 1D. We can easily see that these irreps can be identified by an integer J in the set $\{0, \ldots, N-1\}$ such that the irrep labeled by J is

$$k \in Z_N \to U_J(k) = \mathrm{e}^{\mathrm{i}2\pi Jk/N}. \tag{75}$$

So an arbitrary (non-projective) unitary representation of Z_N, $k \in Z_N \to U(k)$, can be decomposed as

$$U(k) = \bigoplus_{J,\alpha} \mathrm{e}^{\mathrm{i}Jk2\pi/N} |J, \alpha\rangle\langle J, \alpha|, \tag{76}$$

where α labels copies 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

$$|\psi\rangle = \sum_{J,\alpha} \psi(J,\alpha)|J,\alpha\rangle. \tag{77}$$

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

$$\{p_\psi(J) \equiv \sum_{\alpha} |\psi(J,\alpha)|^2 : J = 0,\ldots,N\}.$$

On the other hand, the characteristic function of ψ is by definition the function $k \in \{0,\ldots,N-1\} \to \langle\psi|U(k)|\psi\rangle$, that is,

$$\chi_\psi(k) = \sum_{J,\alpha} |\psi(J,\alpha)|^2 \, \mathrm{e}^{\mathrm{i}2\pi Jk/N}. \tag{78}$$

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, $\chi_\phi(k)$, is non-zero for all k's, it follows from theorem 6 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

$$q(J) \equiv \sum_{k} \frac{\chi_\psi(k)}{\chi_\phi(k)} \mathrm{e}^{\mathrm{i}2\pi Jk/N} \tag{79}$$

is positive for all $J = 0,\ldots,N$. So to summarize, the necessary and sufficient condition for the existence of a Z_N-covariant channel which transforms ψ to ϕ is that

$$\forall J \in \{0,\ldots,N\}: \quad \sum_{k} \frac{\chi_\psi(k)}{\chi_\phi(k)} \mathrm{e}^{\mathrm{i}2\pi Jk/N} \geqslant 0. \tag{80}$$

Consider the case of Z_2 which has only two group elements denoted by $\{e,\pi\}$ where e is the identity of the 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 non-trivial ($J = 1$) 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 because 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

$$\chi_\psi(k) = p_\psi(J = 0) + (-1)^k p_\psi(J = 1). \tag{81}$$

So $\chi_\psi(0) = 1$ and $\chi_\psi(1) = 2p_\psi(J = 0) - 1$. Then equation (80) implies that the transformation $\psi \xrightarrow{G\text{-cov}} \phi$ is possible iff

$$q(0) = \frac{\chi_\psi(0)}{\chi_\phi(0)} + \frac{\chi_\psi(1)}{\chi_\phi(1)} \geqslant 0 \tag{82}$$

and

$$q(1) = \frac{\chi_\psi(0)}{\chi_\phi(0)} - \frac{\chi_\psi(1)}{\chi_\phi(1)} \geqslant 0. \tag{83}$$

Since $\frac{\chi_\psi(0)}{\chi_\phi(0)}$ is always equal to one it turns out that the above two inequalities are equivalent to $|\chi_\psi(1)| \leqslant |\chi_\phi(1)|$, i.e.

$$\left|p_\psi(J=0) - p_\psi(J=1)\right| \leqslant \left|p_\phi(J=0) - p_\phi(J=1)\right|. \tag{84}$$

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

$$\min\{p_\phi(J=0),\, p_\phi(J=1)\} \leqslant \min\{p_\psi(J=0),\, p_\psi(J=1)\} \tag{85}$$

which is exactly the same condition previously obtained in [3] using a totally different approach. Equation (80) is the generalization of this specific result for arbitrary cyclic group Z_N.

8. 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 catalyst [23].

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 the process.

We shall say that the conversion ψ to ϕ is a non-trivial 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 a non-trivial 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 transformation which takes ψ to ϕ. Then from theorem 6 we know that if there is no G-covariant transformation from ψ to ϕ then there is no analytic positive definite function f over the group G that satisfies

$$\forall g \in G:\ \chi_\psi(g) = \chi_\phi(g) f(g). \tag{86}$$

On the other hand, if this transformation is possible using a catalyst ζ with characteristic function χ_ζ then there should exist an analytic positive definite function f' such that

$$\forall g \in G: \chi_\psi(g)\chi_\zeta(g) = \chi_\phi(g)\chi_\zeta(g) f'(g). \tag{87}$$

Now clearly for all points $g \in G$ for which $\chi_\zeta(g) \neq 0$, equation (87) 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 transforms ψ to ϕ, in contradiction with our assumption. This argument shows that the role of a catalyst is specified by the elements of the group at which the characteristic function of the catalyst is zero; for these specific group elements, although $\chi_\psi(g) \neq \chi_\phi(g) f'(g)$, nonetheless $\chi_\psi(g)\chi_\zeta(g) = \chi_\phi(g)\chi_\zeta(g) f'(g)$. This argument shows that there is an important distinction between the cases of compact connected Lie groups and finite groups or Lie groups which are not connected.

8.1. Compact connected Lie groups

In the case of compact connected 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 catalyst, it is also possible without any catalyst. To see this, first note that for any finite-dimensional representation of a compact Lie group there is a neighborhood around the identity element of the group within which the characteristic functions of all pure states are non-zero (otherwise there would be a unitary which is arbitrarily 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 equation (87) holds then the following equation holds:

$$\chi_\psi(g) = \chi_\phi(g) f'(g). \tag{88}$$

But since all these functions are analytic and since the group G is connected, if the above equality is true for a neighborhood around the identity element of G then it will be true for all G. Then by theorem 6 we can conclude that there exists a G-covariant channel which transforms ψ to ϕ (without the 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 7. *For symmetries associated with compact connected Lie groups, there are no examples of non-trivial catalysis using a finite catalyst.*

8.2. Finite groups

The above argument clearly does not work in the case of finite groups. Indeed, as we will see in the following, in the case of finite groups there are states for which the characteristic function is zero for all $g \in G$ except the identity. If we use such a state as a catalyst, equation (87) holds for all group elements and consequently for any pair of states ψ and ϕ, one can always transform one to the other using the catalyst. (Indeed as we show in the following one can always transform any mixed state to any other mixed state using such a catalyst.)

For a group with a finite number of elements, it is possible for the catalyst to consist of a system with a Hilbert space $\mathcal{H}$ having dimension greater than or equal to the order of the group. In this case, the representation of the group can be the left regular representation on the Hilbert space $\mathcal{H}$, $g \to T_{\mathrm{L}}(g)$, such that

$$\forall g \in G: \quad T_{\mathrm{L}}(g)|h\rangle = |gh\rangle, \tag{89}$$

where $\{|h\rangle : h \in G\}$ is an orthonormal basis for $\mathcal{H}$. Now note that the characteristic function of any state $|h\rangle$ is $\chi_h(g) = \langle h|T_L(g)|h\rangle = \delta_{e,g}$, the Kronecker-delta function centered on the identity group element. Equation (87) then implies that such a state can catalyze any pure-to-pure transformation.

Also it is straightforward to show that for any pair of states ρ and σ (pure or mixed) there exists a G-covariant channel which transforms $\rho \otimes |h\rangle\langle h|$ to $\sigma \otimes |h\rangle\langle h|$. One realization of this G-covariant map is the following:

$$\mathcal{E}_h(X) \equiv \sum_{g\in G} \mathrm{tr}\left([\mathbb{I} \otimes |g\rangle\langle g|]\, X\right) U(gh^{-1})\sigma U^\dagger(gh^{-1}) \otimes |g\rangle\langle g|, \tag{90}$$

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 of ρ.[15]

So unlike the case of connected compact Lie groups, in the case of a symmetry described by a finite group, catalysts can be helpful.

9. 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 operations. We are interested to know whether it is possible to transform a given state ψ to the state ϕ_i, $i = 1, \ldots, N$ 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 8. *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*

$$\chi_\psi(g) = \sum_i p_i f_i(g)\chi_{\phi_i}(g). \tag{91}$$

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 2. *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.*

These results are proven at the end of the section.

[15] This fact can be made intuitive by imagining that the restriction to G-covariant operations results from one party, Bob, lacking a shared reference frame with another party, Alice. In this case, our interconvertibility problem is described as follows: Alice sends to Bob a pair of systems which are described by the state $\rho \otimes |h\rangle\langle h|$ relative to her frame and asks him to transform these to $\sigma \otimes |h\rangle\langle h|$, again relative to her frame. One can think of the second system as a token of Alice's reference frame. Because the group is finite, Bob can simply measure $\{|g\rangle\langle g| : g \in G\}$ on the token and determine precisely the relationship between their reference frames. Thereafter, he can perform any operation relative to Alice's frame. In other words, for finite groups, the fact that one can prepare a perfect token of a reference frame using a finite-dimensional system is equivalent to the fact that one can find a finite-dimensional catalyst that makes possible any state transformation.

9.1. 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 1). Let $\mathrm{Irreps}_{\mathrm{U}(1)}(\psi)$ be the set of eigenvalues of the number operator N to which the pure state ψ assigns non-zero weight. Assuming that ψ can be transformed to ϕ with non-zero probability under a $U(1)$-covariant operation, one can easily show that

1. the cardinality of $\mathrm{Irreps}_{\mathrm{U}(1)}(\psi)$ is larger than or equal to the cardinality of $\mathrm{Irreps}_{\mathrm{U}(1)}(\phi)$, i.e.

$$\left|\mathrm{Irreps}_{\mathrm{U}(1)}(\phi)\right| \leqslant \left|\mathrm{Irreps}_{\mathrm{U}(1)}(\psi)\right|, \tag{92}$$

2. $$\max\{\mathrm{Irreps}_{\mathrm{U}(1)}(\phi)\} - \min\{\mathrm{Irreps}_{\mathrm{U}(1)}(\phi)\} \leqslant \max\{\mathrm{Irreps}_{\mathrm{U}(1)}(\psi)\} - \min\{\mathrm{Irreps}_{\mathrm{U}(1)}(\psi)\}.$$

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 non-zero component of $\mathrm{e}^{\mathrm{i}m\theta}$ 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 $\mathrm{e}^{\mathrm{i}m\theta}$ will be positive. This implies that for any non-zero probability p, the coefficient of $\mathrm{e}^{\mathrm{i}m\theta}$ 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 non-zero p. This proves the claim. Item 1 is proven similarly.

Item 2 was obtained by a different argument in [3].[16]

9.2. Example: $SO(3)$-covariant stochastic maps

Let $\mathrm{Irreps}_{SO(3)}(\psi)$ be the set of all angular momentum quantum numbers j corresponding to irreps of $SO(3)$ to which the pure state ψ assigns non-zero weight.

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 $\mathrm{Irreps}_{SO(3)}(\psi)$ is larger than or equal to the cardinality of $\mathrm{Irreps}_{SO(3)}(\phi)$, i.e.

$$\left|\mathrm{Irreps}_{SO(3)}(\phi)\right| \leqslant \left|\mathrm{Irreps}_{SO(3)}(\psi)\right|, \tag{93}$$

2. $$\max\{\mathrm{Irreps}_{SO(3)}(\phi)\} - \min\{\mathrm{Irreps}_{SO(3)}(\phi)\} \leqslant \max\{\mathrm{Irreps}_{SO(3)}(\psi)\} - \min\{\mathrm{Irreps}_{SO(3)}(\psi)\},$$

3. $$\max\{\mathrm{Irreps}_{SO(3)}(\phi)\} \leqslant \max\{\mathrm{Irreps}_{SO(3)}(\psi)\}. \tag{94}$$

The proofs of items 1 and 2 are similar to the case of $U(1)$. To prove item 3 note that the maximum value of j to which $\chi_\phi(\theta) f(\theta)$ assigns non-zero weight is greater than or equal to $j_{\max}(\phi)$. So if $j_{\max}(\phi)$ is strictly greater than $j_{\max}(\psi)$, then for any non-zero 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 non-zero

[16] The set $\mathrm{Irreps}_{\mathrm{U}(1)}(\phi)$ was called the 'number spectrum' of ϕ in [3].

probability to another pure state which assigns some amplitude to an angular momentum higher than j.

9.3. *Proof of theorem 8*

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 $\mathcal{H}_{\text{in}}$) unitarily interacts with an ancillary system (with Hilbert space $\mathcal{H}_{\text{anc}}$). Now we consider the total Hilbert space $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{anc}}$ as

$$\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{anc}} = \bigoplus_i \mathcal{H}_i \otimes \mathcal{H}'_i \otimes |i\rangle\langle i|. \tag{95}$$

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

$$V|\psi\rangle|\nu\rangle = \sum_i \sqrt{p_i}|\phi_i\rangle|\eta_i\rangle|i\rangle, \tag{96}$$

where $|\psi\rangle$ is the initial state of the system and $|\nu\rangle$ is the initial state of the ancilla.

Now according to an extension of Stinespring's dilation theorem for G-covariant quantum operations, if the state-to-ensemble transformation is G-covariant then one can choose the initial state $|\nu\rangle$ of ancilla, the unitary V, and the basis $\{|i\rangle\}$ to all be G-invariant [17] .

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

$$\chi_\psi(g)\mathrm{e}^{\mathrm{i}\theta(g)} = \sum_i p_i \chi_{\nu_i}(g)\chi_{\phi_i}(g)\mathrm{e}^{\mathrm{i}\alpha_i(g)}, \tag{97}$$

where $\mathrm{e}^{\mathrm{i}\theta(g)}$ is the characteristic function of the G-invariant ancilla $|\nu\rangle$ and $\{\mathrm{e}^{\mathrm{i}\alpha_i(g)}\}$ are the characteristic functions of the G-invariant states $\{|i\rangle\}$. Now because the product of two characteristic functions is also a characteristic function, $\chi_{\nu_i}(g)\mathrm{e}^{\mathrm{i}\alpha_i(g)}\,\mathrm{e}^{-\mathrm{i}\theta(g)}$ 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 (91) 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 listed in section 5.2 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 1 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 1. Then, equation (91) 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.

Acknowledgments

We thank Sarah Croke for a discussion about Gram matrices, Giulio Chiribella for a discussion about Noether's theorem and Gilad Gour for general discussions. Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. IM is supported by a Mike and Ophelia Lazaridis fellowship.

Appendix A. Short review of projective unitary representations

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

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 a 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 non-zero 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 cocycle, i.e. $U(g_1)U(g_2) = \omega(g_1, g_2)U(g_1g_2)$ and $V(g_1)V(g_2) = \omega(g_1, g_2)V(g_1g_2)$ for a cocycle $\omega(g_1, g_2)$ are said to be in the same *factor system*.

Theorem A.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:

$$\mathcal{H} = \bigoplus_\mu \mathcal{M}_\mu \otimes \mathcal{N}_\mu, \tag{A.1}$$

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 copies of representation μ (the dimension of $\mathcal{N}_\mu$ is equal to the multiplicity of the irrep μ in this representation). Then $U(g)$ can be written as

$$U(g) = \bigoplus_\mu U_\mu(g) \otimes \mathbb{I}_{\mathcal{N}_\mu}, \tag{A.2}$$

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:

$$A = \bigoplus_{\mu} \mathbb{I}_{\mathcal{M}_\mu} \otimes A_{\mathcal{N}_\mu}, \tag{A.3}$$

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

Theorem A.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:*

$$\int_G \mathrm{d}g\ U^{(\mu)}_{i,j}(g)\overline{U}^{(\nu)}_{k,l}(g) = \frac{\delta_{\mu,\nu}\delta_{i,k}\delta_{j,l}}{d_\mu}, \tag{A.4}$$

where $\mathrm{d}g$ 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 the 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[17]. 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.

[17] To see this, first note that by redefining the cocycle one can always choose the unitaries $\{U(g)\}$ to have determinant equal to one. Then by looking at the determinant of both sides of equation (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 the representation and so the values of $\omega(g_1, g_2)$ are 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.

Appendix B. Input–output Hilbert spaces

In general the input and output Hilbert space of a time evolution are not the same ($\mathcal{H}_{\rm in} \neq \mathcal{H}_{\rm out}$). 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 ($\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out}$) 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 time evolution of the extended system 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 $\{U_{\rm in}(g) : g \in G\}$ and $\{U_{\rm out}(g) : g \in G\}$. Suppose the time evolution is G-covariant, i.e. $\mathcal{E} \circ \mathcal{U}_{\rm in}(g) = \mathcal{U}_{\rm out}(g) \circ \mathcal{E}$ 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 $\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out}$ such that this extended time evolution respects the natural representation of G on $\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out}$ given by $\{U_{\rm in}(g) \oplus U_{\rm out}(g) : g \in G\}$. 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.

B.1. General G-covariant channels

Suppose $\mathcal{E}$ is a channel (completely-positive trace-preserving linear map) from $\mathcal{B}(\mathcal{H}_{\rm in})$ to $\mathcal{B}(\mathcal{H}_{\rm out})$ which is G-covariant, i.e. for all $g \in G$ we have $U_{\rm out}(g)\mathcal{E}[\cdot]U_{\rm out}^{\dagger}(g) = \mathcal{E}(U_{\rm in}(g)[\cdot]U_{\rm in}^{\dagger}(g))$. Then we can always extend this channel to $\tilde{\mathcal{E}}$, a G-covariant channel from $\mathcal{B}(\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out})$ to itself, by defining

$$\tilde{\mathcal{E}} \equiv \mathcal{E}(\Pi_{\rm in}[\cdot]\Pi_{\rm in}) + \frac{I_{\mathcal{H}_{\rm in}\oplus\mathcal{H}_{\rm out}}}{d_{\rm in} + d_{\rm out}} \mathrm{tr}(\Pi_{\rm out}[\cdot]\Pi_{\rm out})m, \tag{B.1}$$

where $I_{\mathcal{H}_{\rm in}\oplus\mathcal{H}_{\rm out}}/(d_{\rm in} + d_{\rm out})$ is the completely mixed state on $\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out}$. 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 $\mathcal{H}_{\rm in}$, i.e. $\tilde{\mathcal{E}}(\Pi_{\rm in}[\cdot]\Pi_{\rm in})$, is equal to $\mathcal{E}(\cdot)$.

On the other hand, if there is a G-covariant channel from $\mathcal{B}(\mathcal{H}_{\rm in} \oplus \mathcal{H}_{\rm out})$ to itself which maps all operators in $\mathcal{B}(\mathcal{H}_{\rm in})$ to operators in $\mathcal{B}(\mathcal{H}_{\rm out})$ then clearly by restricting its input to $\mathcal{B}(\mathcal{H}_{\rm in})$ we get a valid G-covariant channel from $\mathcal{B}(\mathcal{H}_{\rm in})$ to operators in $\mathcal{B}(\mathcal{H}_{\rm out})$.

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 the group G on the Hilbert space is $\{U(g) : g \in G\}$. Define $\Pi_{\rm in}$ and $\Pi_{\rm out}$ 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 $\Pi_{\rm in}$ and $\Pi_{\rm out}$ commute with all $\{U(g) : g \in G\}$. Therefore the subspaces associated to these projectors, $\mathcal{H}_{\rm in}$ and $\mathcal{H}_{\rm out}$, have a natural representation of the group G given by $\{\Pi_{\rm in}U(g)\Pi_{\rm in}\}$ and $\{\Pi_{\rm out}U(g)\Pi_{\rm out}\}$. Now $\tilde{\mathcal{E}} \equiv \mathcal{E}(\Pi_{\rm in}[\cdot]\Pi_{\rm in})$ is a new G-covariant quantum channel which maps states from $\mathcal{B}(\mathcal{H}_{\rm in})$ to $\mathcal{B}(\mathcal{H}_{\rm out})$ and $\tilde{\mathcal{E}}(\rho_i) = \sigma_i$.

B.2. G-invariant unitaries and G-invariant isometries

Basically we can repeat all of these observations to prove the equivalence of a G-invariant unitary where the input and output spaces are the same and a G-invariant isometry where the input and output 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 $\forall g \in G : V U_{\text{in}}(g) = U_{\text{out}}(g) V$ 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 following: suppose V is an isometry from H_{in} to H_{out} which is G-invariant i.e. $\forall g \in G : V U_{\text{in}}(g) = U_{\text{out}}(g) V$. Then there exits a unitary V_{ext} on $\mathcal{H}_{\text{in}} \oplus \mathcal{H}_{\text{out}}$ such that $\forall g :\in G : V_{\text{ext}}(U_{\text{in}}(g) \oplus U_{\text{out}}(g)) = (U_{\text{in}}(g) \oplus U_{\text{out}}(g)) V_{\text{ext}}$ and moreover $V = \Pi_{\text{out}} V_{\text{ext}} \Pi_{\text{in}}$ where $\Pi_{\text{in/out}}$ is the projector to $\mathcal{H}_{\text{in/out}}$. This is shown by the following lemma.

Lemma B.1. *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 $W_{G\text{-inv}}$ such that $\forall g \in G : [W_{G\text{-inv}}, U(g)] = 0$ and $W_{G\text{-inv}} \Pi = W \Pi$.*

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 irreps,

$$U(g) = \bigoplus_\mu U_\mu(g) \otimes I_{\mathcal{N}_\mu}. \tag{B.2}$$

Since Π commutes with all $\{U(g) : g \in G\}$ it has a simple form in this basis:

$$\Pi = \bigoplus_\mu I_\mu \otimes \Pi^{(\mu)}, \tag{B.3}$$

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:

$$W\Pi = \bigoplus_\mu I_\mu \otimes (W^{(\mu)} \Pi^{(\mu)}). \tag{B.4}$$

$\Pi W^\dagger W \Pi = \Pi$ implies that ${\Pi^{(\mu)}} {W^{(\mu)}}^\dagger W^{(\mu)} \Pi^{(\mu)} = \Pi^{(\mu)}$. Therefore $W^{(\mu)} \Pi^{(\mu)}$ acts unitarily 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

$$W_{G\text{-inv}} = \bigoplus_\mu I_\mu \otimes \tilde{W}^{(\mu)}. \tag{B.5}$$

Clearly it commutes with all $\{U(g)\}$ and $\tilde{W}\Pi = W\Pi$. □

Appendix C. Characteristic functions and pairwise distinguishability

In this section we discuss the interpretation of the amplitude of the characteristic function of $|\psi\rangle$ 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 non-increasing 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 every pair of elements in the group orbit of that state. This is not the case however. It is true that if two sets of states (in particular, two group orbits) are reversibly interconvertible (i.e. they have the same Gram matrix), then every pair from the first has the same distinguishability as the corresponding pair from the second. The opposite implication, however, 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 [19]. 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 [25]. 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 [25] 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, 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 absolute values of the characteristic functions for the two states, which encode the pairwise distinguishability of elements of the orbits of the states, are exactly the same. This follows from the fact that

$$|\chi_{\uparrow\downarrow}(\Omega)| = |\langle\uparrow_{\hat{z}}|\langle\downarrow_{\hat{z}}|\,[U(\Omega)\otimes U(\Omega)]\,|\uparrow_{\hat{z}}\rangle|\downarrow_{\hat{z}}\rangle| = |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle| \times |\langle\downarrow_{\hat{z}}|U(\Omega)|\downarrow_{\hat{z}}\rangle|$$

and

$$|\chi_{\uparrow\uparrow}(\Omega)| = |\langle\uparrow_{\hat{z}}|\langle\uparrow_{\hat{z}}|\,[U(\Omega)\otimes U(\Omega)]\,|\uparrow_{\hat{z}}\rangle|\uparrow_{\hat{z}}\rangle| = |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle| \times |\langle\uparrow_{\hat{z}}|U(\Omega)|\uparrow_{\hat{z}}\rangle|$$

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 that set implies that the relevant global properties of the set are encoded in the *phases* of the components of the Gram matrix, or equivalently, for group orbits, in the phase of the characteristic function of the state generating the orbit.

One may think that the insufficiency of pairwise distinguishabilities for specifying the content of a set is a uniquely quantum phenomenon, but this is not the case. A simple example (attributed to Peter Shor in [19]) shows that the phenomenon can also arise with sets of classical probability distributions. 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

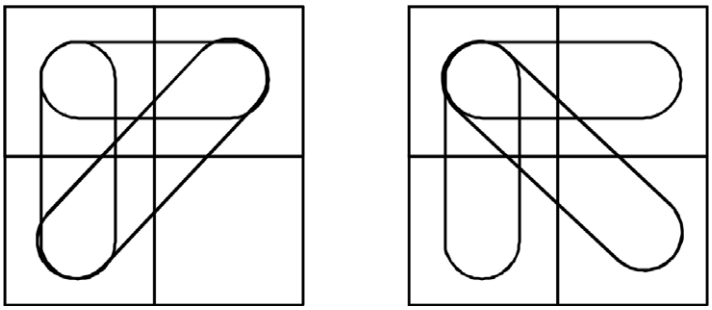

Figure C.1. Example of two ensembles of classical probability distributions that have different information content, but for which the pairwise distinguishability are the same.

illustrated by the 'sausages' in figure C.1. It is clear that the pairwise overlaps are the same for the two sets but that they are not reversibly interconvertible[18].

Appendix D. 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 [26]. 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 [26–28].

D.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.

$$f_x(t) = \int dF(x) e^{itx}. \tag{D.1}$$

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:

$$f_{x+y}(t) = f_x(t) f_y(t). \tag{D.2}$$

[18] It should be noted that the existence of this classical analogue demonstrates that the phenomenon in question can be added to the long list of those which are not obvious if one adopts the view that quantum states are states of reality, but are both intuitive and natural if one adopts the view that quantum states are states of incomplete knowledge [22].

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

$$\langle x^n \rangle = \mathrm{i}^{-n} \frac{\mathrm{d}^n}{\mathrm{d}t^n} f_x(t) \mid_{t=0} . \tag{D.3}$$

Sometimes it is more favorable to use *cumulants* of the random variable instead where the nth order cumulant is defined as the nth order derivative of the logarithm of the characteristic function at the point 0, multiplied by i^{-n}:

$$\kappa^{(n)} \equiv \mathrm{i}^{-n} \frac{\mathrm{d}^n}{\mathrm{d}t^n} \log(f_x(t)) \mid_{t=0} . \tag{D.4}$$

The first and second cumulants are the mean and the 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 (i) $f(0) = 1$, (ii) $f(t)$ is continuous at the origin, and (iii) 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 $t_1, \ldots, t_n$ 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. [24].

D.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

$$\mathrm{tr}(\rho L^k) = \mathrm{i}^{-k} \frac{\partial^k}{\partial \theta^k} \chi_\rho(\mathrm{e}^{\mathrm{i}\theta L}) \mid_{\theta=0} . \tag{D.5}$$

In particular the first derivative ($k = 1$) determines the expectation value of the generator. This is just property 7 of characteristic functions from section 5.2.

Similarly we can define *cumulants* of the observable L, where the nth order cumulant is defined as the nth order derivative of the logarithm of the characteristic function at the identity element multiplied by i^{-n}:

$$\kappa_L^{(n)} \equiv \mathrm{i}^{-k} \frac{\partial^k}{\partial \theta^k} \log[\chi_\rho(\mathrm{e}^{\mathrm{i}\theta L})] \mid_{\theta=0} . \tag{D.6}$$

The first and second cumulants are the mean and the 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 the 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 $\mathrm{tr}(\rho) = 1$ implies that $\chi(e) = 1$ (where e is the identity of the 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 the 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 D.1. *A complex function $\phi(g)$ on a group G is positive definite if for all choices $m \in \mathbb{N}$, $g_1, \ldots, g_m \in G$ and $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$*

$$\sum_{i,j=1}^{m} \bar{\alpha}_i \alpha_j \phi(g_i^{-1} g_j) \geqslant 0. \tag{D.7}$$

For the case of compact Lie groups where the function should also be continuous we can express the condition as

Definition D.2. *A continuous function $\phi(g)$ on a group G with the Haar measure $\mathrm{d}g$ is called positive definite if it satisfies*

$$\int \int \mathrm{d}g\, \mathrm{d}h\ \bar{f}(g)\phi(g^{-1}h) f(h) \geq 0 \tag{D.8}$$

for any $f \in L^1(G)$.

Now using the Fourier transform, one can easily prove a theorem similar to Bochner's theorem [26, 27]:

Theorem D.1. *A complex function $\phi(g)$ on the finite or compact Lie group G is the characteristic function of a quantum state in a finite-dimensional 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 $B^{(\mu)} \equiv d_\mu \int \mathrm{d}g U^{(\mu)}(g^{-1})\phi(g)$. Then the set of operators $\{B^{(\mu)}\}$ is the reduction onto irreps of a valid quantum state iff (i) $\sum_\mu \mathrm{tr}(B^{(\mu)}) = 1$ and (ii) all operators $\{B^{(\mu)}\}$ are positive definite. The first condition expresses the fact that the trace of the state is 1 and is guaranteed by $\phi(e) = 1$. On the other hand, $B^{(\mu)}$ is positive iff $\mathrm{tr}(FF^\dagger B^{(\mu)}) \geqslant 0$ 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, equation (58), we get

$$\mathrm{tr}(FF^\dagger B^{(\mu)}) = d_\mu^2 \int \int \mathrm{d}h_1\, \mathrm{d}h_2 f(h_1)\overline{f(h_2)}\phi(h_1^{-1}h_2). \tag{D.9}$$

So if $\phi(g)$ is positive definite and therefore satisfies equation (D.8) 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, namely, the GNS construction. A specific form of this theorem states

Theorem D.2 (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*

$$\phi(g) = \langle\psi|\, U(g)\, |\psi\rangle\,. \tag{D.10}$$

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 functions is exactly the same as the set of all characteristic functions of states.

Appendix E. More on the approximate notion of unitary *G*-equivalence

In this section, we prove theorem 3 and present some other versions of this result.

Using the standard bounds between fidelity and trace distance of two operators [5], we can express this result in terms of the trace distance between the reductions. As it may be useful in future applications, we present this reformulation of the condition as a corollary of theorem 3.

Corollary E.1. *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*

$$|\langle\psi_2|V|\psi_1\rangle| \geqslant 1 - \frac{1}{2}\sum_{\mu} \|F_1^{(\mu)} - F_2^{(\mu)}\|. \tag{E.1}$$

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

$$\begin{aligned}\chi^{(\mu)}_{\psi_{1,2}}(g) &\equiv \operatorname{tr}(U^{(\mu)}(g)F^{(\mu)}_{1,2})\\ &= d_\mu \operatorname{tr}(U^{(\mu)}(g)\int \mathrm{d}h U^{(\mu)}(h^{-1})\chi_{\psi_{1,2}}(h))\\ &= d_\mu \left(\varphi_\mu * \chi_{\psi_{1,2}}\right)(g),\end{aligned}$$

where $\varphi_\mu(g) = \operatorname{tr}(U^{(\mu)}(g))$ is the character of irrep μ and $*$ is the convolution operation defined in equation (59).

Corollary E.2. *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*

$$|\langle\psi_2|V|\psi_1\rangle| \geqslant 1 - \frac{1}{2}]\left(\sum_\mu d_\mu^2\right)\int \mathrm{d}g|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)| \tag{E.2}$$

and

$$|\langle\psi_2|V|\psi_1\rangle| \geqslant 1 - \frac{1}{2}\sum_\mu d_\mu^2\left(\int \mathrm{d}g\ |\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)|\right), \tag{E.3}$$

where the summation is over all irreps in which ψ_1 and ψ_2 have non-zero components.

To prove theorem 3, we first recall a well-known theorem by Uhlmann (see e.g. [29]).

Theorem E.1 (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 a 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. $\mathrm{tr}_{\mathcal{H}'}(|\alpha_k\rangle\langle\alpha_k|) = A_k$. In this case,*

$$\mathrm{Fid}(A_1, A_2) \equiv \|\sqrt{A_1}\sqrt{A_2}\| \tag{E.4}$$

$$= \max\{|\langle\alpha_1|\alpha_2\rangle| : tr_{\mathcal{H}'}(|\alpha_2\rangle\langle\alpha_2|) = A_2\}. \tag{E.5}$$

Proof of theorem 3 and remark 1. Suppose $\mathcal{M}_\mu\otimes\mathcal{N}_\mu$ is the subspace associated to irrep μ in $\mathcal{H}$ and Π_μ is the projective operator to this subspace. Define

$$|\psi_{1,2}^{(\mu)}\rangle \equiv \Pi_\mu|\psi_{1,2}\rangle. \tag{E.6}$$

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

$$|\langle\psi_2|V|\psi_1\rangle| = |\sum_\mu\langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle| \leqslant \sum_\mu|\langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle|. \tag{E.7}$$

Also define

$$F_{1,2}^{(\mu)} \equiv \mathrm{tr}_{\mathcal{N}_\mu}(|\psi_{1,2}^{(\mu)}\rangle\langle\psi_{1,2}^{(\mu)}|), \tag{E.8}$$

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

$$\mathrm{tr}_{\mathcal{N}_\mu}(|\widetilde{\psi}^{(\mu)}\rangle\langle\widetilde{\psi}^{(\mu)}|) = \mathrm{tr}_{\mathcal{N}_\mu}(|\psi_1^{(\mu)}\rangle\langle\psi_1^{(\mu)}|) = F_1^{(\mu)}. \tag{E.9}$$

Since $|\widetilde{\psi}^{(\mu)}\rangle$ and $|\psi_2^{(\mu)}\rangle$ are purifications of $F_1^{(\mu)}$ and $F_2^{(\mu)}$, then according to Uhlmann's theorem,

$$|\langle\psi_2^{(\mu)}|\widetilde{\psi}^{(\mu)}\rangle| \leqslant \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}). \tag{E.10}$$

This inequality together with the inequality (E.7) implies the bound (43).

Now we prove that this bound is achievable. According to Uhlmann's theorem there exists a purification of $F_1^{(\mu)}$, denoted by $|\phi^{(\mu)}\rangle$, such that

$$\mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) = |\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle|. \tag{E.11}$$

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

$$V \equiv \bigoplus_\mu e^{i\theta_\mu} I \otimes V^{(\mu)}, \tag{E.12}$$

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 phase. Note that with this definition V is a G-invariant unitary. Then we get

$$|\langle\psi_2|V|\psi_1\rangle| = |\sum_\mu e^{i\theta_\mu}\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle| = \sum_\mu |\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle|, \tag{E.13}$$

where the second equality holds because we have chosen $\{e^{i\theta_\mu}\}$ such that all the terms in the summand have the same phase. Therefore for this G-invariant unitary we have

$$|\langle\psi_2|V|\psi_1\rangle| = \sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}). \tag{E.14}$$

This completes the proof of theorem 3. To prove remark 1, we infer from equation (E.11) that

$$\begin{aligned}\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) &= \sum_\mu |\langle\psi_2^{(\mu)}|\phi^{(\mu)}\rangle| \\ &\leqslant \sum_\mu \sqrt{\langle\psi_2^{(\mu)}|\psi_2^{(\mu)}\rangle}\sqrt{\langle\phi^{(\mu)}|\phi^{(\mu)}\rangle} \\ &\leqslant \sqrt{\sum_\mu \langle\psi_2^{(\mu)}|\psi_2^{(\mu)}\rangle}\sqrt{\sum_\mu \langle\phi^{(\mu)}|\phi^{(\mu)}\rangle} = 1,\end{aligned}$$

where both of the 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 $\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \leqslant 1$ and the equality holds only if

$$\forall\mu : \ |\psi_2^{(\mu)}\rangle\langle\psi_2^{(\mu)}| = |\phi^{(\mu)}\rangle\langle\phi^{(\mu)}|. \tag{E.15}$$

But $|\psi_2^{(\mu)}\rangle$ is a purification of $F_2^{(\mu)}$ and $|\phi^{(\mu)}\rangle$ is a purification of $F_1^{(\mu)}$. So the above equality implies that

$$\forall\mu : \ F_1^{(\mu)} = F_2^{(\mu)}. \tag{E.16}$$

This completes the proof of remark 1. □

To prove corollary E.1, we begin by recalling some facts about the trace distance. For density operators ρ_1 and ρ_2 it is well known that $\| \rho_1 - \rho_2 \| \geqslant 2(1 - \mathrm{Fid}(\rho_1, \rho_2))$ [5, 29]. 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 E.1. *Suppose A_1 and A_2 are two positive operators. Then*

$$\|A_1 - A_2\| \geqslant \mathrm{tr}(A_1) + \mathrm{tr}(A_2) - 2\mathrm{Fid}(A_1, A_2). \tag{E.17}$$

We now provide the proof.

Proof of corollary E.1. According to lemma E.1,

$$\mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) \geqslant \frac{1}{2}\left(\mathrm{tr}(F_1^{(\mu)}) + \mathrm{tr}(F_2^{(\mu)}) - \|F_1^{(\mu)} - F_2^{(\mu)}\|\right), \tag{E.18}$$

which implies

$$\begin{aligned}\sum_\mu \mathrm{Fid}(F_1^{(\mu)}, F_2^{(\mu)}) &\geqslant \frac{1}{2}\left(\sum_\mu \mathrm{tr}(F_1^{(\mu)}) + \sum_\mu \mathrm{tr}(F_2^{(\mu)}) - \sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\|\right) \\ &= 1 - \frac{1}{2}\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\|,\end{aligned}$$

where we have used the fact that the sum of the traces of the elements of the reduction onto irreps is 1. Combining this bound with theorem 3, we obtain the desired result. □

Proof of corollary E.2. According to the Fourier transform, equation (54),

$$F_{1,2}^{(\mu)} = d_\mu \int \mathrm{d}g\; U^{(\mu)}(g^{-1})\chi_{\psi_{1,2}}(g). \tag{E.19}$$

Therefore

$$\begin{aligned}\|F_1^{(\mu)} - F_2^{(\mu)}\| &= d_\mu \left\| \left| \int \mathrm{d}g\; U^{(\mu)}(g^{-1}) \left[\chi_{\psi_1}(g) - \chi_{\psi_2}(g)\right] \right| \right\| \\ &\leqslant d_\mu \int \mathrm{d}g\; \|U^{(\mu)}(g^{-1})\| \left|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)\right|.\end{aligned}$$

Since $U^{(\mu)}(g^{-1})$ is a unitary acting on a d_μ-dimensional space, $\|U^{(\mu)}(g^{-1})\| = d_\mu$. So we have

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| \leqslant d_\mu^2 \int \mathrm{d}g \left|\chi_{\psi_1}(g) - \chi_{\psi_2}(g)\right|. \tag{E.20}$$

Therefore we have

$$\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\| \leqslant \left(\sum_\mu d_\mu^2\right) \int \mathrm{d}g |\chi_{\psi_1}(g) - \chi_{\psi_2}(g)|, \tag{E.21}$$

where the summation is over all irreps in which ψ_1 and ψ_2 have non-zero 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

$$F_{1,2}^{(\mu)} = d_\mu \int \mathrm{d}g\; U^{(\mu)}(g^{-1})\chi_{\psi_{1,2}}^{(\mu)}(g). \tag{E.22}$$

Therefore

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| = d_\mu \| \int \mathrm{d}g\ U^{(\mu)}(g^{-1}) \left[\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right] \|$$

$$\leqslant d_\mu \int \mathrm{d}g\ \|U^{(\mu)}(g^{-1})\| \left|\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right|.$$

Using the fact that $\|U^{(\mu)}(g^{-1})\| = d_\mu$ again, we have

$$\|F_1^{(\mu)} - F_2^{(\mu)}\| \leqslant d_\mu^2 \int \mathrm{d}g \left|\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)\right|. \tag{E.23}$$

Therefore we have

$$\sum_\mu \|F_1^{(\mu)} - F_2^{(\mu)}\| \leqslant \sum_\mu d_\mu^2 \int \mathrm{d}g\ |\chi_{\psi_1}^{(\mu)}(g) - \chi_{\psi_2}^{(\mu)}(g)|, \tag{E.24}$$

where the summation is over all irreps μ in which $F_1^{(\mu)}$ or $F_2^{(\mu)}$ are non-zero. □

References

[1] Goldstein H 1980 *Classical Mechanics* 2nd edn (Reading, MA: Addison-Wesley)
[2] Bartlett S D, Rudolph T and Spekkens R W 2007 *Rev. Mod. Phys.* **79** 555
[3] Gour G and Spekkens R W 2008 *New J. Phys.* **10** 033023
[4] Gour G, Marvian I and Spekkens R W 2009 *Phys. Rev.* A **80** 012307
[5] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[6] Nielsen M A 1999 *Phys. Rev. Lett.* **83** 436
[7] Wigner E P 1959 *Group Theory* (New York: Academic) pp 233–6
[8] Chiribella G 2006 Optimal estimation of quantum signals in the presence of symmetry *PhD Thesis* University of Pavia (www.qubit.it/educational/thesis/ThesisRevised.pdf)
[9] Chiribella G, Marvian I and Spekkens R W in preparation
[10] Marvian I 2012 Symmetry, asymmetry and quantum information *PhD Thesis* University of Waterloo, Canada
[11] Schuch N, Verstraete F and Cirac J I 2004 *Phys. Rev.* A **70** 042310
[12] Schuch N, Verstraete F and Cirac J I 2004 *Phys. Rev. Lett.* **92** 087904
[13] Vaccaro J A, Anselmi F, Wiseman H M and Jacobs K 2008 *Phys. Rev.* A **77** 032114
[14] Skotiniotis M and Gour G 2012 *New J. Phys.* **14** 073022
[15] Toloui B, Gour G and Sanders B C 2011 *Phys. Rev.* A **84** 022322
[16] Vaccaro J A 2012 *Proc. R. Soc. Lond.* A **468** 1065
[17] Keyl M and Werner R F 1999 *J. Math. Phys.* **40** 3283
[18] Curie P 1894 *J. Physique* **3** 401
[19] Jozsa R and Schlienz J 1999 *Phys. Rev.* A **62** 012301–1
[20] Davidson K 1996 C*-algebras by example *Fields Institute Monographs* (Providence, RI: American Mathematical Society)
[21] Barut A O and Raczka R 1986 *Theory of Group Representations and Applications* (Singapore: World Scientific)
[22] Spekkens R W 2007 *Phys. Rev.* A **75** 032110
[23] Jonathan D and Plenio M 1999 *Phys. Rev. Lett.* **83** 3566

[24] Gnedenko B V 1962 *The Theory of Probability* (New York: Chelsea)
[25] Gisin N and Popescu S 1999 *Phys. Rev. Lett.* **83** 432
[26] Gu Y 1985 *Phys. Rev.* A **32** 1310
[27] Korbicz J K and Lewenstein M 2006 *Phys. Rev.* A **74** 022318
[28] Korbicz J K, Wehr J and Lewenstein M 2008 *Commun. Math. Phys.* **281** 753
[29] *John Watrous's Lecture Notes on the Theory of Quantum Information* www.cs.uwaterloo.ca/∼watrous/quant-info/