Tight reference frame–independent quantum teleportation

Dominic Verdon Jamie Vicary
Department of Computer Science Department of Computer Science
University of Oxford University of Oxford
dominic.verdon@cs.ox.ac.uk jamie.vicary@cs.ox.ac.uk

March 16, 2016

Abstract

We give a tight scheme for teleporting a quantum state between two parties, whose reference frames are misaligned by some action of a finite symmetry group, satisfying a certain property. Unlike previously proposed schemes, ours requires no additional tokens or data to be passed between the participants; the same amount of classical information is transferred as for ordinary quantum teleportation, and the Hilbert space of the entangled resource is of the same size. Using the terminology of Peres and Scudo, the key idea is that the classical channel conveys \textit{unspeakable} information.

1 Introduction

1.1 The problem and our result

Recently many authors have recognised the importance of developing a theory of quantum information which takes account of the reference frames by which a system’s state is defined [2, 10, 12, 13]. In this paper we treat the problem of teleporting a quantum state between two parties who do not share a common reference frame. Quantum teleportation is a foundational quantum protocol with important applications [8, 9]. It was recognised some time ago [7] that a shared reference frame is a hidden additional resource assumed in classical teleportation protocols; indeed, it is highly likely that two parties using a teleportation protocol to transmit a quantum state over long distances will be uncertain about the alignment of their respective reference frames. This problem is therefore natural and important.

In this paper we exhibit a new teleportation protocol, requiring only local operations and classical communication, which in many cases allows perfect teleportation between two parties when their reference frames are not aligned. No additional resources or prior communication are required compared to traditional quantum teleportation; we only demand that the group $G$ of reference frame transformations is finite, and that the group admits a certain mathematical property. We demonstrate that these tight reference frame–independent (RFI) teleportation protocols correspond exactly to $G$-equivariant
unitary error bases, a structure we define. We prove that these bases do not exist for all finite groups, and we investigate construction methods for scenarios where they do. In particular, we provide a simple sufficient condition for the existence of RFI teleportation protocols on systems of dimension less than 5.

The key to our new protocol lies in the way that the result of the measurement is communicated between the parties: in the terminology of Peres and Scudo [15], we use unspeakable classical information, rather than speakable information which can be carried by a traditional classical channel. An example of unspeakable information is the choice of ‘up’ versus ‘down’, to be agreed by two parties who do not share a common reference frame; no amount of communication through a shared classical channel can decide the matter, but the transfer of a single oriented physical system from one party to the other, such as an arrow, is sufficient.

The fundamental concept of $G$-equivariant error basis was developed from investigations in categorical quantum mechanics, by characterizing the concept of quantum teleportation as a structure internal to a category, and applying it in the category of unitary representations of a finite group. Having recognized the mathematical richness of the construction, further investigations led to its interpretation as described in this article. We believe this serves as a good advert for categorical quantum mechanics, as a toolkit for developing new and interesting concepts in quantum information.

In Section 2 we give an informal worked example of our procedure, and in Section 3 we give a careful analysis of its mathematical basis. In Section 4 we show how the idea of $G$-equivariant teleportation arises from ideas of categorical quantum mechanics. In Section 5 we prove a variety of existence, nonexistence and construction results regarding $G$-equivariant unitary error bases.

1.2 Previous results

The problem of RFI teleportation was discussed at length in [5], where the authors distinguished teleportation of speakable information, where the transferred state need only have the same coordinates in Bob’s reference frame as it had in Alice’s; and teleportation of unspeakable information, where an external observer would see that the state of the system itself is transferred. Here we will be concerned with teleportation of unspeakable information; from this point forward we will use the word ‘teleportation’ to mean only this. We are only interested in teleportation protocols with zero probability of failure.

It was demonstrated in [5] that teleportation is impossible when the group of reference frame transformations is a nontrivial compact connected Lie group and the representation on the system to be teleported does not factor through a representation of a finite group. As observed in that paper, this leaves the case of a finite group of reference frame transformations open.

A number of resolutions have previously been proposed. In [5], it was suggested that Alice could transmit half of a maximally entangled token state, in the regular representation, in advance of performing the protocol; the two parties could then use this to synchronise their operations. This method, however, requires Alice to be able to initialise an entangled state on a pair of systems each carrying the regular representation of the transformation group, a procedure which may be experimentally difficult or impossible.

Another relevant result can be found in [10]. In that work, it was shown that it is possible to perform quantum protocols using a second shared system as a quantum reference frame. This general result, intended for application to quantum cryptography, may be
used to create reference frame–independent teleportation protocols. These protocols are formally identical to the token state method, but operationally more practicable; Alice and Bob simply initialise an additional shared entangled state at the same time as they create the first, take half each and use it to synchronise their operations. The problems of the token state method therefore persist in this case, although without the additional difficulty of communicating half of the second entangled state from one party to the other.

Finally, various solutions have also been proposed which use prior communication to align both parties’ reference frames in advance of performing a normal teleportation protocol; methods are described in [2]. This increases the amount of classical information that must be communicated for successful teleportation. Moreover, the alignment step must be repeated every time teleportation is to be performed, since the relative reference frame may change over time. This could lead to significant overhead. Note that in our protocol, the teleportation concludes successfully without any information about the relative reference frame being transferred.

2 Example of the procedure

In this section we give an informal account of the problem of reference frame–independent quantum teleportation, and of our new solution. This is followed by a more mathematically precise description in the next section.

Suppose that Alice and Bob have laboratories which are well-separated in space, and that they can communicate through a classical channel. Using this channel, they decide that Alice will teleport a single qubit to Bob, which is initially in a pure state. Alice has an auxiliary qubit in her possession, which she earlier entangled as the first qubit in a Bell state $|\eta\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; the second qubit of the entangled pair is currently in Bob’s local environment.

Before they begin the procedure, they attempt to align their reference frames. They lack the necessary equipment to do this by an absolute method, such as observing the stars, so they must do it by communication between their ships. They use the following method: Alice emits a beam of light, polarized vertically with respect to her local reference frame, aimed towards Bob, who rotates his laboratory until his local vertical coordinate is aligned with the polarization direction.

This procedure has an obvious flaw: one party might be upside down relative to the other, since polarization has a $\mathbb{Z}_2$ symmetry. Nonetheless, Alice and Bob continue with their teleportation procedure. Using their classical communication channel, they decide to follow a procedure by which Alice will measure her initial system together with her part of the entangled state in the basis $|\phi_i\rangle$ and communicate the result to Bob, who will apply the corresponding correction $U_i$. We define $|\phi_i\rangle = (\mathbb{1} \otimes U^T_i) |\eta\rangle$, where $U^T_i$ denotes the transpose of the matrix $U_i$, $\mathbb{1}$ denotes the 2-by-2 identity matrix, and $|\eta\rangle$ is the Bell state as given above. The $U_i$ are defined as follows:

\[
U_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad U_2 = \frac{1}{4} \begin{pmatrix} -\sqrt{2} - \sqrt{6} & -\sqrt{2} + \sqrt{6} \\ -\sqrt{2} + \sqrt{6} & -\sqrt{2} - \sqrt{6} \end{pmatrix}
\]

\[
U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad U_3 = \frac{1}{4} \begin{pmatrix} \sqrt{2} - \sqrt{6} & -\sqrt{2} - \sqrt{6} \\ -\sqrt{2} - \sqrt{6} & \sqrt{2} - \sqrt{6} \end{pmatrix}
\]

It can readily be checked that this data forms an unitary error basis, and so by the results of Werner [17] gives correct data for the execution of an ordinary quantum teleportation procedure for a single qubit, when the shared state is the Bell state $|\eta\rangle$. 

3
If Bob was fortunate and managed to align his reference frame correctly with Alice’s, then the parties are carrying out standard quantum teleportation, and the procedure will be successful. However, if his reference frame is upside-down with respect to Alice’s, then from Alice’s perspective this induces a unitary action of the group $\mathbb{Z}_2$ on his local qubit. We suppose that this action is as follows, where $a$ is the nontrivial element of $\mathbb{Z}_2$:

$$
\pi(a) = \begin{pmatrix}
\sqrt{3}/2 & 1/2 \\
1/2 & -\sqrt{3}/2
\end{pmatrix}
$$

The details of this unitary operator will depend on the physics of the quantum object in which Bob’s half of the entangled pair is embodied. From the perspective of Alice’s reference frame, Bob’s qubit does not update according to the unitary $U_i$ as indicated by Alice; it updates according to the unitary $\pi(a)^\dagger U_i \pi(a)$. A straightforward calculation then shows that Bob in fact receives a mixed state; quantum information has been irrevocably lost, and correctness of the scheme has been destroyed by the misalignment in their reference frames. From Bob’s perspective, he correctly applied the unitary $U_i$, but the teleportation failed for a different reason: the entangled state they shared was not the Bell state, but rather $(1 \otimes \pi(a)) \eta$, with the $\pi(a)$ factor appearing as in his reference frame as the qubit has been rotated.

In our new procedure, rather than communicate two bits to Bob using their shared classical channel, she sends two physical objects: arrows, of the sort a medieval archer might use. She orients these arrows according to the measurement result that she obtained, in the following way:

$$
\begin{align*}
0 & \mapsto \{\uparrow\uparrow\} \\
1 & \mapsto \{\downarrow\downarrow\} \\
2 & \mapsto \{\uparrow\downarrow\} \\
3 & \mapsto \{\downarrow\uparrow\}
\end{align*}
$$

Each arrow is pointing either up or down with respect to Alice’s local vertical axis. She physically sends these arrows through space to Bob’s laboratory, who observes their local orientations and infers the measurement result 0, 1, 2 or 3 that Alice obtained. Suppose Bob’s laboratory is correctly aligned with Alice’s; then he will correctly infer Alice’s measurement result, and he will apply the unitary correction operator as before. In this case, the two parties have simply executed a traditional quantum teleportation protocol, albeit one where the two classical bits of information were transferred from Alice to Bob in an unusual way.

Now we suppose that Bob’s laboratory is aligned upside-down with respect to Alice’s. Then, if Alice attempts to send the message 0, 1, 2 or 3, Bob will receive it as 1, 0, 3 or 2 respectively, since the arrows will appear to him with the opposite orientations. Furthermore, just as before, when Bob applies a unitary $U_i$, its action is seen in Alice’s reference frame as $\pi(a)^\dagger U_i \pi(a)$. We now see the point of the entire construction: the unitary error basis is carefully chosen so that these effects cancel out. Indeed, the following equations can be easily verified:

$$
\begin{align*}
\pi(a)^\dagger U_0 \pi(a) &= U_1 \\
\pi(a)^\dagger U_1 \pi(a) &= U_0 \\
\pi(a)^\dagger U_2 \pi(a) &= U_3 \\
\pi(a)^\dagger U_3 \pi(a) &= U_2
\end{align*}
$$

As a result, the quantum teleportation will still conclude successfully, even though Bob’s reference frame was misaligned.

In summary, by a careful choice of the unitary error basis, and by transferring the measurement result as unspeakable rather than speakable information, the quantum teleportation procedure can be carried out in a way which is robust against this restricted
sort of reference frame error. Note in particular that only 2 bits of classical information were transferred from Alice to Bob, just as with the traditional teleportation procedure. Also note that the unspeakable information Bob receives from Alice is uniformly random, since Alice’s measurement results are; in particular, Bob receives no information during the protocol about whether or not his reference frame is correctly aligned with Alice’s.

3 Mathematical description of the proposal

3.1 Traditional teleportation

Teleportation is a well-understood procedure. In its traditional form [3, 17], where all parties’ reference frames are perfectly aligned, it works as follows. Note that we only consider tight quantum teleportation in this paper; that is, the state spaces of the initial system and the entangled systems all have the same dimension, which is equal to the number of classical bits transferred.

Procedure 3.1 (Traditional quantum teleportation). Alice wants to teleport her state $|\phi\rangle$ to Bob; she has one half of a maximally entangled bipartite state $\omega$, and Bob the other. She performs a measurement with respect to an orthonormal basis of effects $F_i$ on the bipartite system built from her initial system and her half of the entangled state. She sends the measurement result $x$ to Bob through a perfect classical channel. Bob then performs a unitary operator $T_x$ on his half of the entangled state. The data $(\omega, \{F_i\}, \{T_i\})$ is correct if Bob is guaranteed to receive the state $|\phi\rangle$ at the end of the procedure.

A complete description of correct data $(\omega, \{F_i\}, \{T_i\})$ was given by Werner [17], as follows.

Definition 3.2. For a Hilbert space $H$, a unitary error basis is a basis of unitary operators $U_i \in B(H)$, which are orthonormal under the Hilbert-Schmidt inner product:

$$\text{Tr}(U_i^\dagger U_j) = \text{dim}(H) \delta_{ij}$$

Theorem 3.3 (Werner). Up to equivalence, teleportation schemes for systems with Hilbert space $H$ are in one to one correspondence with unitary error bases on $H$.

Under this correspondence, the shared entangled state $\omega$ is the Bell state $\sum_i |i\rangle \otimes |i\rangle$ for any orthonormal basis $\{|0\rangle, |1\rangle, \ldots\}$. Alice measures in the maximally entangled basis $\{|\phi_0\rangle, |\phi_1\rangle, \ldots\}$, where $|\phi_x\rangle \in H \otimes H$ is defined as $\sum_i |i\rangle \otimes U_x |i\rangle$. Bob’s correction for the measurement outcome $x$ is $U_x^T$.

3.2 Reference frame–independent quantum teleportation

We now fully describe the problem we solve.

Problem 3.4 (Reference frame–independent quantum teleportation). Alice and Bob are spatially-separated quantum information theorists with a classical communication channel. Alice wants to communicate a quantum state to Bob using a teleportation scheme. Each party has one half of an entangled state which they created at some point in the past, when they were together and their reference frames were aligned. However, since then, their reference frames have shifted. This shift in reference frames is described by the action of unknown elements $g_A, g_B$ of the group $G$ of reference frame transformations.
(i) Is there a teleportation scheme – that is, a valid choice of measurement effects \( F_x \) and corrections \( T_x \) – such that Procedure 3.1 is guaranteed to teleport Alice’s state to Bob regardless of the alignment of their reference frames?

(ii) If not, can we develop a different teleportation procedure, using only local operations and classical communication, that is guaranteed to teleport Alice’s state to Bob regardless of the alignment of their reference frames?

**Remark 3.5.** This problem is a useful foundation for our analysis, but hardly captures the full range of situations where it will be useful. Our analysis can be applied verbatim, for instance, to any situation where some active group of transformations acts on Alice and Bob’s systems, provided that the same group element acts on both of Alice’s systems. Even if this latter condition does not hold, many elements of the analysis will still be relevant.

We now demonstrate how the shift in reference frames causes a serious problem for Procedure 3.1. First we note the following lemma.

**Lemma 3.6.** Under the conditions of Problem 3.4, Procedure 3.1 will work for all reference frame alignments if and only if the operations \( F_x \) and \( T_x \) are all intertwiners for the group action.

**Proof.** We express the operations with reference to the original shared reference frame. Let Alice and Bob’s frame shifts be described by group elements \( g_A \) and \( g_B \) respectively. Alice measures \( F_x \) relative to her reference frame; in the original frame the operation she has performed is \( \pi(g_A)^\dagger F_x \pi(g_A) \). She then sends the result \( x \) to Bob, who performs the operation \( T_x \) relative to his frame; in the original frame the operation he has performed will be \( \pi(g_B)^\dagger T_x \pi(g_B) \). In general, the channel will therefore only work for all reference frame configurations when, for all \( g_A, g_B \), \( \pi(g_A)^\dagger F_x \pi(g_A) = F_{gA(x)} \) and \( \pi(g_B)^\dagger T_x \pi(g_B) = T_{gA(x)} \), for some action of \( G \) on the set of measurement outcomes. Since \( \pi(e)^\dagger T_x \pi(e) = T_x \) for the identity \( e \), this clearly implies that \( g(x) = x \) for all \( g \). The result follows.

We now demonstrate that Procedure 3.1 works only for a trivial \( G \)-action.

**Proposition 3.7.** Procedure 3.1 will only work for all reference frame alignments when \( H \) is a direct sum of identical one-dimensional representations of \( G \); that is, when \( G \) acts by a global phase.

**Proof.** By Theorem 3.3 and Proposition 3.6, Procedure 3.1 will work only if all projections \( |\phi_i \rangle \langle \phi_i| \) and corrections \( U_i \) are intertwiners. By the definition of \( |\phi_i \rangle \) in Theorem 3.3, it is sufficient that all \( U_i \) be intertwiners. Let us assume that this is the case. Since the \( G \)-action is trivial on a basis of \( \text{End}(H) \), it must be completely trivial on \( \text{End}(H) \). Therefore we have \( H \otimes H^* \simeq n \cdot 1 \). By straightforward character theory, there can only be one copy of \( 1 \) in the product of an irreducible representation with its dual. Breaking \( H \) up into simple factors, it follows by counting dimensions that they must all be identical and one dimensional.

### 3.3 Our new scheme

We now give a precise statement of our new procedure.
**Procedure 3.8** (Reference frame–independent quantum teleportation). Alice wants to teleport her state $|\phi\rangle$ to Bob; she has one half of a maximally-entangled bipartite state $\omega$, and Bob the other. She forms the bipartite system given by her initial system together with her half of the entangled state in the basis $F_x$. Bob then performs a unitary operator $T_x$ on his half of the entangled state. The data $(\omega, F_x, T_x)$ is correct if Bob is guaranteed to receive the state $|\phi\rangle$ at the end of the procedure.

The only difference is that, instead of measuring the bipartite system and communicating the result to Bob through a conventional classical channel, she sends the decohered bipartite system itself. The distinction is that misalignment of reference frames will not affect the way Bob perceives the data arriving through a separate classical channel, but it will affect the way that he perceives the decohered bipartite system; this procedure allows the state of measurement outcomes to carry a $G$-action. In the terminology of Peres and Scudo [15], an ordinary classical channel communicates *speakable* information, but a classical object passed physically from one party to another communicates *unspeakable* information.

**Remark 3.9.** It might not be necessary to send the decohered system if one can find another mode of classical communication capable of communicating unspeakable information. An example of this was given in Section 2, in which Alice’s measurement result was encoded in the spatial orientations of some physical objects. Whenever the finite group $G$ is a subgroup of $SO(3)$ and the reference frame corresponds to a direction in space, we may use the method of Section 2; in other cases, however, the more general approach of Procedure 3.8 may be required.

The basic data of Procedure 3.8 is the same as for Procedure 3.1, and so Theorem 3.3 still applies. However, not all unitary error bases give rise to successful teleportation schemes under this procedure. We now investigate which of them do.

**Definition 3.10** ($G$-equivariant unitary error basis). For a Hilbert space $H$ equipped with a unitary representation of $G$, a unitary error basis is $G$-equivariant when the elements are permuted by the natural action $M \mapsto \pi(g)M\pi(g)^\dagger$ of $G$ on $\text{End}(H)$. Explicitly, $\pi(g)U_i\pi(g)^\dagger = U_{\sigma_g(i)}$ for some permutation $\sigma_g$ of the set $\{1, \ldots, d^2\}$.

**Theorem 3.11.** Procedure 3.8 will succeed for any reference frame misalignment $g \in G$ just when the unitary error basis $U_i$ is $G$-equivariant.

**Proof.** We again work in Alice and Bob’s original lab frame. Alice decoheres in the orthonormal basis $\{\pi(g_A)|\phi_0\rangle, \pi(g_A)|\phi_1\rangle, \ldots\}$. Bob then measures in the orthonormal basis $\{\pi(g_B)|\phi_0\rangle, \pi(g_B)|\phi_1\rangle, \ldots\}$, and, depending on his measurement outcome $x$, performs the corresponding correction $\pi(g_B)U_x^T\pi(g_B)^\dagger$.

We first note that, putting Alice’s decoherence and Bob’s measurement together as one operation, we get a teleportation scheme under Definition 3.1. Therefore, by Theorem 3.3, Alice’s decoherence operation followed by Bob’s measurement must be a measurement in some orthonormal basis of maximally entangled states; clearly that must be the basis that Bob measures in. Letting Bob’s measurement channel be $M_1$ and Alice’s decohering channel be $M_2$, it follows that $M_1 \circ M_2 = M_1$; this can clearly only be true if the projection basis for $M_2$ is the same as the projection basis for $M_1$. We therefore see that the basis $\{\pi(g_A)|\phi_0\rangle, \pi(g_A)|\phi_1\rangle, \ldots\}$ must be some reordering of the basis.
\{ \pi(g_B) | \phi_0 \rangle, \pi(g_B) | \phi_1 \rangle, \ldots \}, \text{ for all } g_A, g_B. \text{ This is exactly } G\text{-equivariance of the UEB } U_i.

We now demonstrate that this condition is sufficient to guarantee success for Procedure 3.8. Suppose \( U_i \) is \( G \)-equivariant. Then Alice’s decohering operation is exactly the same as it would have been if her reference frame had not shifted at all. Bob measures \textit{and} performs the correction; the correction therefore corresponds to the measurement and the result follows. \( \square \)

### 4 Classical structures in \( \text{Rep}(G) \)

Teleportation in the context of a finite group \( G \) can be described elegantly in the framework of \textit{categorical quantum mechanics} [1]. One key strategy in this research programme is to understand features of quantum information in terms of the category \( \text{FHilb} \) of finite-dimensional Hilbert spaces and linear maps, and then to generalize them by applying them in different categories. The concept of \( G \)-equivariant quantum teleportation arises by understanding the categorical structure of the traditional quantum teleportation procedure, and then applying it in \( \text{Rep}(G) \), as we now explore. This technical section of the paper will make use of well-known ideas from categorical quantum mechanics, of which full details are available in the provided references; for reasons of space, proofs in this section are omitted.

The following definition gives our abstract categorical description of quantum teleportation, in terms of classical structures in a symmetric monoidal category [6].

**Definition 4.1.** In a dagger-compact category, a \textit{quantum teleportation procedure} on an object \( A \) with a right dual is a classical structure on the object \( A \otimes A^* \), satisfying the following condition, where \( c \) is some scalar:

\[
\text{comultiplication} = c \cdot \text{unit} \tag{2}
\]

This definition is motivated by the following theorem; recall Werner’s Theorem 3.3.

**Theorem 4.2.** Quantum teleportation procedures in \( \text{FHilb} \) correspond precisely to \textit{unitary error bases}.

We now summarize the application of these ideas in a group representation category.

**Definition 4.3.** For a group \( G \), the dagger-compact category \( \text{Rep}(G) \) has objects given by unitary representations of \( G \), morphisms given by intertwiners, and a dagger-compact structure inherited from the underlying Hilbert spaces.

**Theorem 4.4.** Quantum teleportation procedures in \( \text{Rep}(G) \) correspond precisely to \( G \)-equivariant unitary error bases.
Finally, we observe that the constructions of unitary error bases in Theorem 5.11 and Remark 5.12 carry over straightforwardly to the $G$-equivariant setting because they are essentially categorical constructions; the Hadamard construction, for instance, is defined in terms of two special commutative dagger Frobenius algebras and an isomorphism between them. In $\text{Rep}(G)$, this reduces exactly to the intertwining Hadamard matrix and $G$-equivariant orthonormal basis of Theorem 5.11. In this sense, these constructions are much more natural than, for instance, the construction of unitary error bases using projective group representations [11]; indeed, it is difficult to see how the latter construction could be brought into the $G$-equivariant framework.

5 Existence and construction of RFI teleportation protocols

We have demonstrated that $G$-equivariant UEBs are exactly the structures we need to perform reference frame–independent teleportation protocols, but it is still unclear how to construct them for a given representation $H$, if they exist at all. We cannot hope for a general classification of $G$-equivariant UEBs, since there is not even a classification in the case where the $G$-action is trivial\(^1\), although many construction methods exist [11, 14, 17]. In this section we will demonstrate that $G$-equivariant unitary error bases need not exist on every representation, meaning that RFI teleportation is not always possible. We will then demonstrate that several UEB constructions carry over naturally to the $G$-equivariant setting, allowing us to construct RFI teleportation protocols for a wide variety of systems.

We begin with a definition.

**Definition 5.1.** A $G$-equivariant orthonormal basis for some representation $V$ is an orthonormal basis of $V$ whose elements are permuted by the action of $G$.

**Remark 5.2.** $G$-equivariant unitary error bases are $G$-equivariant orthonormal bases of $\text{End}(H) \simeq H \otimes H^*$, all of whose elements are unitary maps.

It will transpire that we can use $G$-equivariant orthonormal bases on $H$ to construct $G$-equivariant UEBs for $H$. Moreover, if we prove that there are no $G$-equivariant orthonormal bases on $\text{End}(H)$, it follows by Remark 5.2 that there will be no $G$-equivariant UEBs for $H$; we will use this fact to demonstrate that RFI teleportation protocols need not always exist. Our first step is therefore a classification of $G$-equivariant orthonormal bases.

5.1 A classification of $G$-equivariant orthonormal bases

We begin with a simple lemma. Let $G$-$\text{Set}$ be the category whose objects are sets carrying an action of $G$, and whose morphisms are $G$-equivariant functions between them. Then there exists a functor $\mathcal{M} : G$-$\text{Set} \to \text{Rep}(G)$, which, given a $G$-set, constructs the free Hilbert space on its elements, and extends the $G$-action and morphisms linearly.

**Lemma 5.3.** $G$-equivariant orthonormal bases exist only on representations isomorphic to those in the image of $\mathcal{M}$.

\(^1\)The problem of classifying UEBs is closely related to the difficult problem of classifying Hadamard matrices [16].
Proof. Immediate, since a \( G \)-equivariant orthonormal basis has an underlying Hilbert space isomorphic to the free Hilbert space on the elements of the chosen basis, which \( G \) acts on by permutations.

We begin by presenting a simple classification of \( G \)-sets due to Burnside [4].

**Definition 5.4.** Given two \( G \)-sets \((X_1, \sigma_1)\) and \((X_2, \sigma_2)\), their **disjoint union** \((X_1 \sqcup X_2, \sigma_1 \sqcup \sigma_2)\) is the disjoint union of \( X_1 \) and \( X_2 \) as sets with the natural induced action.

**Definition 5.5.** Given a subgroup \( H \) of \( G \), the **coset space** \((G/H, \sigma_H)\) is the \( G \)-set whose elements are the cosets of \( H \) in \( G \), and whose \( G \)-action \( \sigma_H \) is the natural action of \( G \) by left multiplication on those cosets.

**Lemma 5.6.** Any \( G \)-set is isomorphic to a disjoint union of coset spaces. Two coset spaces are isomorphic as \( G \)-sets if and only they correspond to conjugate subgroups.

**Proof.** See [4].

**Remark 5.7.** In modern language, Lemma 5.6 states that \( G \)-Set is a semisimple fusion category whose simple objects correspond to conjugacy classes of subgroups in \( G \). It is easy to see that the functor \( \mathcal{M} \) is additive; the disjoint union of two \( G \)-sets will be sent under \( \mathcal{M} \) to the direct sum of their corresponding representations. In order to classify all objects in the image of \( \mathcal{M} \), therefore, it is sufficient to find the image of the coset spaces under \( \mathcal{M} \). We will call those representations the basic permutation representations.

In order to identify the basic permutation representations, we now state an obvious but critical lemma regarding the character of the permutation representation induced by \( \mathcal{M} \) on a \( G \)-set.

**Lemma 5.8.** Given a \( G \)-set \((X, \sigma)\), let \( \chi : G \rightarrow \mathbb{R} \) be the character of \( \mathcal{M}(X, \sigma) \). Then the following holds:

\[
\chi(g) = |\{ x \in X \mid g \cdot x = x \} |
\]  

**Proof.** The character \( \chi(g) \) is exactly the trace of the matrix representing \( g \); the result follows trivially from the definition of \( \mathcal{M}(X, \sigma) \).

We may therefore identify the basic permutation representations by taking a representative of every conjugacy class of subgroups of \( G \), finding the number of fixed points of the action of each element of \( G \) on the corresponding coset spaces, then decomposing the resulting characters using the character table to find the corresponding representations.

### 5.2 Existence of RFI teleportation protocols

Using the results of Subsection 5.1, we now exhibit a representation for which no \( G \)-equivariant UEBs exist, and on which quantum teleportation is therefore impossible.

**Proposition 5.9.** There is no RFI protocol to teleport the state of the 2-dimensional irreducible representation \( V \) of \( S_3 \).

**Proof.** Using the method outlined in Subsection 5.1, we find that the characters of the basic permutation representations are as follows:
The character of $V \otimes V^*$ is $4|0|1$, which clearly cannot be composed as a sum of characters of basic permutation representations. By Remark 5.2, the result follows.

Remark 5.10. This argument does not extend to all irreducible representations. The endomorphism space of the 2-dimensional irreducible representation of $D_8$, for instance, is a sum of basic permutation representations.

5.3 Construction of RFI teleportation protocols

Although RFI teleportation protocols need not always exist, they can often be constructed. We now demonstrate that, if we can find a $G$-equivariant orthonormal basis on $H$, and a Hadamard matrix which commutes with all $\pi(G)$ in that basis, we can perform RFI teleportation on $H$.

Theorem 5.11. Let $|v_i\rangle$ be a $G$-equivariant orthonormal basis on $H$. In this basis all $\pi(g)$ will be permutation matrices. Let $H$ be a Hadamard matrix that commutes with all $\pi(G)$ in this basis. Then the following family is a $G$-equivariant UEB:

$$ (U_H)_{ij} = \frac{1}{N} H \circ \text{diag}(H, j)^\dagger \circ H^\dagger \circ \text{diag}(H^T, i) \quad (4) $$

Proof. It was already proved in [14] that this is a UEB; we therefore need only show that it is $G$-equivariant. Since $H \in C_{U(n)}(G)$ we have that $gU_{ij}g^\dagger = \frac{1}{n} H \circ (g \circ \text{diag}(H, j)^\dagger \circ g^\dagger) \circ H^\dagger \circ (g \circ \text{diag}(H^T, i) \circ g^\dagger)$. We see easily that $g \circ \text{diag}(H, j)^\dagger \circ g^\dagger = g \circ \text{diag}(H^*, j) \circ g^\dagger = \text{diag}(H^* \circ g, j)$. Now note that the fact that $H$ commutes with all elements of $G$ means that permuting the columns of $H$ is exactly the same as permuting the rows, since $gH = Hg$ for all $g \in G$. So $\text{diag}(H^* \circ g, j) = \text{diag}(g \circ H^*, j) = \text{diag}(H^*, g \cdot j)$. A similar argument works for $\text{diag}(H^T, i)$. □

Remark 5.12. If the assumptions of Theorem 5.11 are satisfied, it is possible to construct many more $G$-equivariant UEBs using quantum Latin squares (QLSs) [14]; this construction will give $G$-equivariant UEBs provided the linear map defining the QLS is an intertwiner.

We finish this section with a simple sufficient condition for the existence of tight RFI protocols on systems of dimension less than 5. Firstly we prove a lemma.

Lemma 5.13. Let $M$ be a matrix of dimension $\geq 3$ defined by two complex parameters $a$ and $b$, where all entries on the diagonal are $a$, and all other entries are $b$. Let $\alpha = |a|\alpha, b = |b|\beta$ where $\alpha, \beta \in U(1)$ and $|a|, |b| \neq 0$. Then $M$ is unitary precisely when the following conditions are satisfied:

$$ \frac{n-2}{n} \leq |a| \leq 1 \quad (5) \quad |b|^2 = \frac{1 - |a|^2}{n-1} \quad (6) \quad \text{Re}(\alpha^*\beta) = \frac{2 - n |b|}{2 |a|} \quad (7) $$
Proof. For unitarity it is sufficient that the rows form an orthonormal basis. It is clear from the symmetry of $Q$ that it is sufficient for one row vector to be normal, and one pair of row vectors to be orthogonal. This gives us two equations in $a$ and $b$:

\[ |b|^2 = \frac{1 - |a|^2}{n - 1} \tag{8} \]
\[ \text{Re}(a^*b) = \frac{2 - n}{2} |b|^2. \tag{9} \]

We will demonstrate that (5) is necessary and sufficient for us to find $b$ satisfying these equations. It is obvious that (8) is satisfiable if and only if $|a| \leq 1$. Letting $a = |a|\alpha, b = |b|\beta$, Equation (9) becomes

\[ \text{Re}(\alpha^*\beta) = \frac{2 - n}{2} \frac{|b|}{|a|}. \]

Since $-1 \leq \text{Re}(\alpha^*\beta) \leq 1$ and $\alpha, \beta$ can be freely adjusted to give $\text{Re}(\alpha^*\beta)$ any value in that range, we see that the following is necessary and sufficient for (9) to be soluble:

\[ \frac{(2 - n)^2 |b|^2}{4 |a|^2} \leq 1 \]

Use of the identity (8) and a short calculation demonstrates that this is equivalent to the lower bound in the inequality (5). \qed

**Theorem 5.14.** Suppose $H$ admits a $G$-equivariant orthonormal basis, and is of dimension less than 5. Then there exists a RFI teleportation protocol for $H$.

**Proof.** We construct a $G$-equivariant UEB for $H$. Expressed in the $G$-equivariant orthonormal basis, $\pi(G)$ will be some subgroup of the permutation matrices $S_n$. To use Theorem 5.11, we must find a Hadamard matrix commuting with $\pi(G)$. In the worst case, $\pi(G)$ will be the whole group $S_n$ of permutation matrices. (This situation is realised for the representation $1 \oplus V$ of $S_n$, where $V$ is the fundamental $(n-1)$-dimensional representation of $S_n$).

We will demonstrate that, when $H$ is of dimension less than 5, we can find a Hadamard matrix which commutes with all the permutation matrices. First we eliminate the degenerate cases $n = 1$ and $n = 2$. Clearly for $n = 1$ we can perform RFI teleportation by Proposition 3.7, For $n = 2$ the following family of Hadamard matrices commutes with $S_2$, where $|a| = |b| = 1/\sqrt{2}$ and $\text{Re}(a^*b) = 0$:

\[
\begin{pmatrix}
a & b \\
b & a
\end{pmatrix}
\]

From now on we may therefore assume $n \geq 3$.

It is easy to see that the centraliser $C_{M_n}(S_n) \subset M_n$ is the set of matrices defined by two complex parameters $a$ and $b$, where all entries on the diagonal are $a$, and all other entries are $b$. The conditions necessary for such a matrix to be unitary were given in Lemma 5.13. Setting $|a| = |b|$ in (6), it follows that $|a| = 1/\sqrt{n}$. This is compatible with (5) only for $n \leq 4$. \qed
References

[1] S. Abramsky and B. Coecke. Categorical quantum mechanics. In Dov M. Gabbay Daniel Lehmann, Kurt Engesser, editor, Handbook of Quantum Logic and Quantum Structures, pages 261 – 323. Elsevier, Amsterdam, 2009. http://dx.doi.org/http://dx.doi.org/10.1016/B978-0-444-52869-8.50010-4 doi:http://dx.doi.org/10.1016/B978-0-444-52869-8.50010-4.

[2] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. Rev. Mod. Phys., 79:555–609, Apr 2007. http://dx.doi.org/10.1103/RevModPhys.79.555 doi:10.1103/RevModPhys.79.555.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys. Rev. Lett., 70:1895–1899, Mar 1993. http://dx.doi.org/10.1103/PhysRevLett.70.1895 doi:10.1103/PhysRevLett.70.1895.

[4] W. Burnside. Theory of Groups of Finite Order. Dover Books on Mathematics Series. Dover Publications, 2004.

[5] G. Chiribella, V. Giovannetti, L. Maccone, and P. Perinotti. Teleportation transfers only speakable quantum information. Phys. Rev. A, 86:010304, Jul 2012. http://dx.doi.org/10.1103/PhysRevA.86.010304 doi:10.1103/PhysRevA.86.010304.

[6] B. Coecke, D. Pavlovic, and J. Vicary. A new description of orthogonal bases. Mathematical Structures in Computer Science, 23:555–567, 6 2013. http://dx.doi.org/10.1017/S0960129512000047 doi:10.1017/S0960129512000047.

[7] S. J. Van Enk. The physical meaning of phase and its importance for quantum teleportation. Journal of Modern Optics, 48(13):2049–2054, 2001. http://arxiv.org/abs/http://dx.doi.org/10.1080/09500340108240906 arXiv:http://dx.doi.org/10.1080/09500340108240906, http://dx.doi.org/10.1080/09500340108240906 doi:10.1080/09500340108240906.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. Rev. Mod. Phys., 74:145–195, Mar 2002. http://dx.doi.org/10.1103/RevModPhys.74.145 doi:10.1103/RevModPhys.74.145.

[9] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature, 402(6760):390–393, Nov 1999. http://dx.doi.org/10.1038/46503 doi:10.1038/46503.

[10] A. Kitaev, D. Mayers, and J. Preskill. Superselection rules and quantum protocols. Phys. Rev. A, 69:052326, May 2004. http://dx.doi.org/10.1103/PhysRevA.69.052326 doi:10.1103/PhysRevA.69.052326.

[11] E. Knill. Non-binary unitary error bases and quantum codes. Jun 1996. http://dx.doi.org/10.2172/373768 doi:10.2172/373768.

[12] I. Marvian and R. W. Spekkens. The theory of manipulations of pure state asymmetry: I. basic tools, equivalence classes and single copy transformations. New Journal of Physics, 15(3):033001, 2013.
[13] I. Marvian and R. W. Spekkens. Asymmetry properties of pure quantum states. *Phys. Rev. A*, 90:014102, Jul 2014. http://dx.doi.org/10.1103/PhysRevA.90.014102
doi:10.1103/PhysRevA.90.014102.

[14] B. Musto and J. Vicary. Quantum Latin squares and unitary error bases. *ArXiv e-prints*, April 2015. http://arxiv.org/abs/1504.02715 arXiv:1504.02715.

[15] A. Peres and P. F. Scudo. Unspeakable quantum information. *eprint arXiv:quant-ph/0201017*, January 2002. http://arxiv.org/abs/quant-ph/0201017 arXiv:quant-ph/0201017.

[16] F. Szöllősi. *Construction, classification and parametrization of complex Hadamard matrices*. PhD thesis, The University of Wisconsin - Madison, 2011.

[17] R. F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001.