Tight Reference Frame–Independent
Quantum Teleportation

Dominic Verdon

Department of Computer Science
University of Oxford
Oxford, UK

`dominic.verdon@cs.ox.ac.uk`

Jamie Vicary

Department of Computer Science
University of Oxford
Oxford, UK

`jamie.vicary@cs.ox.ac.uk`

We give a tight scheme for teleporting a quantum state between two parties whose reference frames are misaligned by an action of a finite symmetry group. 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. In the terminology of Peres and Scudo, our protocol relies on classical communication of *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, 11, 13, 14]. It was recognised some time ago [7] that a shared reference frame is a hidden implicit assumption in the conventional description of quantum teleportation, an assumption which it is reasonable to challenge, since it is clearly possible that two parties attempting teleportation across a large distance will be uncertain about their relative reference frames. Quantum teleportation is a foundational quantum protocol with important applications [9, 10]; the problem of teleporting a quantum state between two parties who do not share a reference frame is therefore natural and important.

A successful reference frame–independent teleportation protocol is one where any observer with their own fixed reference frame will agree that Alice's quantum state has been successfully transferred to Bob, regardless of the orientation of Alice and Bob's frames; this was referred to in [5] as 'teleportation of unspeakable information'. Here we consider perfect teleportation, where Alice's state is transferred to Bob with certainty.

The effect of a change in reference frame alignment on the perceived state of a system may be encoded formally as the unitary action of a group of reference frame transformations on the Hilbert space of the system under consideration. It has been shown [5] that if the group of reference frame transformations contains $U(1)$ and the action is nontrivial, then reference frame–independent teleportation is impossible. In this paper we show that when the group of reference frame transformations is finite, reference frame–independent teleportation is possible in some nontrivial cases.

We will demonstrate that reference frame–independent (RFI) teleportation protocols correspond exactly to *G-equivariant unitary error bases*, a structure we define, and develop methods of constructing these bases when they exist. In particular, we provide a simple sufficient condition for the existence of RFI teleportation protocols for systems of dimension less than 5.

The nature of the classical channel through which the result of Alice's measurement is communicated is crucial to our new protocol. In the terminology of Peres and Scudo [17], our protocol requires classical transmission of *unspeakable information*, rather than of *speakable information*. An example of unspeakable information is the choice of a direction in space, to be agreed by two parties who do not share a common directional reference; no amount of communication through a generic shared classical channel can decide the matter, but the fidelitous transfer from one party to the other of a single oriented physical system, such as an arrow, is sufficient.

We foresee two further applications of this result, both of which merit further investigation:

- *Reference frame hiding.* Our result demonstrates that it is possible for two parties with secret reference frame configurations to perform teleportation of a quantum state without transmitting any information about those configurations, either to each other or to a third party. We have outlined such a scenario in the main example in Section 2.

- *Infinite groups of reference frame transformations.* Although reference frame–independent teleportation is impossible for an infinite Lie group, our result may be useful in the infinite case for developing protocols for imperfect quantum teleportation, a problem which has already been investigated [15]. Firstly, it may be possible in some situations to render the group of reference frame transformations finite using limited prior communication or some other approach. Secondly, imperfect infinite-group reference frame–independent teleportation procedures may be attained as limits of perfect finite-group schemes.

The fundamental concept of a *G*-equivariant unitary error basis was developed from investigations in categorical quantum mechanics [1]. We characterised teleportation schemes as structures internal to the category of finite dimensional Hilbert spaces, and investigated corresponding structures in the category of unitary representations of a finite group; these corresponding structures were exactly the *G*-equivariant unitary error bases. Following their discovery, further investigation demonstrated their relevance to the problem of RFI teleportation. This exemplifies the utility of categorical quantum mechanics as a toolkit for developing new and interesting concepts in quantum information.

The outline of the paper is as follows. In Section 2 we give an informal worked example of our procedure, and in Section 3 we provide a more formal presentation, along with further examples. In Section 4 we show how reference frame–independent teleportation schemes are related to ideas in categorical quantum mechanics. In Section 5 we prove a variety of existence, nonexistence and construction results for *G*-equivariant unitary error bases.

1.2 Previous results

It was demonstrated in [5] that teleportation is impossible when the group of reference frame transformations is a infinite 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 open the question of whether quantum teleportation is possible in the case of a finite group of reference frame transformations, without additional resources or prior communication. The protocol we exhibit provides an affirmative answer to this question.

A number of other solutions for the finite case have 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 [11], where 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; see [2]. This increases the amount of classical information that must be communicated for successful teleportation. Moreover, this procedure is not robust against changes in the alignment of Alice and Bob's reference frames, which must stay constant if the protocol is to succeed. Our protocol, in contrast, is robust against reference frame changes even while the classical message from Alice to Bob is in transit. We only require that the alignment of Bob's reference frame is constant for the short time between his receipt of the classical information and his application of the unitary correction.

However, we emphasize that our solution applies only when the system to be teleported carries a representation of the group of reference frame transformations G which admits a G-equivariant unitary error basis. The other approaches described above do not have this limitation.

2   Example of the procedure

In this section we give an informal account of the problem of reference frame–independent quantum teleportation, in the specific case where the systems are two-dimensional and the reference frame corresponds to a choice of spatial direction. This is followed by a more general and mathematically precise treatment in the next section.

Alice and Bob are quantum information theorists in separate laboratories, which do not necessarily have the same orientation in space. However, their relative orientations are not completely unknown: we are given some finite subgroup $G \subset SO(3)$, the group of rigid spatial rotations, with the promise that there is some element $g \in G$ which relates Alice's and Bob's frames. The group G is common knowledge to both parties.

The task is to perform teleportation of a quantum state from Alice to Bob, without revealing their spatial orientations, either to each other or to a potential eavesdropper. There are a variety of reasons why this may be advantageous: this information may be strategically or cryptographically valuable, and hence they may prefer not to divulge it for reasons of privacy; they may prefer to conserve limited bandwidth, and hence to not communicate redundant reference frame alignment information if it can be avoided; or they may simply be disoriented, and not aware of their own orientations.

In this example, we consider the case that $G = \mathbb{Z}_2$, meaning that their laboratories may be in one of two possible orientations which are related by a $180°$ rotation about some given axis. We suppose that

the nontrivial element $a \in G$ acts on the qubit to be teleported as follows:[1]

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

The fact that this matrix is nontrivial corresponds to the fact that the quantum system is not symmetric under the rotation operation.

Alice and Bob agree in advance to perform quantum teleportation as follows. 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 $|\phi_i\rangle = (\mathbb{1} \otimes U_i^{\mathrm{T}}) |\eta\rangle$, where U_i^{T} denotes the transpose of the matrix U_i, the symbol $\mathbb{1}$ denotes the 2-by-2 identity matrix, and $|\eta\rangle$ is the Bell state given above. The U_i are defined as follows:

$$U_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad\qquad U_2 = \frac{1}{4} \begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad\qquad U_3 = \frac{1}{4} \begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

It can readily be checked that this data forms an *unitary error basis*, and so by the results of Werner [18] gives correct data for the execution of an ordinary quantum teleportation procedure for a single qubit, when the shared state is the Bell state $|\eta\rangle$.

If Bob's reference frame is correctly aligned with Alice's, then they are carrying out ordinary quantum teleportation, and the procedure will be successful. However, if his reference direction is upside-down with respect to Alice's, then teleportation does not proceed successfully. From Alice's perspective, Bob's correction is *not* in fact the unitary U_i corresponding to her measurement result, but rather the unitary $\pi(a)^\dagger U_i \pi(a)$; a straightforward calculation then shows that Bob will receive a mixed state, and quantum information has been irrevocably lost. From Bob's perspective, he correctly applied the unitary U_i, but the teleportation failed because the measurement result i that Alice communicated to him did not correspond to the state she actually measured, which was $(\mathbb{1} \otimes \pi(a)) |\phi_i\rangle$.

We now provide a resolution. In our new procedure, rather than communicating the two bits encoding the measurement result to Bob using their shared classical channel, Alice sends two *physical objects* to Bob: arrows, of the sort a medieval archer might use. She orients these arrows according to the measurement result that she obtained, using the following encoding, where her reference direction is written as ↑:

$$0 \mapsto \{\uparrow\uparrow\} \qquad\qquad 1 \mapsto \{\downarrow\downarrow\} \qquad\qquad 2 \mapsto \{\uparrow\downarrow\} \qquad\qquad 3 \mapsto \{\downarrow\uparrow\}$$

One at a time, she physically sends these arrows through space to Bob's laboratory.

Bob 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 corresponding unitary correction. In this case, the two parties have 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. 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

---

[1]It will be seen later that the specific choice of $\pi(a)$ is irrelevant, and all that determines whether reference frame–independent teleportation is possible is the isomorphism class of the representation of G.

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:

$$\pi(a)^\dagger U_1 \pi(a) = U_0 \qquad\qquad \pi(a)^\dagger U_3 \pi(a) = U_2$$
$$\pi(a)^\dagger U_0 \pi(a) = U_1 \qquad\qquad \pi(a)^\dagger U_2 \pi(a) = U_3$$

As a result, the quantum teleporation will conclude successfully, even though Alice's and Bob's reference directions were 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, and the Hilbert space of the entangled resource is of minimal dimension, so this procedure is *tight* in the sense of Werner [18]. 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 the relative alignment between the two reference frames. Finally, it is clear that the procedure would succeed even if Bob's reference frame were constantly changing between the two alignments, as long as the alignment stays constant between Bob's receipt of the arrows and his application of the unitary correction.

3   Mathematical description of the proposal

3.1   Traditional teleportation

Teleportation is a well-understood procedure. It is traditionally formulated under the assumption that both parties have aligned reference frames [3, 18]. (Note that we only consider *tight* quantum teleportation in this paper, where the state spaces of the initial system and of the entangled systems all have the same dimension, which is equal to the number of classical bits transferred, and the procedure succeeds with probability 1; this corresponds to the informal restriction of 'no additional resources or prior communication'.) The traditional formulation is as follows.

Procedure 3.1 (Teleportation without communication of unspeakable information)**.** Alice wants to teleport her state $|\phi\rangle$ to Bob; she has one half of a maximally–entangled bipartite state ω, 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 generic 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 [18], 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:

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

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 ω is the Bell state $\sum_i |i\rangle \otimes |i\rangle$ for any orthonormal basis $\{|0\rangle, |1\rangle, \dots\}$. Alice measures in the maximally–entangled basis $\{|\phi_0\rangle, |\phi_1\rangle, \dots\}$, 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 capable of performing local operations and classical communication. Each party has one half of an entangled state which they created at some point in the past using a shared reference frame. Alice wants to use this entanglement to communicate a quantum state to Bob by teleportation. However, their reference frames are now misaligned; in some observer's fixed reference frame, their frame alignments will be 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?

We will now show that the answer to (i) is almost always negative. First we note the following lemma.

Lemma 3.5. *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 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, $\pi(g_A)^\dagger F_x \pi(g_A) = F_{g_A(x)}$ and $\pi(g_B)^\dagger T_x \pi(g_B) = T_{g_A(x)}$, 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. $\qquad\square$

We now demonstrate that Procedure 3.1 works only for a trivial G-action, rendering it inadequate for reference frame–independent teleportation in any nontrivial case.

Proposition 3.6. *Procedure 3.1 will only work for all reference frame alignments when G acts by a global phase.*

Proof. By Theorem 3.3 and Proposition 3.5, 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 $H \otimes H^* \simeq n \cdot \mathbb{1}$. By straightforward character theory, there can only be one copy of $\mathbb{1}$ 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

In answer to (ii), we will now present our new scheme for teleportation using unspeakable information transfer.

Procedure 3.7 (Teleportation with communication of unspeakable information)**.** Alice wants to teleport her state $|\phi\rangle$ to Bob; she has one half of a maximally-entangled bipartite state ω, and Bob the other. She forms the bipartite system given by her initial system together with her half of the entangled state, and sends it to Bob through a classical channel which is decoherent in the basis F_x. Bob then performs a unitary operator T_x on his half of the entangled state. The data (ω, F_x, T_x) is *correct* if Bob is guaranteed to receive the state $|\phi\rangle$ at the end of the procedure.

Remark 3.8. The key aspect of Procedure 3.7 is that misalignment of reference frames will not affect the way Bob perceives the data arriving through a generic classical channel, but it will affect his perception of the decohered bipartite system. In other words, the information Bob receives from Alice will depend in a nontrivial way on the alignment of his reference frame.

The basic data of Procedure 3.7 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 teleporation schemes under this procedure. We now investigate which of them do.

Definition 3.9 (*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 σ_g of the set $\{1, \ldots, d^2\}$.

Theorem 3.10. *Procedure 3.7 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 $\{\pi(g_B)|\phi_0\rangle, \pi(g_B)|\phi_1\rangle, \ldots\}$, for all g_A, g_B. This is exactly *G*-equivariance of the UEB U_i.

We now demonstrate that this condition is sufficient to guarantee success for Procedure 3.7. 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 *and* performs the correction; the correction therefore corresponds to the measurement and the result follows. □

In Procedure 3.7, we have specified that Alice send the decohered bipartite system itself, since this is always theoretically possible. However, in practise it may be experimentally more practicable to use some other means of classically communicating unspeakable information; the important thing is that the classical data should *itself* carry the same G-action as the corresponding G-equivariant measurement basis. An example was given in Section 2, where Alice's measurement result was encoded in the spatial orientations of some physical objects. In order to demonstrate that this approach is applicable to other types of reference frame uncertainty, we provide two further examples of unspeakable encodings of classical information.

Example 3.11.   (i) *Time.*   Suppose the computational basis states of Alice and Bob's systems are nondegenerate energy eigenstates (for example, eigenstates of the photon number operator). Here they will need to share a time reference. Let the time translation operator $U(t)$ have periodicity $U(t+T) = U(t)$ for some T. Suppose that the group $U(1)$ of time translations has been discretised to some cyclic subgroup $\mathbb{Z}_n$ of translations by T/n. Alice and Bob's reference frame configurations will correspond to their zeroes of time. Signals sent by Alice to to Bob which arrive, according to her reference frame, at time $m_A T/n$, arrive for Bob at a different time $m_B T/n$, depending on the difference between their reference frames. By encoding her measurement result in the time of arrival of signals, Alice may construct G-equivariant teleportation protocols.

   (ii) *Circular polarisation.*   Suppose Alice and Bob are working with photonic qubits whose computational basis states are left and right circular polarisation. In this case, the group of reference frame transformations will correspond to planar rotations of the axes perpendicular to the propagation direction. Suppose that the group $U(1)$ of planar rotations has been discretised to some cyclic subgroup $\mathbb{Z}_n$ of rigid rotations by multiples of $2\pi/n$, and that Alice can classically communicate linearly polarised light to Bob. By communicating frame configurations using beams of linearly polarised light, Alice may encode measurement results in the angle difference between Bob's frame and the commmunicated frame, allowing her to construct G-equivariant teleportation protocols.

4   Classical structures in $\mathrm{Rep}(G)$

Teleportation in the context of a finite group G can be described elegantly in the framework of *categorical quantum mechanics* [1]. One key strategy in this research programme is to understand features of quantum information in terms of the category **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 **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.

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 *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:

$$
\begin{array}{ccc}
\boxed{\text{comultiplication}} & = & c \cdot \boxed{\text{unit}}
\end{array}
\tag{1}
$$

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

Theorem 4.2. *Quantum teleportation procedures in* **FHilb** *correspond precisely to 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 **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* **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 **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 [12]; 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[2], although many construction methods exist [12, 16, 18]. 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 protcols 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 $\mathrm{End}(H) \simeq H \otimes H^*$, all of whose elements are unitary maps.

---

[2]The problem of classifying UEBs is closely related to the difficult problem of classifying Hadamard matrices [8].

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 $\mathrm{End}(H)$, 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-**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 $\mathscr{M} : G\text{-}\mathbf{Set} \to \mathbf{Rep}(G)$, 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 $\mathscr{M}$.*

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, σ_1) and (X_2, σ_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 σ_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 $\mathscr{M}$ is additive; the disjoint union of two G-sets will be sent under $\mathscr{M}$ to the direct sum of their corresponding representations. In order to classify all objects in the image of $\mathscr{M}$, therefore, it is sufficient to find the image of the coset spaces under $\mathscr{M}$. 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 $\mathscr{M}$ on a G-set.

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

$$\chi(g) = |\{ x \in X \mid g \cdot x = x \}| \tag{2}$$

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

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:

Representation / Conjugacy class	()	(1,2)	(1,2,3)
$\mathcal{M}(G/C_1)$	6	0	0
$\mathcal{M}(G/C_2)$	3	1	0
$\mathcal{M}(G/C_3)$	2	0	2
$\mathcal{M}(G/C_4)$	1	1	1

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:*

$$(U_H)_{ij} = \frac{1}{N} H \circ \mathrm{diag}(H,j)^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T,i) \tag{3}$$

Proof. It was already proved in [16] 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 $gU_{ij}g^\dagger = \frac{1}{n} H \circ (g \circ \mathrm{diag}(H,j)^\dagger \circ g^\dagger) \circ H^\dagger \circ (g \circ \mathrm{diag}(H^T,i) \circ g^\dagger)$. We see easily that $g \circ \mathrm{diag}(H,j)^\dagger \circ g^\dagger = g \circ \mathrm{diag}(H^*,j) \circ g^\dagger = \mathrm{diag}(H^* \circ g, j)$. 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 $\mathrm{diag}(H^* \circ g, j) = \mathrm{diag}(g \circ H^*, j) = \mathrm{diag}(H^*, g \cdot j)$. A similar argument works for $\mathrm{diag}(H^T,i)$.   □

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) [16]; 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 ≥ 3 defined by two complex parameters a and b, where all entries on the diagonal are a, and all other entries are b. Let $a = |a|\alpha, b = |b|\beta$ where $\alpha, \beta \in U(1)$ and $|a|, |b| \neq 0$. Then M is unitary precisely when the following conditions are satisfied:*

$$\frac{n-2}{n} \leq |a| \leq 1 \quad (4) \qquad |b|^2 = \frac{1-|a|^2}{n-1} \quad (5) \qquad Re(\alpha^*\beta) = \frac{2-n}{2}\frac{|b|}{|a|} \quad (6)$$

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:

$$|b|^2 = \frac{1-|a|^2}{n-1} \tag{7}$$

$$Re(a^*b) = \frac{2-n}{2}|b|^2. \tag{8}$$

We will demonstrate that (4) is necessary and sufficient for us to find b satisfying these equations. It is obvious that (7) is satisfiable if and only if $|a| \leq 1$. Letting $a = |a|\alpha, b = |b|\beta$, Equation (8) becomes

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

Since $-1 \leq Re(\alpha^*\beta) \leq 1$ and α, β can be freely adjusted to give $Re(\alpha^*\beta)$ any value in that range, we see that the following is necessary and sufficient for (8) to be soluble:

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

Use of the identity (7) and a short calculation demonstrates that this is equivalent to the lower bound in the inequality (4). $\qquad \square$

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 $\mathfrak{S}_n$, where V is the fundamental $(n-1)$-dimensional representation of $\mathfrak{S}_n$).

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 3.6, For $n = 2$ the following family of Hadamard matrices commutes with S_2, where $|a| = |b| = 1/\sqrt{2}$ and $Re(a^*b) = 0$:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

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 (5), it follows that $|a| = 1/\sqrt{n}$. This is compatible with (4) only for $n \leq 4$. $\qquad \square$

References

[1] Samson Abramsky & Bob Coecke (2009): *Categorical Quantum Mechanics*. In Dov M. Gabbay Daniel Lehmann, Kurt Engesser, editor: *Handbook of Quantum Logic and Quantum Structures*, Elsevier, pp. 261–323, doi:10.1016/B978-0-444-52869-8.50010-4.

[2] Stephen Bartlett, Terry Rudolph & Rob Spekkens (2007): *Reference frames, superselection rules, and quantum information*. Rev. Mod. Phys. 79, pp. 555–609, doi:10.1103/RevModPhys.79.555.

[3] Charles Bennett, Giles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres & William K. Wootters (1993): *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Phys. Rev. Lett. 70, pp. 1895–1899, doi:10.1103/PhysRevLett.70.1895.

[4] William Burnside (2004): *Theory of Groups of Finite Order*. Dover Books on Mathematics Series, Dover Publications.

[5] Giulio Chiribella, Vittorio Giovannetti, Lorenzo Maccone & Paolo Perinotti (2012): *Teleportation transfers only speakable quantum information*. Phys. Rev. A 86, p. 010304, doi:10.1103/PhysRevA.86.010304.

[6] Bob Coecke, Dusko Pavlovic & Jamie Vicary (2013): *A new description of orthogonal bases*. Mathematical Structures in Computer Science 23, pp. 555–567, doi:10.1017/S0960129512000047.

[7] Steven J. van Enk (2001): *The physical meaning of phase and its importance for quantum teleportation*. Journal of Modern Optics 48(13), pp. 2049–2054, doi:10.1080/09500340108240906.

[8] Ferenc Szöllősi (2011): *Construction, classification and parametrization of complex Hadamard matrices*. Ph.D. thesis, The University of Wisconsin, Madison.

[9] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel & Hugo Zbinden (2002): *Quantum cryptography*. Rev. Mod. Phys. 74, pp. 145–195, doi:10.1103/RevModPhys.74.145.

[10] Daniel Gottesman & Isaac L. Chuang (1999): *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*. Nature 402(6760), pp. 390–393, doi:10.1038/46503.

[11] Alexei Kitaev, Dominic Mayers & John Preskill (2004): *Superselection rules and quantum protocols*. Phys. Rev. A 69, p. 052326, doi:10.1103/PhysRevA.69.052326.

[12] Emanuel Knill (1996): *Non-binary unitary error bases and quantum codes*. doi:10.2172/373768.

[13] Iman Marvian & Robert W. Spekkens (2013): *The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations*. New Journal of Physics 15(3), p. 033001, doi:10.1103/physreva.90.014102.

[14] Iman Marvian & Robert W. Spekkens (2014): *Asymmetry properties of pure quantum states*. Phys. Rev. A 90, p. 014102, doi:10.1103/PhysRevA.90.014102.

[15] Ugo Marzolino & Andreas Buchleitner (2015): *Quantum teleportation with identical particles*. Phys. Rev. A 91, p. 032316, doi:10.1103/PhysRevA.91.032316.

[16] Benjamin Musto & Jamie Vicary (2016): *Quantum Latin squares and unitary error bases*. Quantum Information and Computation. To appear.

[17] Asher Peres & Petra F. Scudo (2002): *Unspeakable quantum information*. quant-ph/0201017.

[18] Reinhard Werner (2001): *All teleportation and dense coding schemes*. Journal of Physics A: Mathematical and General 34(35), p. 7081, doi:10.1088/0305-4470/34/35/332.