

# Algebraic quantum structures for reference frame-independent quantum teleportation and pseudo-telepathy

Dominic Verdon

A thesis presented for the degree of  
Doctor of Philosophy



Department of Computer Science  
University of Oxford

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>I</b>	<b>Reference frame-independent quantum teleportation</b>	<b>7</b>
<b>2</b>	<b>Reference frames in quantum teleportation</b>	<b>8</b>
2.1	Reference frames in quantum teleportation . . . . .	8
2.1.1	Reference frames and transformations . . . . .	9
2.1.2	Quantum teleportation . . . . .	10
2.1.3	Example: reference frame uncertainty in ground-to satellite teleportation . . . . .	11
2.2	Categorical-algebraic approach . . . . .	13
2.2.1	A categorical setting for reference frames in quantum mechanics	13
2.2.2	An algebraic formulation of teleportation schemes . . . . .	15
<b>3</b>	<b>Perfect tight reference frame-independent teleportation for finite transformation groups</b>	<b>19</b>
3.1	Introduction . . . . .	19
3.2	Example . . . . .	22
3.3	Perfect tight reference frame-independent teleportation for finite trans- formation groups . . . . .	25
3.4	Requirement I: Unspeakable channels . . . . .	28
3.4.1	Construction from quantum systems . . . . .	28
3.4.2	Construction from shared classical system . . . . .	28
3.5	Requirement II: Equivariant unitary error bases . . . . .	32
3.5.1	Classification for qubits . . . . .	32
3.5.2	Higher dimensions . . . . .	46
3.6	Appendix to Chapter 3 . . . . .	49
3.6.1	Existence of $G$ -invariant maximally entangled states . . . . .	49

<b>4</b>	<b>Perfect and tight teleportation schemes for compact Lie transformation groups</b>	<b>50</b>
4.1	Introduction . . . . .	50
4.2	Example . . . . .	55
4.3	Encoding schemes for continuous channels . . . . .	60
4.3.1	Continuous unspeakable channels . . . . .	60
4.3.2	Compatible encoding schemes for continuous actions . . . . .	60
4.4	Two teleportation procedures . . . . .	61
4.4.1	Teleportation without realignment . . . . .	62
4.4.2	Teleportation with realignment . . . . .	64
4.5	Continuous reference frame channels . . . . .	65
4.5.1	Continuous reference frame channels . . . . .	65
4.5.2	Encoding schemes for continuous reference frame channels . . . . .	67
4.6	Teleportation schemes for compact Lie transformation groups . . . . .	69
4.6.1	Tight teleportation scheme . . . . .	69
4.6.2	Perfect teleportation scheme . . . . .	70
4.7	Phase reference frame uncertainty revisited . . . . .	70
4.8	Channel purity calculations for tight scheme . . . . .	73
4.8.1	Map purity . . . . .	73
4.8.2	Calculations for $U(1)$ . . . . .	75
4.8.3	Calculations for $SU(2)$ . . . . .	76
4.9	Appendix to Chapter 4 . . . . .	78
4.9.1	Proof of Theorem 6 . . . . .	78
4.9.2	Voronoi cells . . . . .	80
<b>II</b>	<b>Quantum pseudo-telepathy</b>	<b>83</b>
<b>5</b>	<b>Pseudo-telepathy and noncommutative mathematics</b>	<b>84</b>
<b>6</b>	<b>Quantum bijections and quantum isomorphisms</b>	<b>90</b>
6.1	Introduction . . . . .	90
6.1.1	Background . . . . .	90
6.1.2	Overview of this chapter . . . . .	92
6.1.3	Notation and conventions. . . . .	93
6.1.4	The graphical calculus of string diagrams . . . . .	93
6.2	Frobenius monoids and Gelfand duality . . . . .	94
6.2.1	Frobenius monoids . . . . .	94
6.2.2	Gelfand duality for finite sets . . . . .	96

6.3	Quantum bijections . . . . .	98
6.3.1	Definition . . . . .	98
6.3.2	Quantum bijections between classical sets . . . . .	100
6.3.3	The direct sum of quantum bijections . . . . .	101
6.3.4	The category $\mathbf{QPerm}(A)$ . . . . .	102
6.3.5	Splitting in $\mathbf{QPerm}(A)$ . . . . .	104
6.3.6	Classification of quantum bijections . . . . .	105
6.4	Quantum graph theory . . . . .	106
6.4.1	Quantum graphs . . . . .	106
6.4.2	Quantum graph isomorphisms . . . . .	107
<b>7</b>	<b>A group-theoretical construction of quantum pseudo-telepathy</b>	<b>109</b>
7.1	Introduction . . . . .	109
7.1.1	Overview . . . . .	109
7.1.2	Summary . . . . .	110
7.2	Technical background . . . . .	112
7.2.1	Groups of central type . . . . .	112
7.2.2	Projective representation theory . . . . .	113
7.2.3	Representations of groups of central type . . . . .	115
7.2.4	Graphs with symmetry . . . . .	118
7.3	Quantum bijections from classical symmetries . . . . .	119
7.3.1	Simple dagger Frobenius algebras in $\mathbf{Hilb}_G$ . . . . .	119
7.3.2	Splitting the algebras . . . . .	122
7.3.3	Composition and direct product . . . . .	126
7.4	Quantum pseudo-telepathy . . . . .	129
7.4.1	From classical symmetries to graph isomorphisms . . . . .	129
7.4.2	The graph $\Gamma_{L,\psi}$ . . . . .	130
7.4.3	Conditions for pseudo-telepathy . . . . .	133
7.5	Linear constraint systems . . . . .	135
7.5.1	Definition . . . . .	135
7.5.2	Operator solutions from groups of central type . . . . .	136
7.5.3	A characterisation of quantum solutions obtained from central type groups . . . . .	139
<b>III</b>	<b>Conclusions</b>	<b>144</b>
<b>8</b>	<b>Conclusions</b>	<b>145</b>

# Chapter 1

## Introduction

Quantum information theory deals with the application of quantum mechanical systems to information processing tasks such as communication, computation and cryptography [21, 44, 79]. This endeavour has brought together physicists, mathematicians and computer scientists, and has led to a fruitful interchange of ideas from these three fields.

Theoretical computer science employs category theory in areas such as categorical logic [62], type systems [46], and programming language semantics [39]. Category theory also plays a crucial unifying role in many areas of modern mathematics. The philosophy of category theory is that one should consider a mathematical object, not in terms of its elements, but rather in terms of the structure-preserving maps (morphisms) between it and other such objects. *Categorical quantum mechanics* [1] applies categorical techniques to the study of quantum information theory. The basic category of interest is **FHilb**, whose objects and morphisms are finite-dimensional Hilbert spaces and linear maps respectively. Quantum structures such as finite-dimensional  $C^*$ -algebras can be treated abstractly as objects in this category carrying certain algebraic structure.

Various positive consequences of this change in perspective have already been explored in the literature:

- A maximally entangled bipartite pure state of a pair of identical systems is precisely the unit of a dagger duality in **FHilb**; quantum teleportation can therefore be understood as a consequence of the ‘snake equations’ defining such a duality [1, Section 2.1].
- As a compact closed category [55], **FHilb** admits a flexible and intuitive graphical calculus [52, 53, 88] from which the Choi-Jamiołkowski isomorphism and

the interchange law for monoidal product and composition emerge trivially.

- Formulating quantum structures in terms of maps gives them a process-theoretic interpretation; orthonormal bases, for instance, can be defined by copying and comparison of classical information [30]. Quantum theory can even be rederived using axioms inspired by the process-theoretic approach [87].
- Categorical-algebraic structures relevant to quantum mechanics can be considered in other categories with similar structure, or vice versa, leading to new insights in quantum and other theories [48, 80].

In this thesis we will further demonstrate the utility of the categorical-algebraic perspective in quantum information theory by obtaining new insights in two different areas.

**Reference frame-independent quantum teleportation.** Based on an algebraic formulation of quantum teleportation in the category of finite dimensional unitary representations of a compact Lie group, we propose schemes for quantum teleportation between parties with misaligned reference frames. These schemes do not depend on prior alignment or the use of decoherence-free subspaces, and are robust against changes in reference frame alignment during execution. They utilise algebraic structures called equivariant unitary error bases, which we completely classify for qubits. We consider applications of these results, and show how similar schemes could be developed for other multi-party protocols such as quantum key distribution.

Most of this work appeared in the following papers:

- *Tight quantum teleportation without a shared reference frame* (with Jamie Vicary)  
<https://arxiv.org/abs/1710.01060>  
Phys. Rev. A 98, 012306 (2018).
- *Quantum teleportation with infinite reference frame uncertainty and without prior alignment* (with Jamie Vicary)  
<https://arxiv.org/abs/1802.09040>  
Submitted for publication.
- *Tight reference frame-independent quantum teleportation* (with Jamie Vicary)  
<https://arxiv.org/abs/1710.01060>  
QPL2016, EPTCS, 236:202-214 (2017).

**Quantum graph isomorphisms.** In two recent papers, a compositional theory of quantum functions was developed, which allows one to use categorical and algebraic techniques to treat controlled projective measurement (considered as a ‘quantum assisted function’ from the control set to the outcome set). A consequence of this work is a classification and construction of quantum graph isomorphisms, perfect quantum strategies for a nonlocal game. Here we give a concrete presentation of this construction, and show how it can be used to construct instances of quantum pseudo-telepathy.

- *A compositional approach to quantum functions* (with Benjamin Musto and David Reutter)

<https://arxiv.org/abs/1711.07945>

J. Math. Phys. 59, 081706 (2018).

- *The Morita theory of quantum graph isomorphisms* (with Benjamin Musto and David Reutter)

<https://arxiv.org/abs/1801.09705>

Commun. Math. Phys. (2018).

**Credit.** The research in Part 1 of this thesis was conducted in collaboration with Jamie Vicary. The research in Part 2 of this thesis was conducted in collaboration with Benjamin Musto and David Reutter.

**Thanks.** Thanks to Jamie Vicary, my supervisor, for patient direction and encouragement throughout the last four years. Thanks to Benjamin Musto and David Reutter, for an enjoyable and fruitful collaboration. Thanks to my parents, who taught me intellectual curiosity and perseverance. I thank God for my limited understanding of this small part of what He creates; I am humbled by my ignorance.

# Part I

## Reference frame-independent quantum teleportation



# Chapter 2

## Reference frames in quantum teleportation

### 2.1 Reference frames in quantum teleportation

A shared reference frame is an important implicit assumption underlying the correct execution of many quantum protocols [14, 44, 45, 56, 67, 68, 94]. As quantum technologies move into space [7, 84, 104] and handheld devices [37, 38, 99], scenarios where this assumption is violated are naturally encountered. This problem has already received attention in the case of ground-to-satellite quantum key distribution [7, 61, 63, 93]; there is also a smaller body of work on quantum teleportation without a shared reference frame [25, 69, 70], which is increasingly important as quantum repeaters [75] and ground-to-satellite quantum teleportation [84] become experimentally viable.

One general approach to overcoming reference frame misalignment is simply to align reference frames before beginning the quantum procedure. This problem has been studied for specific cases including temporal [23], directional [8, 81], Cartesian [24] and permutational [59] reference frames; see [14] for a general review. However, this is not applicable if reference frame alignment drifts significantly on timescales shorter than the time taken to perform the protocol, and may be difficult if alignment between more than two parties is necessary [50, 51]. Prior alignment also involves communication of reference frame information, which may be cryptographically sensitive in some scenarios [13, 49, 56]; although it is possible to align reference frames in a cryptographically secure way [26], this requires additional resources such as shared classical randomness. Another general approach involves the use of decoherence-free subspaces [64]; as this requires larger Hilbert spaces, prac-

tical implementation can be nontrivial, although experimental solutions have been developed for optical systems [34].

In the following three chapters we will discuss the particular problem of *quantum teleportation* in the situation of reference frame misalignment. In particular, we will exhibit new schemes for teleportation which are resistant to the effect of reference frame misalignment, and which do not require prior alignment or the use of decoherence free subspaces.

### 2.1.1 Reference frames and transformations

First, we recall the mathematical formalism of reference frame transformations in quantum mechanics [14]. Let  $\mathcal{F}$  be the space of configurations of the reference frame, and let  $V$  be the  $d$ -dimensional Hilbert space of a system whose states are described with respect to this frame. Let  $G$  be the group of reference frame transformations, which has a transitive left action on  $\mathcal{F}$ . The Hilbert space  $V$  carries a unitary representation  $\rho : G \rightarrow B(V)$ , which encodes how states transform under a change in frame configuration: a state with vector  $|\psi\rangle$  in frame configuration  $f \in \mathcal{F}$  will have vector  $\rho(g)|\psi\rangle$  in configuration  $g \cdot f$ . Let  $g_{AB} \in G$  be the reference frame transformation taking Alice's frame  $f_A \in \mathcal{F}$  onto Bob's frame  $f_B \in \mathcal{F}$ ; that is,  $f_B = g_{AB} \cdot f_A$ .

**Proposition 1.** *A state with vector  $|\psi\rangle$  in Bob's frame has vector  $\rho(g)^\dagger |\psi\rangle$  in Alice's frame. A linear map with matrix  $M : V \rightarrow V$  in Bob's frame has matrix  $\rho(g)^\dagger M \rho(g)$  in Alice's frame. For any  $X \in L(V)$ , let  $[X] : L(V) \rightarrow L(V)$  be defined by  $[X](\rho) = X\rho X^\dagger$ ; with this notation, a general quantum channel  $\Phi : L(V) \rightarrow L(V)$  in Bob's frame is the operation  $[\rho(g)^\dagger] \circ \Phi \circ [\rho(g)]$  in Alice's frame.*

*Proof.* By definition a state described in Alice's frame as  $|\psi\rangle$  will be described in Bob's frame as  $\rho(g)|\psi\rangle$ ; the first equation follows immediately.

For the linear maps, consider that a linear map is defined by its matrix elements in some orthonormal basis. Bob performs the operation with matrix elements  $M_{ij}$  in his frame; that is, he performs the operation  $M_B$  such that  $\langle i_B | M_B | j_B \rangle = M_{ij}$ . Now note that  $|i_B\rangle = \rho(g)^\dagger |i_A\rangle$ , so  $M_{ij} = \langle i_B | M_B | j_B \rangle = \langle i_A | \rho(g) M_B \rho(g)^\dagger | j_A \rangle$ . In Alice's frame, therefore, Bob has performed the operation  $M_B$  such that  $\rho(g) M_B \rho(g)^\dagger = M_A$ ; this operation is therefore related to  $M_A$  by  $M_A = \rho(g)^\dagger M_B \rho(g)$ . To extend the same argument to general quantum channels, use the fact that all channels can be expressed using Kraus maps:

$$\Phi(\rho) = \sum_i E_i \rho E_i^\dagger$$

We already know how the  $E_i$  transform, so the result follows.  $\square$

## 2.1.2 Quantum teleportation

We begin by recalling the conventional teleportation procedure. This procedure was called ‘tight’ by Werner [103], as the dimensions of the Hilbert spaces involved are minimal.

**Procedure 1** (Conventional tight teleportation [18]). Alice holds an  $n$ -dimensional quantum system, prepared in a state  $|\psi\rangle$ . Separately, Alice and Bob hold an entangled pair of  $n$ -dimensional quantum systems, in a maximally entangled state  $(1 \otimes X) |\eta\rangle$  for some unitary  $X$ , where

$$|\eta\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n |ii\rangle$$

is the generalised Bell state.<sup>1</sup> Alice performs a joint measurement on the system to be teleported and her entangled system, described by an orthonormal basis  $|\phi_i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ . She communicates the classical measurement result  $i$  to Bob using a perfect classical channel; Bob then performs the unitary correction  $U_i$  on his half of the entangled state. The procedure is successful if Bob’s system is now in the state  $|\psi\rangle$ .

A complete description of correct procedures was given by Werner.

**Definition 1.** For a Hilbert space  $H$ , a *unitary error basis* (UEB) is a basis of unitary operators  $\{U_i\}_{i \in I}$ , with  $I = \{0, 1, \dots, \dim(H)^2 - 1\}$ , such that for all  $i, j \in I$  we have:

$$\text{Tr}(U_i^\dagger U_j) = \delta_{ij} \dim(H) \tag{2.1}$$

Under this correspondence, we construct Alice’s joint measurement basis as

$$|\phi_i\rangle := (\mathbb{1} \otimes X^T U_i^T) |\eta\rangle, \tag{2.2}$$

and Bob performs the correction  $U_i$  from the unitary error basis when he receives the measurement result  $i$  from Alice. Werner showed [103, Theorem 1] that all correct measurement and correction data for Procedure 1 can be obtained from a unitary error basis in this way.

---

<sup>1</sup>All maximally entangled states of a bipartite system are of this form.

### 2.1.3 Example: reference frame uncertainty in ground-to satellite teleportation

We can now present an example of the effect of reference frame misalignment on teleportation, based on a recent experimental implementation of ground-to-satellite quantum teleportation [84].

Alice is on Earth and possesses a qubit  $\rho$ , which she wants to transfer to Bob on an orbital satellite. They share an optical link through which they can perform quantum or classical communication, mediated by individual photons or classical beams of light. They use a similar protocol to that of Bouwmeester et al [20], except without postselecting on a single outcome of Alice’s measurement. Explicitly:

1. Alice creates a pair of photons in a Bell state  $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , where  $|0\rangle$  is left and  $|1\rangle$  right circular polarisation<sup>2</sup>.
2. Alice transmits one of these photons to Bob through the optical link, using the link as a quantum channel. Bob, upon receipt, transfers its state to some memory qubit.
3. Alice performs a measurement on her memory qubit and the other entangled photon, in the Bell basis  $|\phi_i\rangle = (\mathbb{1} \otimes U_i^T) |\phi^+\rangle$ . ( $U_i$  will be defined shortly.)
4. Alice communicates the outcome  $i$  corresponding to her measured state  $|\phi_i\rangle$  to Bob through the optical link, using the link as a classical channel. (She could, for instance, encode the result in the duration of a number of light pulses.)
5. Bob performs a corresponding Pauli correction  $U_i$  on his memory qubit:

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad U_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad U_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad U_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

If the operations are performed perfectly this will result in perfect teleportation, as can easily be checked.

Fidelitous communication of one half of the photon pair is an experimental problem which has been treated elsewhere with some success [84]. However, there is another, equally significant, problem in Stage 5: *reference frame uncertainty arising from rotation of the satellite*.<sup>3</sup> The situation is shown in Figure 2.1. The reference

---

<sup>2</sup>Polarisation is a suitable degree of freedom because of its known resilience to atmospheric turbulence on travel through free space [4]; viability in this setting has already been demonstrated experimentally [84].

<sup>3</sup>This problem was not discussed in the recent paper of Ren et al. [84], since their protocol postselected on measurement outcome 0, for which Bob need not perform a correction operation.

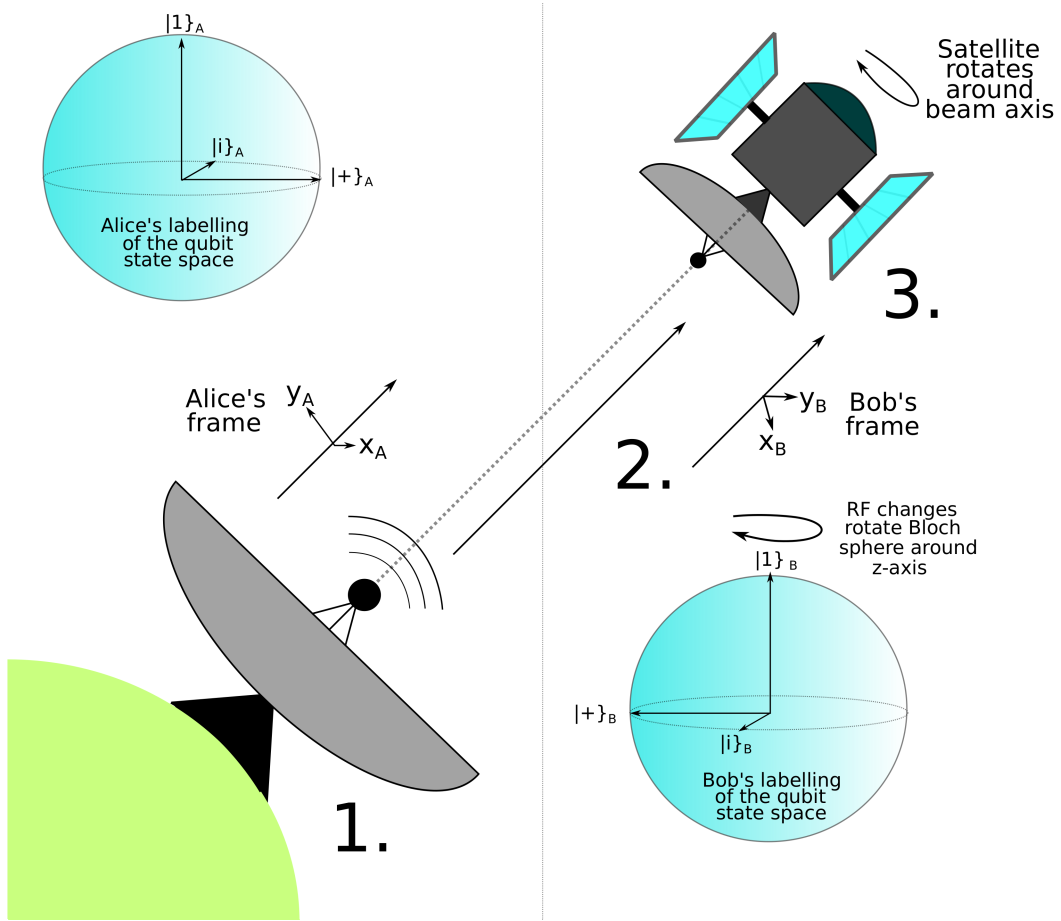


Figure 2.1: The ground-to-satellite teleportation setup.

frame transformation group is the 2D rotation group  $U(1)$ . If  $\theta \in [0, 2\pi)$  is the angle of a clockwise rotation of the 2D Cartesian frame, we have the following action on the state of the photon:

$$\theta \mapsto \rho(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2i\theta} \end{pmatrix}$$

Here the vector acted on by the matrix is  $(v_L, v_R)^T$ , where  $v_L$  is the left and  $v_R$  the right circular polarisation coefficient. The transfer of the photon to Bob's memory qubit will require some operation in his frame, so the final state of the memory qubit will carry the same action of the transformation group.

We work in Alice's reference frame. Suppose that her measurement result is  $i$ . Due to the unknown rotation of the satellite, the correction Bob performs will not be  $U_i$ , but rather  $\rho(\theta)^\dagger U_i \rho(\theta)$ , and it is easy to check that the state of Bob's qubit following the protocol is  $\rho(\theta)^\dagger U_i \rho(\theta) U_i^\dagger |\psi\rangle$ , where Alice's original state was  $|\psi\rangle$ . Since we do not know the value of  $\theta \in U(1)$  which describes the true reference frame misalignment, we must 'twirl' [14]—that is, average over the entire group  $U(1)$ —to obtain the effective final state. If Alice's initial state is  $\sigma$ , and she measures  $i$ , then Bob's final state is  $\sigma'_i$ , given as follows:

$$\sigma'_i = \frac{1}{2\pi} \int_0^{2\pi} d\theta \mathcal{C}[\rho(\theta)^\dagger U_i \rho(\theta) U_i^\dagger](\sigma) \quad (2.3)$$

Here and throughout the following two chapters we use the notation  $\mathcal{C}[M](\sigma) = M\sigma M^\dagger$ . If Alice measures 0 or 3, the channel works perfectly, since  $U_0$  and  $U_3$  are stabilised under conjugation by elements of  $\rho(U(1))$ . However, if Alice measures 1 or 2 the channel will be totally decohering. On average, the channel therefore has the following action:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b/2 \\ c/2 & d \end{pmatrix} \quad (2.4)$$

In what follows we will discuss how to achieve a higher quality of teleportation in this situation and others. We will return to this example in Section 4.7.

## 2.2 Categorical-algebraic approach

### 2.2.1 A categorical setting for reference frames in quantum mechanics

In order to gain some insight into the problem discussed in the previous section, we introduce a categorical setting for quantum mechanics which incorporates reference

frame-dependence. Let  $G$  be the group of reference frame transformations, which we assume to be a compact Lie group. We consider the category  $\mathbf{Rep}(G)$ , whose objects are finite dimensional unitary representations of  $G$ ; we write these representations as  $(H, \pi)$ , where  $H$  is the underlying Hilbert space and  $\pi : G \rightarrow \text{End}(H)$  is the homomorphism specifying the representation. The morphisms  $f : (H_1, \pi_1) \rightarrow (H_2, \pi_2)$  are *intertwiners*; that is, linear maps satisfying the equation

$$\pi_2(g) (f(v)) = f (\pi_1(g) (v)). \quad (2.5)$$

The category  $\mathbf{Hilb}$  of finite dimensional Hilbert spaces and linear maps is a special case of  $\mathbf{Rep}(G)$  where  $G$  is trivial. The generalisation  $\mathbf{Rep}(G)$  preserves many of the properties of  $\mathbf{Hilb}$ ; it has duals, for instance, and a direct sum such that every object splits as a sum of simple objects (the irreducible representations). There is a faithful *fibre functor*  $\mathbf{Rep}(G) \rightarrow \mathbf{Hilb}$ , which takes each representation  $(H, \pi)$  to its underlying Hilbert space  $H$ , and each intertwiner to its underlying linear map.

There are two equivalent ways to interpret the morphisms in  $\mathbf{Rep}(G)$ . The first is in terms of a *superselection rule* placing restrictions on permissible transitions. From this perspective, the objects of  $\mathbf{Rep}(G)$  are superselected quantum systems, the superselection sectors are the isotypic components of the representation, and the morphisms are permissible transitions. In fact, up to particle statistics, the categories  $\mathbf{Rep}(G)$  capture *all* superselection rules for particles in  $(3 + 1)$  dimensions. Indeed, the following Tannaka-type theorem of Doplicher and Roberts [35] shows that the *symmetric tensor \*-categories* associated with superselection rules are all categories of representations of compact Lie groups, up to a  $\mathbb{Z}_2$ -grading.

**Theorem 1** ([74, Theorem 2.18]). *For any symmetric tensor \*-category  $\mathbf{C}$ , there exists a compact Lie supergroup<sup>4</sup>  $(G, k)$ , unique up to isomorphism, and an equivalence  $F : \mathbf{C} \rightarrow \mathbf{Rep}(G, k)$ .*

The bosonic sector of any superselection rule can therefore be described using  $\mathbf{Rep}(G)$ , where  $G$  is the corresponding compact Lie group.

The second interpretation makes explicit use of reference frames. In this interpretation, a certain reference frame with transformation group  $G$  is fixed; the objects of  $\mathbf{Rep}(G)$  are quantum systems described according to that frame, and the morphisms are reference frame-independent transformations; that is, transformations which will be described or performed identically regardless of the configuration of the reference frame.

Superselection and reference frame dependence are physically very closely connected. This was noted as far back as the work of Aharonov and Bohm [3], and

---

<sup>4</sup>[74, Definition 2.13].

has been considered more recently in the theory of *quantum reference frames* [14]. The connection may be briefly summarised as follows. In one direction, reference frame dependence induces a superselection restriction when there is no reference frame available to break the symmetry of a quantum system; in this case, the permitted transitions are precisely the frame-independent transitions, and the superselection rule is therefore described by the category  $\mathbf{Rep}(G)$ . On the other hand, one may break a superselection restriction corresponding to a compact group by using a physical system carrying the regular representation of  $G$  as a *quantum reference frame* [3, 14, 56], following the prescription in [56, Section II.C]. In this case the reference frame system is sometimes called a *reservoir*.

For our work on quantum teleportation, we will consider  $\mathbf{Rep}(G)$  as the category of systems described according to a fixed reference frame with transformation group  $G$ . However, it is worth bearing in mind that the categorical structures we describe here may also be interpreted in terms of a superselection rule.

### 2.2.2 An algebraic formulation of teleportation schemes

We now formulate teleportation procedures as algebraic structures in the category  $\mathbf{Hilb}$  of finite dimensional Hilbert spaces and linear maps, before investigating the corresponding structures in the category  $\mathbf{Rep}(G)$ .

It was shown by Coecke et al. [30] that orthonormal bases correspond precisely to special dagger commutative Frobenius algebras, or *classical structures*, in  $\mathbf{Hilb}$ . Indeed, every orthonormal basis  $\{|i\rangle\}$  of a Hilbert space  $V$  defines

- a *copying* map

$$\begin{aligned} \delta : V &\rightarrow V \otimes V \\ |i\rangle &\mapsto |i\rangle \otimes |i\rangle, \end{aligned}$$

which perfectly copies every vector in the orthonormal basis;

- a *comparison* map

$$\begin{aligned} m : V \otimes V &\rightarrow V \\ |i\rangle \otimes |j\rangle &\mapsto \delta_{ij} |i\rangle, \end{aligned}$$

which checks equality of two basis states;



- a *unit* map

$$\mathbb{1} \rightarrow V$$

$$1 \mapsto \frac{1}{\dim(V)} \sum_i |i\rangle,$$

where  $\mathbb{1}$  is the one-dimensional Hilbert space, which maps the scalar unit to the normalised sum over basis elements;

- and a *counit* map

$$\epsilon : V \rightarrow \mathbb{1}$$

$$|i\rangle \mapsto 1,$$

which takes every basis vector to the scalar unit.

Together, these maps obey the relations of a special commutative dagger Frobenius algebra. Moreover, from such an algebra, it is possible to recover the orthonormal basis defining it as the set of ‘copyable states’ [30, Theorem 5.1.]. Orthonormal bases therefore acquire a process-theoretic interpretation as structures permitting the extraction, copying and comparison of classical data from a quantum system.

We consider teleportation from this perspective. Recalling Definition 1, we make a categorical-algebraic definition of a teleportation procedure. We shall use tensor diagrams throughout this thesis; the first appears here. The wires correspond to Hilbert spaces and the boxes to linear maps, and they are read from bottom to top. Arrows on the wires are used to distinguish Hilbert spaces from their duals; a Hilbert space  $H$  has a wire with an upwards arrow, and the dual space  $H^*$  has a wire with a downwards arrow.

**Definition 2.** In the category of finite-dimensional Hilbert spaces and linear maps, a *quantum teleportation procedure* on a Hilbert space  $H$  is a classical structure on the object  $H \otimes H^*$ , satisfying the following condition, where  $c$  is some scalar:

The diagram shows an equality between two tensor expressions. On the left, a light blue box labeled 'copying' has three vertical wires passing through it. The top wire has an upward arrow, the middle wire has a downward arrow, and the bottom wire has an upward arrow. A curved line (a 'cup') connects the top and middle wires above the box, and another curved line (a 'cap') connects the middle and bottom wires below the box. On the right, a light blue box labeled 'unit' has two vertical wires passing through it. The top wire has an upward arrow and the bottom wire has a downward arrow. To the right of the 'unit' box is a single vertical wire with an upward arrow. The entire right-hand side is preceded by a scalar 'c'. The equation is labeled (2.6) on the far right.

Here the ‘cup’ and ‘cap’ are defined as in (6.2).

By the above discussion, the copyable states form an orthonormal basis of  $V \otimes V^* \simeq \text{End}(V)$ . We now show that this equality imposes unitarity of the elements of this basis, recovering the definition of a unitary error basis (Definition 1). We can expand the copying map in terms of the orthonormal basis elements:

$$\text{copy} = \sum_i \begin{array}{c} \uparrow \downarrow \quad \uparrow \downarrow \\ \triangleleft i \quad \triangleleft i \\ \uparrow \downarrow \\ \triangleleft i \\ \uparrow \downarrow \end{array}$$

Now using the snake equations (6.3) we write the elements of the orthonormal basis (which are matrices) as:

$$\begin{array}{c} \uparrow \downarrow \\ \triangleleft i \end{array} = \begin{array}{c} \uparrow \downarrow \\ \triangleleft i \\ \uparrow \downarrow \end{array} \text{ (with a loop) } =: \begin{array}{c} \uparrow \\ \boxed{M} \\ \downarrow \end{array}$$

Using this, we expand the LHS of (2.6) and simplify using the snake equations:

$$\sum_i \begin{array}{c} \uparrow \downarrow \\ \boxed{M_i} \\ \uparrow \downarrow \\ \boxed{M_i^\dagger} \\ \uparrow \downarrow \end{array} = \sum_i \begin{array}{c} \uparrow \downarrow \\ \boxed{M_i} \\ \uparrow \downarrow \\ \boxed{M_i^\dagger} \\ \uparrow \downarrow \end{array}$$

We now expand the RHS:

$$\sum_i \begin{array}{c} \uparrow \downarrow \\ \boxed{M_i} \\ \uparrow \downarrow \end{array}$$

From this and orthonormality of the matrix basis, it is clear that  $M_i M_i^\dagger = \mathbb{1}$ . The orthonormal basis of matrices is therefore unitary.

What have we gained by redefining a unitary error basis in this way? Firstly, this equation has a clear operational interpretation. On the left hand side, an entangled

state is shared between Alice and Bob. Alice performs a measurement in the unitary error basis, and transmits the measurement information to Bob. Bob then uses the classical information received to perform a correction operation. This is formally equivalent to the right hand side, in which Alice obtains random classical information, and transfers her quantum state to Bob.

Secondly, such structures can be considered outside of the category of Hilbert spaces and linear maps, in categories such as the category **Rel** of finite sets and relations, as well as the fusion categories considered in topological quantum information theory.

In  $\mathbf{Rep}(G)$ , a quantum teleportation procedure on a representation  $(H, \rho)$  is a unitary error basis for  $H$  such that the corresponding classical structure morphisms are intertwiners (2.5). It is sufficient for the unit and the comparison map to be intertwiners, since the other maps are Hermitian adjoints of these. For the comparison map, the intertwining condition (2.5) may be expressed in terms of the unitary error basis as follows:

$$m(\rho(g)U_i\rho(g)^\dagger \otimes \rho(g)U_j\rho(g)^\dagger) = \delta_{ij}U_i$$

For this equation to hold, the conjugation action of  $\rho$  must permute the orthonormal basis of unitary matrices.

In the next two chapters we will see how these permuted bases of unitary matrices may be used to perform reference frame-independent teleportation protocols. (In practise, they need only be permuted up to a phase.) In Chapter 3 we will see how they permit perfect teleportation for certain finite group representations, independent of the relative alignment of Alice and Bob's frames. In Chapter 4 we will see how these results may be applied to obtain tight and perfect teleportation schemes for representations of general compact Lie groups.

# Chapter 3

## Perfect tight reference frame-independent teleportation for finite transformation groups

### 3.1 Introduction

**Main results.** We consider the problem of quantum teleportation between two parties whose local reference frames are misaligned, where the set of possible local reference frame transformations forms a group  $G$  with a unitary representation  $\rho : G \rightarrow U(d)$  on the  $d$ -dimensional system to be teleported. Success of the protocol is judged by a third-party observer who holds full reference frame information, and who must agree that the original state has been teleported perfectly up to a global phase. We present a teleportation scheme for certain  $(G, \rho)$ , where  $G$  is finite, which is guaranteed to succeed regardless of the parties' reference frame configurations and which additionally satisfies the following properties.

- *Tightness.* The parties only require a  $d$ -dimensional maximally entangled resource state, and only 2 dits of classical information are communicated from Alice to Bob.
- *Dynamical robustness (DR).* The scheme is not affected by changes in reference frame alignment during transmission of the classical message from Alice to Bob.
- *No reference frame leakage (NL).* No information about either party's reference frame alignment is transmitted.<sup>1</sup>

---

<sup>1</sup>This has cryptographic significance in some scenarios [13, 49, 56].

Our scheme depends on the existence of a  $G$ -equivariant unitary error basis for the representation  $(G, \rho)$ ; these are orthogonal bases of unitary matrices permuted up to a phase by the conjugation action  $g \cdot M = \rho(g)M\rho(g)^\dagger$ . We exhaustively classify these structures for two-dimensional representations, where the composite homomorphism  $G \xrightarrow{\rho} \text{U}(2) \xrightarrow{q} \text{SO}(3)$ , where  $q$  is the quotient taking a unitary to its corresponding Bloch sphere rotation, allows us to identify faithful representations with subgroups of the 3-dimensional rotation group  $\text{SO}(3)$ . We show that an equivariant unitary error basis exists precisely when this subgroup is isomorphic to one of the following (the generators are listed on the right):

- 1 the trivial group
- $\mathbb{Z}_2$  generated by a  $\pi$  rotation around any axis
- $\mathbb{Z}_3$  generated by a  $2\pi/3$  rotation around any axis
- $\mathbb{Z}_4$  generated by a  $\pi/2$  rotation around any axis
- $D_2$  generated by a  $\pi$  rotation around any axis and a  $\pi$  rotation around a perpendicular axis
- $D_3$  generated by a  $\pi/3$  rotation around any axis and a  $\pi$  rotation around a perpendicular axis
- $D_4$  generated by a  $\pi/2$  rotation around any axis and a  $\pi$  rotation around a perpendicular axis
- $A_4$  rotations preserving a regular tetrahedron centred at the origin
- $S_4$  rotations preserving a regular octahedron or cube centred at the origin

We also provide a construction for any permutation representation with dimension less than 5, and show how to prove nonexistence in some cases.

Our results rely on a new idea regarding the classical communication part of the protocol: we suppose that the readings of the classical channel are *themselves* interpreted with respect to the local reference frame. Mathematically, this corresponds to a nontrivial action of the group of reference frame transformations on the classical channel. Such classical channels have been called ‘unspeakable’ [81]; we provide examples, and show how they can be used to communicate the measurement result. An unspeakable classical channel is a powerful resource which could be used to execute a prior alignment step before the protocol begins, but we emphasize that it is *not* being used in this way here; indeed, by the (NL) property, our protocol in fact transfers no information at all about either party’s reference frame alignment, and makes use of the unspeakable channel in a nontrivial way.

We can give the following simple intuition for how our scheme works. Local reference frame misalignment can cause errors in the performance of the protocol, since Bob will perform correction operations with respect to his own frame, which need not be aligned with the frame in which Alice performed her measurement. But, since in our setting the misalignment also affects the classical channel, it can also cause errors in transmission of the classical measurement result; Bob may, in interpreting the channel reading with respect to his own frame, receive a different measurement value to that transmitted by Alice. In essence, our scheme is constructed so that

these errors exactly cancel out. This intuition makes clear how the (DR) property is possible, since a change in local reference frame alignment also affects reception of the classical communication data, even if it takes place while that information is in transit.

**Related work.** Chiribella et al. [25] considered teleportation with a speakable classical channel only, and showed that when the group  $G$  of reference frame transformations is a continuous compact Lie group, perfect tight teleportation is impossible; this does not contradict our work, which uses an unspeakable classical channel and a finite group  $G$ . (Furthermore, as a consequence of our main results, we show that for finite  $G$ , perfect tight teleportation is indeed possible with a speakable classical channel in some restricted situations; see Corollary 1 and Remark 2.)

Several other solutions for reference frame-independent teleportation for a finite group of reference frame transformations exist in the literature. These all involve establishment of a shared reference frame in some way: by using pre-shared entanglement [25], sharing entanglement during the protocol [56], or transmitting more complex resources [14, Section V.A]. Unlike our scheme, these approaches work for arbitrary  $(G, \rho)$  where  $G$  is finite. However, none of them have all the properties of tightness, dynamical robustness and no reference frame leakage, as our scheme does.

Quantum communication under collective noise corresponding to a finite group was considered by Skotiniotis et al. [89]. From the perspective of our discussion above, their protocol satisfies the (DR) and (NL) properties. However, it requires a quantum channel; it is not a teleportation protocol. Their token could be equally be transmitted using an unspeakable classical channel of the type we construct in Section 3.4. However, we are not transmitting a token in their sense; in particular, the classical system we transmit need not carry a free and transitive action of  $G$ .

**Criticism.** We can criticise our perfect tight scheme as follows. Firstly, as with the alternative solutions discussed above, it works only for finite  $G$ . Secondly, it cannot be implemented for all scenarios  $(G, \rho)$  with finite  $G$ , and, although we provide a range of constructions of equivariant unitary error bases, and completely characterise valid  $(G, \rho)$  for qubit teleportation, we cannot give necessary and sufficient conditions for the applicability of our scheme in higher dimensions. Thirdly, to communicate the measurement result, we do not use an ordinary ‘speakable’ classical channel, but rather an ‘unspeakable’ classical channel; while we provide a number of examples of such channels, it is nevertheless clear that this novel aspect of our approach may raise technological barriers in an implementation. Finally, up to a global phase, the system to be teleported and Bob’s half of the entangled pair must carry the

same representation  $\rho$  of  $G$ , and Alice's half of the entangled pair must transform according to the dual representation  $\rho^*$ ; although this is physically reasonable in view of charge conservation, a situation may arise in which it is hard to construct a system carrying the representation  $\rho^*$ . Very often (for instance, for all representations with real characters),  $\rho \simeq \rho^*$  up to a phase, which solves this problem.

**Outlook.** These results may be applicable to cryptography and security of quantum protocols, as it has been noted that reference frame uncertainty is of cryptographic importance [13, 49, 56], and that a private shared reference frame may be considered as a secret key [13, 49]. In this context, it is useful to know what protocols, such as quantum teleportation, may be performed even in the absence of a shared reference frame, without any transmission of cryptographically sensitive reference frame information.

## 3.2 Example

We begin with an informal example of our perfect tight scheme, in the specific case where the quantum systems are two-dimensional and the reference frame corresponds to a choice of spatial direction. This will be followed by a more general and precise treatment in the next section.

Alice and Bob are quantum information theorists operating on spin- $\frac{1}{2}$  particles. They work in separate laboratories, which do not necessarily have the same orientation in space, and their task is to teleport a quantum state without revealing their spatial orientations, either to each other or to any eavesdropper. Their relative orientations are not completely unknown: the rotation  $g$  taking Alice's Cartesian frame onto Bob's is promised to lie within the subgroup  $\mathbb{Z}_3 \subset \text{SO}(3)$ , the group of rigid spatial rotations through multiples of  $2\pi/3$  radians around some axis. However,  $g \in \mathbb{Z}_3$  is unknown. Let  $a \in \mathbb{Z}_3$  be the transformation rotating the reference frame anticlockwise through  $2\pi/3$  radians. We suppose that the action of  $a$  affects the description of qubit states by the standard spin-1/2 representation:

$$\rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix} \quad (3.1)$$

That is, a state which appears as  $|v\rangle$  in frame configuration  $f$  will appear as  $\rho(a)|v\rangle$  in frame configuration  $a \cdot f$ .

Alice and Bob share the two-qubit entangled state

$$|\eta\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

Note that this state is invariant up to a phase under the action (3.1) of a change in reference frame orientation, so the entanglement will not be degraded by changes in reference frame alignment following its initialisation. All these aspects of the overall setup are common knowledge to both parties.

**Conventional scheme.** Let Alice and Bob perform a conventional teleportation protocol using the following unitary error basis:

$$\begin{aligned}
 U_0 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix} & U_2 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2}e^{2\pi i/3} \\ \sqrt{2} & e^{5\pi i/3} \end{pmatrix} \\
 U_1 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2}e^{4\pi i/3} \\ \sqrt{2}e^{4\pi i/3} & e^{5\pi i/3} \end{pmatrix} & U_3 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2} \\ \sqrt{2}e^{2\pi i/3} & e^{5\pi i/3} \end{pmatrix}
 \end{aligned} \tag{3.2}$$

If the reference frames have the same alignment, the procedure will be successful. However, if the reference frames are misaligned by some nonidentity element  $g \in \mathbb{Z}_3$ , then, from the perspective of Alice's frame, Bob will not perform the intended correction  $U_i$ , but rather  $\rho(g)^\dagger U_i \rho(g)$ . Assuming the uniform distribution over  $\mathbb{Z}_3$ , a simple calculation shows that an input pure state will emerge in a mixed state.

**New scheme.** We now describe our reference frame-independent scheme. Before performing the protocol, Alice and Bob share the coordinates of four unit vectors  $\{v_0, v_1, v_2, v_3\} \in \mathbb{R}^3$ , which form a regular tetrahedron centred on the origin such that, under the reference frame transformation  $a \in \mathbb{Z}_3 \subset \text{SO}(3)$ , the vectors are permuted as follows:

$$a \cdot v_0 = v_1 \quad a \cdot v_1 = v_2 \quad a \cdot v_2 = v_3 \quad a \cdot v_3 = v_0 \tag{3.3}$$

For example, let  $v_0 = \frac{1}{\sqrt{3}}(\hat{x} + \hat{y} + \hat{z})$ ,  $v_1 = \frac{1}{\sqrt{3}}(\hat{x} - \hat{y} - \hat{z})$ ,  $v_2 = \frac{1}{\sqrt{3}}(-\hat{x} + \hat{y} - \hat{z})$  and  $v_3 = \frac{1}{\sqrt{3}}(-\hat{x} - \hat{y} + \hat{z})$ , and suppose that the generating element  $a \in \mathbb{Z}_3$  acts as a right-handed rotation about the axis defined by  $v_0$ .

If Alice obtains measurement result  $i$ , she communicates this to Bob in the following way: she prepares a physical arrow, of the sort a medieval archer might use, arranges it to have the same orientation as the vector  $v_i$ , and then sends it directly to Bob by parallel transport along a known path. When the arrow is received, Bob observes its orientation in his own frame, correcting if necessary for the parallel transport map associated to the path, and matches this with one of the reference orientations  $v_j \in \{v_0, v_1, v_2, v_3\}$ ; he thus obtains the message  $j \in \{0, 1, 2, 3\}$ . He then performs the corresponding unitary correction. This procedure is illustrated in Figure 3.1.



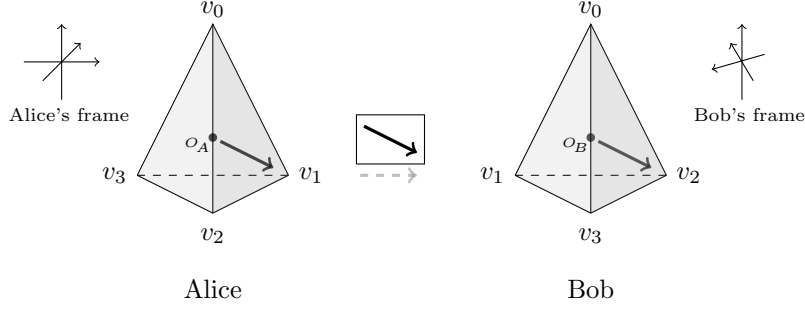


Figure 3.1: In our classical communication procedure, Alice and Bob label the vertices of regular tetrahedra centred on their origins  $O_A$  and  $O_B$ , using their own Cartesian frames. Bob's frame is related to Alice's by a  $2\pi/3$  anticlockwise rotation around the axis defined by  $v_0$ . Upon measuring  $|\phi_1\rangle$ , Alice prepares an arrow pointing to vertex  $v_1$  and sends this to Bob by parallel transport. In Bob's frame this arrow points to vertex  $v_2$ , and so he performs correction  $U_2$ .

Note that Alice transmits no information about her local reference frame by the above procedure, since her measurement result is uniformly random, and thus so is the direction indicated by the arrow. Also, we emphasize that exactly two bits of classical information have been transferred, since there were four possible values upon transmission and four possible values upon receipt.

Suppose that Alice and Bob's laboratories share the same reference frame; that is, their local frames are related by the element  $e \in \mathbb{Z}_3$  of the group of reference frame transformations. Then the arrow's orientation will be the same in Bob's frame as in Alice's frame, and the measurement outcome will be faithfully communicated. In this case the protocol will be successful, and it is identical to the conventional teleportation protocol, albeit with the two classical bits of information transmitted from Alice to Bob in an unusual way.

Now suppose that Alice and Bob's frames are misaligned by the action of the element  $a \in \mathbb{Z}_3$  of the reference frame transformation group. In this case, if Alice sends the result 0, 1, 2, or 3, Bob will receive the result 0, 2, 3 or 1 respectively, because of the transformation properties (3.3) of the arrows. Furthermore, when Bob applies the unitary  $U_i$  in his local frame, its action is seen in Alice's frame as  $\rho(a)^\dagger U_i \rho(a)$ . The following equations describe the consequences of such a conjugation, as can be directly checked using expressions (3.1) and (3.2):

$$\begin{aligned} \rho(a)^\dagger U_0 \rho(a) &= U_0 & \rho(a)^\dagger U_1 \rho(a) &= U_3 \\ \rho(a)^\dagger U_2 \rho(a) &= U_1 & \rho(a)^\dagger U_3 \rho(a) &= U_2 \end{aligned}$$

We now see the point of the entire construction: the unitary error basis (3.2) was carefully chosen so that these two apparent sources of error—in the transmission of the classical measurement result, and in Bob’s unitary correction—exactly cancel each other out. For example, if Alice obtains measurement outcome 1, Bob will receive this as measurement outcome 2, and will perform the correction  $U_2$  in his frame, which in Alice’s frame is equal to  $\rho(a)^\dagger U_2 \rho(a) = U_1$ , and so the intended correction will be carried out after all. As a result, the quantum teleportation will conclude successfully, even though Alice and Bob’s reference frames were misaligned. Similarly, it can be shown that the teleportation is also successful if the frame misalignment is given by the element  $a^2 \in \mathbb{Z}_3$ .

**Discussion.** We have exhibited a procedure for reference frame-independent quantum teleportation in the particular case of spatial reference frame misalignment with transformation group  $\mathbb{Z}_3 \subset \text{SO}(3)$ . This involved a careful choice of unitary error basis (3.2), with communication of the measurement result through a classical channel carrying a compatible nontrivial action (3.3) of the reference frame transformation group. Only 2 bits of classical information were transferred from Alice to Bob, as in a conventional teleportation procedure, and the Hilbert space of the entangled resource was of minimal dimension, so this procedure was *tight* in the sense of Werner [103]. The unspeakable information transmitted by Alice was uniformly random, since Alice’s measurement results were; in particular, Bob, or an eavesdropper on the classical channel, received no information about Alice’s reference frame alignment. Finally, the procedure would have succeeded even if Bob’s reference frame alignment changed during the protocol, while Alice’s measurement result was still in transit.

In this example we chose  $\mathbb{Z}_3 \subset \text{SO}(3)$  as the reference frame transformation group, but the same unitary error basis and classical channel allow reference frame-independent teleportation for the group  $A_4 \subset \text{SO}(3)$  of order 12, as we will see in Section 3.5.

### 3.3 Perfect tight reference frame-independent teleportation for finite transformation groups

A key concept in our new scheme is that of an *unspeakable classical channel*. For simplicity, we only consider perfect classical channels in this paper; whatever reading Alice sends through the channel will be received unaltered by Bob. However, his interpretation of this reading will be affected by his reference frame orientation.

**Definition 3.** For a finite group  $G$ , an *unspeakable classical channel* is a classical channel whose set of messages carries a nontrivial action of the group  $G$  of reference frame transformations.

Writing  $I$  for the set of messages carried by the channel, we can encode the data of an unspeakable channel as a group action  $\sigma : G \times I \rightarrow I$ . For each reference frame transformation  $g \in G$  taking Alice's frame onto Bob's frame, we obtain an invertible function  $\sigma(g, -) : I \rightarrow I$ , which describes how a message input by Alice using her local frame is interpreted by Bob with respect to his local frame. Since this function is invertible, there is no loss of information; however, if the receiver of the message does not know  $g \in G$ , they will be unable to infer which message was actually input. The arrows channel of Section 3.2 was an unspeakable classical channel; we will see more examples in Section 3.4.

We now define our new teleportation scheme. Here we write  $\rho^*$  for the dual representation of  $\rho$ .

**Procedure 2** (Reference frame-independent teleportation). Alice has an  $n$ -dimensional quantum system in a state  $|\psi\rangle$ . Separately, Alice and Bob hold a maximally entangled state  $(\mathbb{1} \otimes X) |\eta\rangle$  of a pair of  $n$ -dimensional quantum systems. They each possess local reference frames with transformation group  $G$ , acting unitarily by a representation  $\rho$  on the system to be teleported, by a representation  $\rho^* \otimes \theta_1$  on Alice's half of the entangled state, and by a representation  $\rho \otimes \theta_2$  on Bob's half of the entangled state, where  $\theta_1, \theta_2$  are any one-dimensional representations of  $G$ .

Alice performs a joint measurement on the system to be teleported and her half of the entangled state, described by an orthonormal basis  $\{|\phi_i\rangle\}$ ,  $|\phi_i\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ . She uses a perfect unspeakable classical channel to communicate the classical measurement result  $i$  to Bob, who receives the message  $\sigma(g, i)$ , where  $g$  is the transformation taking Alice's local frame configuration upon transmission onto Bob's local frame configuration upon receipt. Bob then immediately performs a unitary correction  $U_{\sigma(g,i)}$  on his half of the entangled state.

This was called *teleportation of unspeakable information* by Chiribella et al [25].

*Remark 1.* In Appendix 3.6.1 we show that the conditions on the possible representations carried by each system precisely imply that the maximally entangled state may always be taken to be  $G$ -invariant up to a phase, preventing degradation of entanglement by reference frame transformations.

The measurement and correction operations for Procedure 2, together with the action  $\sigma$  on the unspeakable classical channel, are *correct data* if, regardless of Alice and Bob's reference frame alignments, Bob's system ends in the state  $|\psi\rangle \in \mathbb{C}^n$ , according to a third observer with a fixed frame who can see both laboratories.

**Definition 4** ( $G$ -equivariant unitary error basis). For a finite group  $G$ , and a Hilbert space  $H$  carrying a unitary action  $\rho$  of  $G$ , an *equivariant unitary error basis* (equivariant UEB) for  $(G, \rho)$  is a unitary error basis  $\{U_i\}_{i \in I}$  for  $H$  whose elements are permuted up to a phase by the right conjugation action of  $G$ .<sup>2</sup>

That is, for all  $i \in I$  and  $g \in G$ , and some family of phases  $\xi(i, g) \in \mathbb{C}$ , we have that  $\xi(i, g)\rho(g)^\dagger U_i \rho(g) \in \{U_i\}_{i \in I}$ . Ignoring the phases, we can encode the effect of this conjugation as a right group action  $\tau : I \times G \rightarrow I$ .

**Definition 5** (Orbit type). For a  $G$ -equivariant unitary error basis  $\{U_i\}_{i \in I}$ , we define its *orbit type* as the multiset of sizes of each orbit in  $I$  under the action  $\tau : I \times G \rightarrow I$ .

We now show that the notion of  $G$ -equivariant unitary error basis gives a precise mathematical characterization of correct data for Procedure 2.

**Theorem 2.** *All correct data for Procedure 2 can be obtained from an equivariant unitary error basis  $\{U_i\}$  for  $(G, \rho)$ , with associated right action  $\tau$ . The measurement and correction operations are as in (2.2), and the unspeakable classical channel carries the action  $\tau^{-1} : G \times I \rightarrow I$ .*

*Proof.* We work in Alice's frame. Let Bob's misalignment with respect to this frame be  $g \in G$ . For sufficiency, suppose Alice measures  $x \in I$ ; Bob then reads  $\tau^{-1}(g, x)$  and performs the correction

$$U_{\tau^{-1}(g, x)} = U_x,$$

as required. For necessity, note that the procedure must work for trivial misalignment  $g = e$ ; therefore, by Werner's result [103, Theorem 1], Alice must perform measurements corresponding to a unitary error basis, and Bob must perform the unitary correction  $U_x$  in his own frame whenever he receives  $x \in I$ . The condition on the unspeakable channel is therefore clear.  $\square$

We say that an unspeakable classical channel is *compatible* with an equivariant UEB when it carries the inverse action as in Theorem 2. We see that our scheme can be implemented for some representation  $(G, \rho)$  if and only if there exists an equivariant UEB for  $(G, \rho)$ , and Alice and Bob have access to a compatible unspeakable classical channel.

Before considering equivariant unitary error bases and unspeakable channels in more detail, we note the following obvious corollary of Theorem 2.

---

<sup>2</sup>While the categorical analysis in Chapter 2 required them to be permuted precisely, this weaker definition turns out to be more physically relevant.

**Corollary 1.** *With only a speakable classical channel (that is, a channel carrying a trivial  $G$ -action), Procedure 2 succeeds for all frame alignments only if the action  $\tau : I \times G \rightarrow I$  is trivial; that is, the elements of the orbit type of the equivariant UEB are all 1.*

## 3.4 Requirement I: Unspeakable channels

In this section we address the physical requirement of our scheme, a compatible unspeakable classical channel for a given equivariant UEB.

### 3.4.1 Construction from quantum systems

We begin with a completely general method for constructing such a channel. When Alice performs the measurement on her two systems, they decohere in her measurement basis, and the joint system becomes a single classical object. Alice can transfer this directly to Bob, still in the eigenstate corresponding to her measurement result. Since the reference frame transformation is guaranteed to act as a permutation on measurement outcomes, Bob will also receive the system in an eigenstate, which he can identify by performing the same measurement as Alice. Due to reference frame uncertainty, the result he receives may of course be different to that noted by Alice. The result is an unspeakable classical channel. Since Bob both measures and performs the corresponding corrections in his own frame, the procedure will succeed for any reference frame misalignment.

### 3.4.2 Construction from shared classical system

In some physical situations, the method of Section 3.4.1 involving transfer of the decohered quantum systems may be impractical. We now provide an alternative construction. The problem is the following: given the right action  $\tau : I \times G \rightarrow I$  of a finite group on a finite index set, we must construct a compatible unspeakable classical channel  $\Sigma$  whose set of messages  $M_\Sigma$  can be identified with  $I$ , so that it carries the corresponding left action  $\tau^{-1} : G \times I \rightarrow I$ .

Here we show how this can be done when  $\tau^{-1}$  is a transitive action. This is sufficient since, if  $\tau^{-1}$  is not transitive,  $I$  will split into orbits under it, and the following procedure may be performed:

- After her measurement, Alice communicates the orbit  $O \subset I$  of the index she measured, through a speakable channel.

- She then communicates the precise measurement index  $i \in O$  using an unspeakable classical channel with the set of messages  $O$ , carrying the restricted action  $\tau^{-1}|_O : G \times O \rightarrow O$ , which is transitive.

This procedure still leaks no reference frame information, since the orbit is communicated as speakable information and the outcomes within each orbit are equiprobable. It is still tight, since the classical channel distinguishes only  $d^2$  possible messages, despite being split into speakable and unspeakable parts. It is still dynamically robust, since the orbit is unaffected by reference frame transformations.

We assume, therefore, that the action  $\tau^{-1}$  is transitive. We can then characterise it further using the following well-known fact from group theory [71, Theorem 3.4]. Recall that the set of right cosets  $\{Hg_i\}$  of a subgroup  $H < G$  carries a canonical left action  $g \cdot (Hg_i) = Hg_i g^{-1}$ ; we write this left  $G$ -set as  $G/H$ .

**Lemma 1.** *For any transitive left  $G$ -set  $X$ , there is a unique conjugacy class  $C$  of subgroups of  $G$  such that  $X \simeq G/H$  iff  $H \in C$ .*

It follows that  $\tau^{-1}$  is characterised up to isomorphism by its associated conjugacy class of subgroups. It also follows that any *transitive* unspeakable classical channel  $\Sigma$  (that is, any unspeakable classical channel whose set of messages  $M_\Sigma$  is a transitive  $G$ -set) is characterised by its associated conjugacy class of subgroups  $C_\Sigma$ . Our problem can therefore be rephrased as follows: we need to construct a transitive unspeakable channel for which  $C_\Sigma = C_{\tau^{-1}}$ , so that  $M_\Sigma \simeq G/H \simeq I$  as left  $G$ -sets.

A key construction is the following, which allows us to group together messages in  $M_\Sigma$  to create a new channel with a different associated conjugacy class.

**Construction 1** (Quotient channel). Let  $\Sigma$  be a transitive unspeakable classical channel with associated conjugacy class of subgroups  $C_\Sigma$ , and let  $H_\Sigma \in C_\Sigma$ . Fix an isomorphism  $\alpha : M_\Sigma \simeq G/H_\Sigma$ . Let  $K$  be another subgroup such that  $H_\Sigma < K < G$ .

We obtain a *quotient channel* whose associated conjugacy class of subgroups has representative  $K$ , and whose messages are right cosets  $Kg$ , transmitted as follows. In order to send a coset  $Kg$ , Alice picks uniformly at random any element  $x \in K/H_\Sigma \subset G/H_\Sigma$ , and sends the message  $\alpha^{-1}(xg) \in M_\Sigma$ . Depending on his reference frame orientation, Bob receives some  $y \in M_\Sigma$ , such that  $\alpha(y)$  lies in some right coset of  $K/H_\Sigma$ . He then uses the canonical isomorphism

$$\frac{G/H_\Sigma}{K/H_\Sigma} \simeq G/K$$

to obtain a right coset of  $K$  in  $G$ , which is the message he receives.

We obtain the following corollary. We define a partial order on conjugacy classes of subgroups, where  $C_1 < C_2$  iff  $H_1 < H_2$  for some  $H_1 \in C_1, H_2 \in C_2$ .

**Corollary 2.** *If we have access to a transitive unspeakable classical channel  $\Sigma$  with associated conjugacy class of subgroups  $C_\Sigma$ , and  $C_\Sigma < C_{\tau^{-1}}$ , then we may construct a compatible channel for  $\tau$ .*

*Proof.* Take  $H_{\tau^{-1}} \in C_{\tau^{-1}}, H_\Sigma \in C_\Sigma$  such that  $H_\Sigma < H_{\tau^{-1}}$ , and construct the quotient channel.  $\square$

The trivial subgroup is the only member of its conjugacy class, which we call the *trivial class*. The trivial class is beneath every other conjugacy class of subgroups in the partial ordering. From an transitive unspeakable channel  $\Sigma$  whose associated conjugacy class of subgroups is the trivial class, we may therefore construct a compatible channel for any transitive  $\tau^{-1}$ .

We now show how to use a shared classical system to construct an unspeakable classical channel with trivial associated conjugacy class.

**Definition 6.** A *reference frame system* is a classical system whose configuration is described according to a local reference frame, and whose set of configurations  $C$  carries a free and transitive action of  $G$ .

The details of how this system is shared between Alice and Bob are abstracted away in this approach. The nomenclature is derived from the fact that Alice and Bob each possess physical systems serving as their local reference frames, on which the reference frame transformation group  $G$  acts freely and transitively, by definition.

Alice and Bob will use their shared reference frame system to communicate messages. They associate each of the  $|G|$  configurations of the system to an element of  $G$  using a *labelling*, which is a choice of isomorphism  $l : C \rightarrow G$  depending on their local reference frame configurations. Once Alice fixes a labelling, she can communicate element  $g \in G$  to Bob by preparing the system in the configuration associated to  $g$  in her labelling. Bob will then interpret this configuration with respect to his own labelling.

A labelling  $l : C \rightarrow G$  is obtained by choosing a configuration  $x_e$  such that  $l(x_e) = e$ , where  $e$  is the identity element of  $G$ ; the labelling is then fully determined by the equation  $l(g \cdot x_e) = gl(x_e) = g$ . Alice and Bob both agree on a way to pick  $x_e$  based on their own local frame configuration; this is specified by a map  $\epsilon : \mathcal{F} \rightarrow C$ , where  $\mathcal{F}$  is the space of local frame configurations and  $\epsilon$  satisfies the naturality equation

$$\epsilon(g \cdot f) = g \cdot \epsilon(f). \tag{3.4}$$

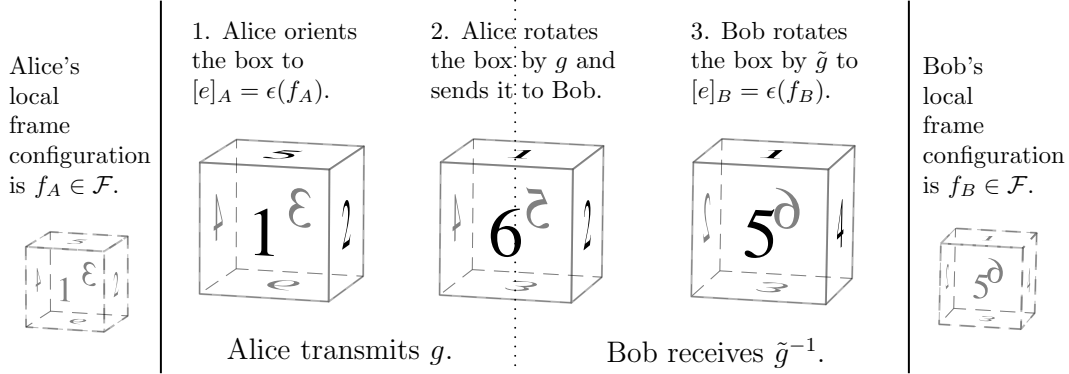


Figure 3.2: The reference frame channel of Example 1, where  $G$  is the group of rigid rotations of a cube. Here Alice transmits a  $\pi/2$ -rotation around the  $x$  axis, and Bob receives a  $\pi$ -rotation around the  $z$ -axis.

We write  $[l(x)]$  to refer to  $x \in C$  when a labelling is fixed. Alice and Bob generally have different labellings  $l_A, l_B$ , so we write  $[l_A(x)]_A, [l_B(x)]_B$  to refer to  $x$  using their respective labellings. We obtain the following proposition.

**Proposition 2.** *A shared reference frame system gives rise to a transitive unspeakable classical channel whose associated conjugacy class of subgroups is trivial.*

*Proof.* From the above discussion, the labelling of the channel is defined as  $[g]_A = g \cdot [e]_A$ ; we have  $[e]_A = \epsilon(f_A)$ , so  $[g]_A = g \cdot \epsilon(f_A) = g \cdot \epsilon(g_{AB}^{-1} \cdot f_B) = (gg_{AB}^{-1}) \cdot [e]_B = [gg_{AB}^{-1}]_B$ . The channel therefore carries the action  $\sigma(g, x) = xg^{-1}$ , and the result follows.  $\square$

By Corollary 2, it is therefore possible to construct a compatible unspeakable channel for any equivariant unitary error basis using a shared reference frame system. We conclude this section by presenting two examples of shared reference frame systems.

*Example 1 (Particle in a box).* Suppose that the quantum systems used in the teleportation protocol are particles in cubic boxes. In order to describe states of and operations on these systems, it is necessary to decide which sides of the box are ‘up’, ‘front’ and ‘right’. Alice and Bob shared such a labelling when they created their entangled pair of boxes; since that time, however, the orientation, and therefore the labelling, of Bob’s box may have altered. The choice of labelling can be seen as a reference frame, whose transformation group is the group of rigid rotations of a cube. One reference frame system here is a classical solid cube, with labelled sides, passed between parties; the map  $\epsilon : \mathcal{F} \rightarrow C$  is defined by labelling the cube identically to the box containing the particle. This is illustrated in Figure 3.2.



*Example 2* (Group of time translations). We suppose that the system to be teleported has a basis of energy eigenstates with different energy eigenvalues. Over the period  $T$  of time evolution, these states will acquire a relative phase. In order to define states and operations, Alice and Bob must choose a time  $t_0$  at which the chosen basis vectors will have trivial phase. If we are promised that Alice and Bob's clocks are related by a time translation in a finite subgroup of  $U(1)$ , then the choice of  $t_0$  corresponds to a reference frame with cyclic transformation group. One reference frame system here is the time of arrival, modulo  $T$ , of a signal transmitted from Alice to Bob; the map  $\epsilon : \mathcal{F} \rightarrow C$  is defined by the signal arriving at one's own time  $t_0$ .

## 3.5 Requirement II: Equivariant unitary error bases

We now turn to the classification and construction of equivariant unitary error bases, the mathematical basis for our scheme.

### 3.5.1 Classification for qubits

We first fully classify equivariant UEBs for two-dimensional representations  $(G, \rho)$ . Let  $q : SU(2) \rightarrow SO(3)$  be the quotient homomorphism taking a qubit unitary to its corresponding Bloch sphere rotation. Our results are outlined in the following theorem.

**Theorem 3** (Classification of equivariant UEBs for qubits). *The existence of unitary error bases of a given orbit type for a unitary representation  $\rho : G \rightarrow U(2)$  depends only on the isomorphism class of the image subgroup  $q(\rho(G)) \subset SO(3)$ , according to the classification given in Table 3.1.*

Whilst in Table 3.1 we have only given the orbit type of the UEBs, in the proof we give now we also describe the associated action  $\tau : I \times G \rightarrow G$ . Before beginning the proof, we make a quick remark.

*Remark 2.* By Corollary 1, tight qubit teleportation without an unspeakable classical channel is possible only when the image of the composite homomorphism  $G \xrightarrow{\rho} U(2) \xrightarrow{q} SO(3)$  is isomorphic to  $1$ ,  $\mathbb{Z}_2$  or  $D_2$ .

We begin by fixing some notation for rotations. Euler showed [42] that every rotation in  $SO(3)$  can be represented uniquely as a rotation through an angle  $0 \leq \theta \leq \pi$  around a given normalised vector  $\hat{n} \in \mathbb{R}^3$ . We write a rotation through an

<b>Isom. class of <math>q(\rho(G))</math></b>	<b>Orbit types and solutions, up to phase</b>	<b>Further details</b>
Trivial	(1,1,1,1) - any UEB	N/A
$\mathbb{Z}_2$	(1,1,1,1) - one 2-parameter family (2,1,1) - one 2-parameter family (2,2) - one 2-parameter family	Proposition 3
$\mathbb{Z}_3$	(3,1) - one 2-parameter family	Proposition 4
$\mathbb{Z}_4$	(2,1,1) - one 2-parameter family	Proposition 5
$\mathbb{Z}_n, n \geq 5$	No solutions	N/A
$D_2$	(1,1,1,1) - one isolated solution (2,1,1) - six isolated solutions (2,2) - three isolated solutions (4) - two isolated solutions	Proposition 7
$D_3$	(3,1) - six isolated solutions	Proposition 8
$D_4$	(2,1,1) - two isolated solutions (2,2) - two isolated solutions	Proposition 9
$D_n, n \geq 5$	No solutions	N/A
Tetrahedral ( $A_4$ )	(4) - two isolated solutions	Proposition 11
Octahedral ( $S_4$ )	(1,3) - one isolated solution	Proposition 12
Icosahedral ( $A_5$ )	No solutions	N/A

Table 3.1: UEB families for qubit representations.

angle  $\theta$  around an axis  $\hat{n}$  as  $r(\theta, \hat{n})$ .<sup>3</sup> Given two rotations  $r(\theta_1, \hat{n}_1)$  and  $r(\theta_2, \hat{n}_2)$ , we write the angle and axis of the composite as  $\theta_{12}$  and  $\hat{n}_{12}$ . For concision, we will occasionally write rotations simply as  $r \in \text{SO}(3)$ , omitting to mention the axis and angle of rotation.

It is well known that unitary operations on a qubit correspond to rotations of the Bloch sphere together with a global phase [79, Exercise 4.8]. It is easy to check that two unitaries  $U_1, U_2$  are orthogonal iff their corresponding Bloch sphere rotations  $q(U_1), q(U_2)$  obey the following condition.

**Definition 7.** Two rotations  $r_1, r_2 \in \text{SO}(3)$  are *Hilbert-Schmidt orthogonal* (HS-orthogonal) if the composite  $r_1^{-1}r_2$  is a rotation through the angle  $\pi$ .

The image of a UEB under the quotient  $q$  will be a set of HS-orthogonal rotations preserved under conjugation by the HS-orthogonal rotations  $q(\rho(g))$  for  $g \in G$ ; this inspires the following definition.

**Definition 8.** A *HS-orthogonal error basis* (OEB) is a family  $\mathcal{O} \subset \text{SO}(n)$  of  $n^2$  HS-orthogonal rotations. For a finite group  $G$  and a homomorphism  $\rho : G \rightarrow \text{SO}(n)$ , an *equivariant HS-orthogonal error basis* for  $(G, \rho)$  is an OEB  $\mathcal{O} \subset \text{SO}(n)$  preserved under conjugation by  $\rho(g)$  for all  $g \in G$ .

In the other direction, given an equivariant OEB for  $(G, q \circ \rho)$ , one may obtain all corresponding equivariant UEBs for  $(G, \rho)$  by picking phases for each rotation. A classification of equivariant UEBs for subgroups  $G \subset \text{U}(2)$  is therefore equivalent to a classification of equivariant OEBs for subgroups  $q(G) \subset \text{SO}(3)$ . Note also that the action of  $\rho(g)$  on the index set of a UEB is identical to the action of  $q(\rho(g))$  on the index set of the corresponding OEB.

**Theorem 4** ([5, Theorem 19.2]). *The finite subgroups of  $\text{SO}(3)$  are as follows:*

- *cyclic groups  $\mathbb{Z}_n$  for  $n \geq 1$ , generated by a rotation through  $2\pi/n$  around a given axis;*
- *dihedral groups  $D_n$  for  $n \geq 1$ , generated by a rotation through  $2\pi/n$  around a given axis and a  $\pi$ -rotation around a perpendicular axis;*
- *the group of orientation-preserving symmetries of a regular tetrahedron, isomorphic to  $A_4$ ;*

---

<sup>3</sup>Note that this notation is slightly redundant because rotations through an angle  $\pi$  around antipodal  $\hat{n}$  are identical, as are all rotations through an angle 0.

- the group of orientation-preserving symmetries of a regular octahedron (or a cube), isomorphic to  $S_4$ ;
- the group of orientation-preserving symmetries of a regular icosahedron, isomorphic to  $A_5$ .

In order to find sets of points preserved under the conjugation action of these subgroups, we recall a useful way to think about conjugation in  $\text{SO}(3)$ . The group  $\text{SO}(3)$  may be viewed as a closed ball  $B(3) \subset \mathbb{R}^3$  of radius  $\pi$ , which we call the  $\text{SO}(3)$ -ball, under the identification

$$r(\theta, \hat{n}) \mapsto \theta \hat{n}. \quad (3.5)$$

Antipodal points on the boundary are identified, since rotation through an angle  $\pi$  around  $\hat{n}$  is the same as rotation through an angle  $\pi$  around  $-\hat{n}$ . Given two rotations  $r_1 = r(\theta, \hat{n})$  and  $r_2$ , we have the identity

$$r_2 r_1 r_2^{-1} = r_2 r(\theta, \hat{n}) r_2^{-1} = r(\theta, r_2(\hat{n})).$$

It follows that, under the identification (3.5), conjugation by a rotation in  $\text{SO}(3)$  corresponds to rotation of the  $\text{SO}(3)$ -ball. Equivariant OEBs for a subgroup are therefore sets of orthogonal points in the  $\text{SO}(3)$ -ball permuted by rotations in that subgroup.

For concision, in what follows we will occasionally conflate points in  $B(3)$  and rotations in  $\text{SO}(3)$ . For instance, we say ‘a point on the  $z$ -axis’ to signify the element of  $\text{SO}(3)$  corresponding to a point on the  $z$ -axis, that is, a rotation around the  $z$ -axis through some angle. We will also write  $\sin(x)$ ,  $\cos(x)$  and  $\tan(x)$  as  $\sin(x)$ ,  $\cos(x)$  and  $\tan(x)$  respectively.

We now recall some useful facts about orthogonality in  $\text{SO}(3)$ .

**Lemma 2.** *Each rotation in  $\text{SO}(3)$  around  $\hat{n}$  is orthogonal to exactly one other rotation around  $\pm\hat{n}$ .*

*Proof.* The composite  $r(\theta_1, \hat{n})^{-1} r(\theta_2, \hat{n})$  is the rotation  $r(\theta_2 - \theta_1, \hat{n})$ . For a given  $\theta_1 \in [0, \pi]$ , there is only one  $\theta_2 \in (-\pi, \pi]$  such that  $\theta_2 - \theta_1$  is an odd multiple of  $\pi$ .  $\square$

**Lemma 3.** *The rotation  $r(\theta_2, \hat{n}_2)$  is orthogonal to the rotation  $r(\pi, \hat{n}_1)$  iff either  $\hat{n}_2$  is orthogonal to  $\hat{n}_1$  or  $\theta_2 = 0$ .*

*Proof.* We have the following standard formula for the rotation angle  $\theta_{12}$  of the composite  $r_2^{-1} \circ r_1$ , where  $r_i$  is a rotation around the axis  $\hat{n}_i$  through an angle  $\theta_i \in$

$[0, \pi]$  [79, Exercise 4.15]:

$$\begin{aligned} \cos(\theta_{12}/2) &= \cos(\theta_1/2) \cos(\theta_2/2) \\ &+ \sin(\theta_1/2) \sin(\theta_2/2) \hat{n}_1 \cdot \hat{n}_2 \end{aligned} \tag{3.6}$$

Orthogonality of  $r_2$  and  $r_1$  is precisely the condition that the LHS is zero. Since the first term on the RHS equals zero when  $\theta_1 = \pi$ , the second term must also. This implies that either  $\hat{n}_1 \cdot \hat{n}_2 = 0$ , in which case the axes of rotation are orthogonal, or  $\sin(\theta_2/2) = 0$ , in which case the other rotation is simply the identity.  $\square$

**Lemma 4.** *Two rotations can be orthogonal only if the angle between the axes of rotation is obtuse. If the angle between the axes is  $\pi/2$  then for orthogonality one rotation must be through the angle  $\pi$ .*

*Proof.* Considering (3.6), we note that both  $\cos(\theta_1/2) \cos(\theta_2/2)$  and  $\sin(\theta_1/2) \sin(\theta_2/2)$  will be positive for  $\theta_1, \theta_2 \in [0, \pi)$ . The sum can only be zero, then, if  $\hat{n}_1 \cdot \hat{n}_2 \leq 0$ , i.e. if the angle between the axes is obtuse. If the angle is  $\pi/2$  then we need  $\cos(\theta_1/2) \cos(\theta_2/2) = 0$ , which implies that one of the rotations is through an angle  $\pi$ .  $\square$

We now begin our classification.

### Subgroups of $\text{SO}(3)$

Any set of orthogonal points will be equivariant for  $\mathbb{Z}_1$ . We proceed directly to the nontrivial cases. Let the  $z$ -axis be the axis of rotation of the generator of  $\mathbb{Z}_n$  which rotates the  $\text{SO}(3)$ -ball through an angle  $2\pi/n$ . Recalling that antipodal points on the ball's surface are identified, we immediately obtain the following characterisation of the orbits under this action.

**Lemma 5.** *The orbit sizes under the conjugation action of  $\mathbb{Z}_n$  on  $\text{SO}(3)$  are:*

- 1, for a point on the axis of rotation;
- $n$ , for a point in the interior of the ball and not on the axis of rotation, on the boundary of the ball and not on the  $xy$ -plane or the axis of rotation, or on the intersection of the boundary of the ball and the  $xy$ -plane when  $n$  is odd;
- $n/2$ , for a point on the intersection of the boundary of the ball and the  $xy$ -plane when  $n$  is even.

**Proposition 3.** *The  $\mathbb{Z}_2$ -equivariant orthogonal error bases are as follows:*

- *for orbit type  $(1,1,1,1)$ , a 2-parameter family of solutions, where two points are rotations around the  $z$ -axis and the other two are  $\pi$ -rotations around orthogonal axes in the  $xy$ -plane;*
- *for orbit type  $(2,1,1)$ , a 2-parameter family of solutions, where one point is a rotation around the  $z$ -axis, another point is a  $\pi$ -rotation around an  $x$ -axis perpendicular to the  $z$ -axis, and the other two points are rotations around axes in the  $yz$ -plane (see Figure 3.3), where the  $y$ -axis is perpendicular to both the  $x$ - and  $z$ -axes;*
- *for orbit type  $(2,2)$ , a 2-parameter family of solutions, where, for an axis  $x$  orthogonal to  $z$  and an axis  $y$  orthogonal to both, two points lie in the  $xz$ -plane and below the  $xy$ -plane, and another two points lie in the  $yz$ -plane and above the  $xy$ -plane (see Figure 3.4).*

*Proof.* *Orbit type  $(1,1,1,1)$ .* By Lemma 2 there can be at most two rotations on the  $z$ -axis. The other two, in order to have orbit size 1, must both be  $\pi$  rotations around different axes in the  $xy$ -plane, which must be orthogonal to each other by Lemma 3. This set of solutions therefore has two independent parameters, namely the angle of one rotation around the  $z$ -axis and the orientation of the perpendicular axes in the  $xy$ -plane.

*Orbit type  $(2,1,1)$ .* Firstly, suppose both the 1-orbits lie off the  $z$ -axis. Then they must be orthogonal  $\pi$ -rotations in the  $xy$ -plane. But then the other two rotations would have to be orthogonal and we would end up in the case  $(1, 1, 1, 1)$ .

Let us now suppose that exactly one of the 1-orbits lies on the  $z$ -axis. The other must be an orthogonal  $\pi$ -rotation; let this be around the  $x$ -axis. Then the 2-orbit must lie in the  $yz$ -plane by Lemma 3. We are therefore looking for three orthogonal points in the  $yz$ -plane, one on the  $z$ -axis and the other two symmetric under a reflection in the  $z$ -axis. Let  $r$  be the rotation angle of the elements in the 2-orbit and  $\theta$  be the angle between them. Here we take  $0 < \theta < 2\pi$ , where  $\theta = 0$  would correspond to both points being on the positive  $z$ -axis. By (3.6) we have the following equation for orthogonality of the elements of the 2-orbit:

$$r = 2 \cos^{-1} \left( \sqrt{\frac{\cos(\theta)}{\cos(\theta) - 1}} \right) \quad (3.7)$$

This has a unique solution  $r \in [\pi/2, \pi]$  for  $\theta \in [\pi/2, 3\pi/2]$ , and none otherwise. Using (3.6), it can be shown similarly that, for given  $\theta$ , there is a unique value of the  $z$ -coordinate of the 1-orbit such that all three points are orthogonal (see Figure 3.3). We

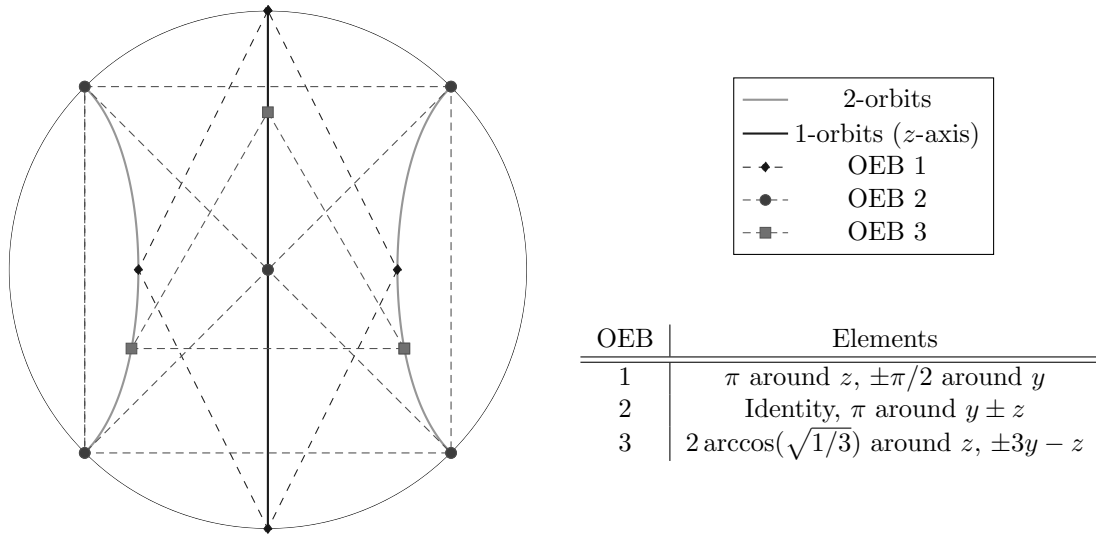


Figure 3.3:  $\mathbb{Z}_2$ -equivariant OEBs with orbit type  $(2,1,1)$ . The diagram shows the intersection of the  $yz$ -plane with the  $SO(3)$ -ball. One 1-orbit of the OEB is a  $\pi$ -rotation around the  $x$ -axis, and the remaining 2-orbit and 1-orbit are rotations around axes in the  $yz$ -plane shown in the diagram. Each 2-orbit is a pair of points with identical  $z$ -value on the two curved gray lines. The corresponding 1-orbit is a point on the  $z$ -axis. Three possible choices of points are given in the table and marked in the figure, joined by dashed lines.

therefore have a 2-parameter family of solutions, where one parameter corresponds to a choice of  $z$ -coordinate  $z_1$  of the 1-orbit on the  $z$ -axis, and the other parameter comes from a choice of orientation of  $x$ -axis.

Suppose now that both 1-orbits lie on the  $z$ -axis; we will demonstrate that we cannot then obtain solutions of this orbit type. Firstly, if the elements of the 2-orbit are  $\pi$ -rotations not in the  $xy$ -plane, then they will not be orthogonal to the 1-orbits on the  $z$ -axis. On the other hand, if the elements of the 2-orbit are rotations through an angle less than  $\pi$  and not in the  $xy$ -plane, then, given that by Lemma 2 the  $z$ -rotations will be on opposite sides of the origin, both elements of the 2-orbit will make an acute angle with one of the  $z$ -rotations, violating Lemma 4. The 2-orbit must therefore lie in the  $xy$ -plane. The rotations of the 2-orbit must be through an angle less than  $\pi$ , or they would form two 1-orbits. But, by Lemma 4, in order to be orthogonal both  $z$ -rotations must then be through an angle  $\pi$ , which would identify them.

*Orbit type (2,2).* Each 2-orbit will lie in a plane through the  $z$ -axis. Again, let  $r$  be

the rotation angle of the elements in the 2-orbit and  $\theta$  be the angle between them; the relationship between  $r$  and  $\theta$  was already given in (3.7).

We must find two 2-orbits where all four elements are pairwise orthogonal. Without loss of generality let the first orbit  $O_1$  lie in the  $xz$ -plane, and let  $\theta_1 \in [\pi/2, \pi]$ . Certainly, the second orbit  $O_2$  must have  $\theta_2 \in [\pi, 3\pi/2]$ , as otherwise the central angle between some pair of elements will be acute. We now show that the orbit  $O_2$  must also lie in the  $yz$ -plane. In other words, the two 2-orbits must lie in orthogonal planes containing the  $z$ -axis, and be on opposite sides of the  $xy$ -plane.

Let  $r_1, r_2 \in [0, \pi]$  be the rotation angles of  $O_1$  and  $O_2$  respectively. Take one element from each orbit, and consider their composition (3.6). With  $r_1, r_2$  fixed, the only thing that can vary on the right hand side of this equation is the angle between the axes of rotation of these elements. This angle will lie between 0 and  $\pi$ , and  $\cos(x)$  is single-valued in that range; therefore, for both elements of the second orbit to be orthogonal to the given element of the first, their axes of rotation must both have an equal central angle with that element. This means that the  $xz$ -plane containing  $O_1$  must be orthogonal to the plane through the  $z$ -axis containing  $O_2$ , which must therefore be the  $yz$ -plane.

With the planes fixed, we now find which angles  $\theta_1 \in [\pi/2, \pi]$  and  $\theta_2 \in [\pi, 3\pi/2]$  defining the two orbits are compatible. By the above discussion, for orthogonality of all elements it is sufficient for a single pair of elements from different orbits to be orthogonal. Unit vectors  $\hat{n}_1, \hat{n}_2$  defining the axes of rotation of a pair of elements in  $O_1, O_2$  respectively may be expressed in Cartesian coordinates as  $\hat{n}_1 = (\sin(\theta_1/2), 0, \cos(\theta_1/2))$  and  $\hat{n}_2 = (0, \sin(\theta_2/2), \cos(\theta_2/2))$ . The orthogonality condition (3.6) then becomes

$$-\cos(r_1/2)\cos(r_2/2) = \sin(r_1/2)\sin(r_2/2)\cos(\theta_1/2)\cos(\theta_2/2). \quad (3.8)$$

Replacing  $\theta_1, \theta_2$  with  $r_1, r_2$  using (3.7), squaring both sides and performing some trigonometric manipulations, we derive

$$r_1 = 2 \cos^{-1} \left( \sqrt{\frac{1}{2} - \cos^2\left(\frac{r_2}{2}\right)} \right)$$

This uniquely determines  $r_1 \in [\pi/2, \pi]$  for any  $r_2 \in [\pi/2, \pi]$ . The solutions of orbit type (2,2) are therefore parametrised by two angle variables; the first is the orientation of the  $x$ -axis and the second is the angle  $r_2$  of one of the rotations in the 2-orbit  $O_2$  lying below the  $xy$ -plane. Two of these solutions are shown in Figure 3.4.  $\square$

**Proposition 4.** *The  $\mathbb{Z}_3$ -equivariant orthogonal error bases are as follows:*



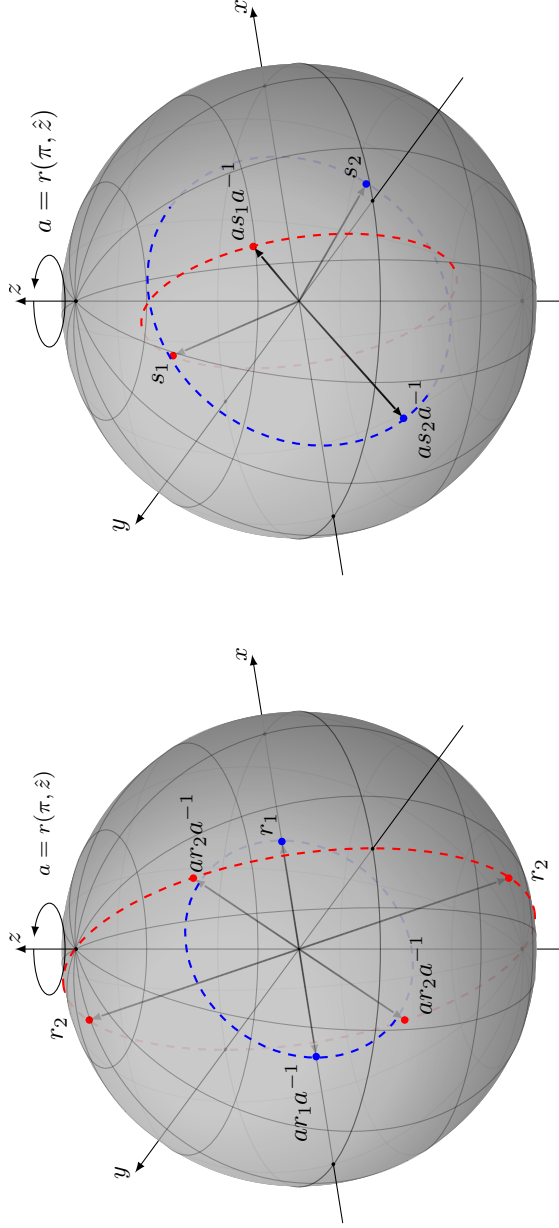


Figure 3.4: Two equivariant OEBs for  $\mathbb{Z}_2$  with orbit type (2,2), pictured in the  $\text{SO}(3)$ -ball. Under the  $\mathbb{Z}_2$  action, the equivariant OEB on the left is generated by  $r_1 = r(\pi/2, \hat{x})$  and  $r_2 = r(\pi, \frac{1}{\sqrt{2}}(\hat{y} + \hat{z}))$  (note the identification of antipodal points), while the equivariant OEB on the right is generated by  $s_1 = r(2\pi/3, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{y} + \hat{z}))$  and  $s_2 = r(2\pi/3, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{x} - \hat{z}))$ .

- for orbit type  $(1,1,1,1)$ , no solutions;
- for orbit type  $(3,1)$ , a 2-parameter family of solutions, forming the vertices of a tetrahedron with one vertex on the  $z$ -axis and the other three forming an equilateral triangle in a plane perpendicular to the  $z$ -axis (see Figure 3.5).

*Proof.* Orbit type  $(1,1,1,1)$ . All the points would need to be on the  $z$ -axis, which is impossible by Lemma 2.

Orbit type  $(3,1)$ . By the classification of orbits (Lemma 5), these OEBs consist of a 1-orbit on the  $z$ -axis and a 3-orbit forming the vertices of an equilateral triangle in a plane perpendicular to the  $z$ -axis. Let one of the elements in the 3-orbit lie in the  $xz$ -plane, so  $(r, \psi, 0)$  are its spherical coordinates. From (3.6) we obtain the following condition for orthogonality of the elements of the 3-orbit:

$$r = 2 \sin^{-1} \left( \frac{\sqrt{2}}{\sqrt{3} \sin(\psi)} \right)$$

Where soluble, this equation completely determines  $r$  for given  $\psi$ . It admits solutions for  $\psi \in [\sin^{-1}(\sqrt{\frac{2}{3}}), \pi - \sin^{-1}(\sqrt{\frac{2}{3}})]$ . By (3.6) we also obtain an equation in  $\psi$  for the height  $z$  of the point on the  $z$ -axis, which is single-valued in the range  $\psi \in [\sin^{-1}(\sqrt{\frac{2}{3}}), \pi - \sin^{-1}(\sqrt{\frac{2}{3}})]$ :

$$z = 2 \tan^{-1} \left( \sqrt{\frac{3}{2}} \cos(r(\psi)/2) \tan(\psi) \right)$$

Under this equation  $z$  can take all values in  $[-\pi, \pi]$ ; the 3-orbit lies on the other side of the  $xy$ -plane. These OEBs therefore form a 2-parameter family, where one parameter is the angle  $\psi$ , and the other is the choice of  $x$ -axis. Two solutions are shown in Figure 3.5.  $\square$

**Proposition 5.** *The  $\mathbb{Z}_4$ -equivariant orthogonal error bases are as follows:*

- for orbit type  $(1,1,1,1)$ , no solutions;
- for orbit type  $(2,1,1)$ , a 2-parameter family of solutions identical to the  $(1,1,1,1)$  solutions for  $\mathbb{Z}_2$  (Proposition 3);
- for orbit type  $(2,2)$ , no solutions;
- for orbit type  $(4)$ , no solutions.

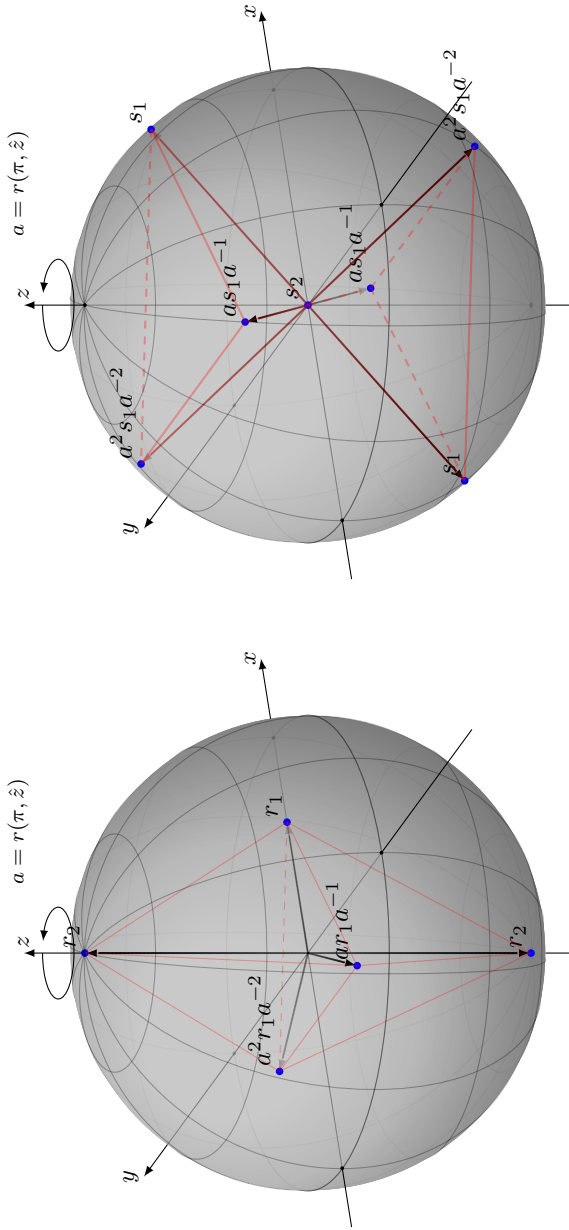


Figure 3.5: Two equivariant OEBs for  $\mathbb{Z}_3$  with orbit type (3,1). Under the  $\mathbb{Z}_3$  action, the equivariant OEB on the left is generated by  $r_1 = r(2 \sin^{-1}(\sqrt{\frac{2}{3}}), \hat{x})$  and  $r_2 = r(\pi, \hat{z})$ , and the equivariant OEB on the right is generated by  $s_1 = r(\pi, \frac{1}{\sqrt{3}}(\sqrt{2}\hat{x} + \hat{z}))$  and  $s_2 = r(0, \hat{z})$ . Note the identification of antipodal points in both cases; this is why the points are vertices of two tetrahedra rather than just one.

*Proof.* *Orbit type (1,1,1,1).* All the points would need to be on the  $z$ -axis, which is impossible by Lemma 2.

*Orbit type (2,1,1).* The 2-orbit must consist of orthogonal  $\pi$ -rotations around axes in the  $xy$ -plane. One parameter therefore corresponds to the rotation angle of one of the rotations on the  $z$ -axis, and the other to the orientation of the orthogonal axes in the the  $xy$ -plane.

*Orbit type (2,2).* These must be four different  $\pi$ -rotations around axes in the  $xy$ -plane. But then they cannot be orthogonal.

*Orbit type (4).* The angle between rotation vectors in a 4-orbit will be acute if they are not in the  $xy$ -plane, so they cannot be orthogonal. If they are in the  $xy$ -plane then as the angle between adjacent vectors is  $\pi/2$ , at least one pair of opposite vectors must be  $\pi$ -rotations by Lemma 4; but then these will be identified and this will not be a 4-orbit.  $\square$

**Proposition 6.** *There are no  $\mathbb{Z}_n$ -equivariant orthogonal error bases for  $n \geq 5$ .*

*Proof.* We handle the odd and even cases separately.

*$n \geq 5$  and  $n$  odd:* The only orbit sizes are 1 and  $n$ . Since we only have four elements in the UEB, all four points must be of orbit size 1; they must therefore all be on the  $\hat{z}$ -axis. But this is impossible by Lemma 2.

*$n \geq 5$  and  $n$  even:* For  $n = 6$ , the orbit sizes are 1, 3 and 6. Since for the reason given above we cannot have four 1-orbits, we must have one 1-orbit and one 3-orbit. However, the axes of the  $\pi$ -rotations will not be orthogonal and so the rotations are not orthogonal by Lemma 3. For  $n = 8$ , the orbit sizes are 1, 4 and 8, so we are forced to have a 4-orbit by Lemma 2. But these  $\pi$  rotations will again not be around orthogonal vectors and are therefore not orthogonal by Lemma 3. For  $n > 8$ , the orbit sizes for elements off the  $\hat{z}$ -axis are all greater than 4.  $\square$

### Dihedral subgroups of $\text{SO}(3)$ .

Let the  $z$ -axis be the axis of cyclic rotation, and let the  $f$ -axis be the perpendicular axis of  $\pi$ -rotation (the ‘flip axis’).

**Proposition 7.** *The  $D_2$ -equivariant orthogonal error bases are as follows:*

- *for orbit type (1,1,1,1), one solution;*
- *for orbit type (2,1,1), six solutions;*

- for orbit type  $(2,2)$ , three solutions;
- for orbit type  $(4)$ , two solutions.

*Proof.* Any solution for  $D_2$  must also be a solution for its  $\mathbb{Z}_2$  subgroup, and we proceed by case analysis of  $\mathbb{Z}_2$ -orbit types, making use of Proposition 3.

$\mathbb{Z}_2$ -orbit type  $(1,1,1,1)$ . Recall that  $\mathbb{Z}_2$ -equivariant OEBs of this type are made up of two  $\pi$ -rotations around orthogonal axes in the  $xy$ -plane and two rotations around the  $z$ -axis. If we fix the flip axis  $f$ , in order that the rotations in the  $xy$ -plane are preserved there are two choices for the axes; either  $f$  and  $g$ , or  $f + g$  and  $f - g$ . In order that the  $z$ -rotations are preserved, there are two choices for the rotation angles; either 0 and  $\pi$ , or  $-\pi/2$  and  $\pi/2$ . The orbit types are  $(1,1,1,1)$ ,  $(2,1,1)$ ,  $(2,1,1)$  and  $(2,2)$ .

$\mathbb{Z}_2$ -orbit type  $(2,1,1)$ . Recall that  $\mathbb{Z}_2$ -equivariant OEBs of this type are made up of a  $\pi$ -rotation around some  $x$ -axis, a rotation around the  $z$ -axis, and two other rotations around axes in the  $yz$ -plane (see Figure 3.3). Fix the flip axis  $f$ . The  $z$ -rotation will be preserved under the flip only if it is through an angle  $\pi$  or 0. This fixes the rotation angle  $r$  of the elements in the 2-orbit as  $\pi/2$  or  $\pi$  respectively. For the  $x$ -rotation to be preserved under the flip, we need either that  $x = f$  or  $y = f$ . In both of these cases, the solutions with  $r = \pi/2$  and  $r = \pi$  are preserved. We therefore obtain four equivariant OEBs with orbit type  $(2,1,1)$ .

$\mathbb{Z}_2$ -orbit type  $(2,2)$ . Consider the 2-parameter family of solutions of orbit type  $(2,2)$ . The 2-orbits  $O_1, O_2$  lie on opposite sides of the  $xy$ -plane, in the  $xz$ - and  $yz$ -planes respectively.  $D_2$  is abelian, so the  $\mathbb{Z}_2$ -orbit pairing will be preserved after the flip. There are therefore two possibilities if the elements are to be preserved under the flip; the flip can either swap the  $xz$ - and  $yz$ -planes or preserve them.

If the planes are preserved then the flip axis must be the  $x$ - or  $y$ -axis, and the 2-orbits must be symmetric under reflection in the  $xy$ -plane. Since one orbit is fixed by the other, this gives two solutions of orbit type  $(2,2)$ , corresponding to a choice of  $r_1 = \pi/2$  or  $r_1 = \pi$  in  $O_1$ , where  $r_i$  is the rotation angle of the elements of  $O_i$  (see Figure 3.3).

If the planes are permuted then the flip axis must be  $v_1 \pm v_2$ , and  $r_1 = r_2$ . Setting  $r_1 = r_2$  in (3.8) and substituting in (3.7), we obtain  $\cos(\theta) = -\frac{1}{3}$ , where  $\theta \in [\pi/2, \pi]$  is the central angle between the elements of each orbit. This has a unique solution in the relevant domain, of orbit type  $(4)$ . There are two of these for a given choice of  $f$ -axis, since we can choose which orbit lies above the  $xy$ -plane.  $\square$

**Proposition 8.** *There are six isolated  $D_3$ -equivariant quotient orthogonal error bases all of orbit type  $(3,1)$ .*

*Proof.* Any solution for  $D_3$  must also be a solution for its  $\mathbb{Z}_3$  subgroup. In Proposition 4 we saw that solutions were the vertices of a 2-parameter family of tetrahedra with one vertex on the  $z$ -axis and the others forming the vertices of an equilateral triangle on the other side of the  $xy$ -plane. The vertex on the  $z$ -axis point must be preserved under reflection in the  $xy$ -plane, so it must be through an angle 0 or  $\pi$ ; the two possibilities were shown in Figure 3.5. For  $z = 0$ , the elements of the 3-orbit will be preserved if the  $fz$  plane is orthogonal to the triangle's medians, giving three solutions. For  $z = \pi$ , the  $f$ -axis must go through any of the three vertices of the triangle, giving three solutions.  $\square$

**Proposition 9.** *The  $D_4$ -equivariant orthogonal error bases are as follows:*

- for orbit type  $(2,1,1)$ , two isolated solutions;
- for orbit type  $(2,2)$ , two isolated solutions.

*Proof.* Any solution for  $D_4$  must also be a solution for its  $\mathbb{Z}_4$  subgroup. In Proposition 5 we saw that these form a single 2-parameter family; they can only be preserved if  $f = x$  or  $f = x + y$ , and the points on the  $z$ -axis are either  $\{0, \pi\}$ , which yields orbit type  $(2, 1, 1)$ , or  $\{-\pi/2, \pi/2\}$ , which yields orbit type  $(2, 2)$ .  $\square$

**Proposition 10.** *There are no  $D_n$ -equivariant orthogonal error bases for  $n \geq 5$ .*

*Proof.* If there is no equivariant OEB for the cyclic subgroup there can be none for the full dihedral group. The result therefore follows from Proposition 6.  $\square$

### Other subgroups of $\text{SO}(3)$ .

**Proposition 11.** *The tetrahedral subgroups have two equivariant orthogonal error bases, both of orbit type  $(4)$ .*

*Proof.* Any solution for the tetrahedral group must also be a solution for its  $\mathbb{Z}_3$  subgroup. These form a 2-parameter family of tetrahedra. Since the tetrahedral group preserves only a regular tetrahedron and its dual, there will be exactly two solutions corresponding to the vertices of those tetrahedra.  $\square$

**Proposition 12.** *The octahedral subgroups have one equivariant orthogonal error basis, of orbit type  $(1, 3)$ .*

*Proof.* Any solution for the octahedral group must also be a solution for its  $D_4$  subgroup. Only one of these equivariant for the full octahedral group, with three points at the face centres of a cube of centre-to-face length  $\pi$ , and the final point at the origin.  $\square$

**Proposition 13.** *The icosahedral subgroups have no equivariant orthogonal error bases.*

*Proof.* There is no equivariant OEB for the  $D_5$  subgroup, so there will be none for the full icosahedral group.  $\square$

### 3.5.2 Higher dimensions

In this section we consider the problem of constructing an equivariant UEB for representations of dimension greater than two.

#### Construction for permutation representations.

Recall that a representation  $\rho : G \rightarrow U(n)$  is a *permutation representation* if there exists an orthonormal basis of  $\mathbb{C}^n$  in which  $\rho(g)$ ,  $g \in G$  are all permutation matrices. In this special case, equivariant UEBs can be constructed from Hadamard matrices satisfying a certain equivariance condition.

**Proposition 14.** *Let  $(G, \rho)$  be a permutation representation, and let  $H$  be a Hadamard matrix that commutes with all permutation matrices  $\rho(g)$ . Then the following are elements of a  $G$ -equivariant unitary error basis:*

$$(U_H)_{ij} = \frac{1}{N} H \circ \text{diag}(H, j)^\dagger \circ H^\dagger \circ \text{diag}(H^T, i) \quad (3.9)$$

Here  $\text{diag}(M, i)$  is the diagonal matrix whose diagonal is the  $i$ th row of  $M$ .

*Proof.* It is proven in [78, Corollary 35] that this is a UEB; showing  $G$ -equivariance is a simple exercise in matrix algebra.  $\square$

We will use this construction to prove Theorem 5. First we need the following lemma.

**Lemma 6.** *Let  $M$  be a circulant matrix of dimension  $\geq 3$  whose first column vector  $(a, b, \dots, b)$  has first entry  $a$  and all other entries  $b$ . 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:*

$$\frac{n-2}{n} \leq |a| \leq 1 \quad (3.10) \quad |b|^2 = \frac{1-|a|^2}{n-1} \quad (3.11) \quad \text{Re}(\alpha^* \beta) = \frac{2-n}{2} \frac{|b|}{|a|} \quad (3.12)$$

*Proof.* For unitarity it is sufficient that the rows form an orthonormal basis. It is clear from the symmetry of  $M$  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  $b$ :

$$|b|^2 = \frac{1 - |a|^2}{n - 1} \quad (3.13)$$

$$\operatorname{Re}(a^*b) = \frac{2 - n}{2}|b|^2. \quad (3.14)$$

We will demonstrate that (3.10) is necessary and sufficient for us to find  $b$  satisfying these equations. It is obvious that (3.13) is satisfiable if and only if  $|a| \leq 1$ . Letting  $a = |a|\alpha, b = |b|\beta$ , equation (3.14) then reads as follows:

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

Since  $-1 \leq \operatorname{Re}(\alpha^*\beta) \leq 1$ , and  $\alpha, \beta$  can be freely adjusted to give  $\operatorname{Re}(\alpha^*\beta)$  any value in that range, we see that the following is necessary and sufficient for (3.14) to be soluble:

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

Use of the equation (3.13) and a short calculation demonstrates that this is equivalent to the lower bound in the inequality (3.10).  $\square$

**Theorem 5.** *There exists a  $G$ -equivariant unitary error basis for every permutation representation  $(G, \rho)$  of dimension less than 5.*

*Proof.* We use the construction in Proposition 14. Expressed in the  $G$ -permuted orthonormal basis,  $\operatorname{Im}(\rho)$  will be some subgroup of the permutation matrices  $S_n$ . To use Theorem 14, we must find a Hadamard matrix in the centraliser of  $\rho(G)$ . In the worst case,  $\operatorname{Im}(\rho)$  will be all permutation matrices.

For dimension less than 5, there exists a Hadamard matrix which commutes with all permutation matrices. We ignore the degenerate case  $n = 1$ . For  $n = 2$  the following family of Hadamard matrices commutes with  $S_2$ , where  $|a| = |b| = 1/\sqrt{2}$  and  $\operatorname{Re}(a^*b) = 0$ :

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

For  $n \geq 3$ , the centraliser of  $S_n$  is the group of circulant matrices of the type described in Lemma 6; the conditions for such a matrix to be unitary were given there. Setting  $|a| = |b|$  in (3.11), it follows that  $|a| = 1/\sqrt{n}$ . This is compatible with (3.10) only for  $n \leq 4$ .  $\square$



Table 3.2: Simple monomial representations for  $A_5$ .

$()$	$(1, 2)(3, 4)$	$(1, 2, 3)$	$(1, 2, 3, 4, 5)$	$(1, 2, 3, 5, 4)$
1	1	1	1	1
5	1	-1	0	0
5	1	2	0	0
6	-2	0	1	1
6	2	0	1	1

### Showing nonexistence.

In this section we provide a method for proving nonexistence of an equivariant unitary error basis for some representations  $(G, \rho)$ .

**Definition 9.** A unitary matrix is *monomial* if it has precisely one nonzero entry in each row and column, all of which are necessarily elements of  $U(1)$ . A representation  $\rho : G \rightarrow U(n)$  on some  $n$ -dimensional vector space  $V$  is *monomial* [33] if it admits an orthonormal basis of  $\mathbb{C}^n$  in which all the matrices  $\rho(g), g \in G$  are monomial.

$G$ -equivariant unitary error bases for  $(G, \rho)$  are  $G$ -equivariant orthonormal bases of  $\text{End}(V) \simeq \rho \otimes \rho^*$ , all of whose elements are unitary maps. Therefore, if  $(G, \rho)$  admits an equivariant UEB, then  $\rho \otimes \rho^*$  must be monomial. It is also well known [33] that every monomial representation is a direct sum of representations induced from one-dimensional representations of subgroups. We therefore obtain the following proposition.

**Proposition 15.** *If  $(G, \rho)$  admits an equivariant UEB, then  $\rho \otimes \rho^*$  must split as a direct sum of representations induced from one-dimensional representations of subgroups.*

This condition is straightforward to check using characters in a computer algebra program such as GAP [43]. As an example, we exhibit a 3-dimensional representation for which no equivariant UEBs exist.

*Example 3.* We show that the 3-dimensional irreducible representations of the alternating group  $A_5$  admit no equivariant unitary error basis. In Table 3.2 are shown the characters of the induced monomial representations of the alternating group  $A_5$  of dimension less than or equal to 9. We see that  $\chi_{V_i}(1, 2, 3, 4, 5) = (\pm\sqrt{5} + 1)/2$ ; this means that  $\chi_{V_i \otimes V_i^*}(1, 2, 3, 4, 5)$  has a multiple of  $\sqrt{5}$  as a summand for both of  $i = 1, 2$ . However, all the monomial characters of  $A_5$  of degree less than 9 have integer values.  $\chi_{V_i \otimes V_i^*}$  can therefore not be decomposed as a  $\mathbb{Z}_+$ -linear combination of monomial characters.

## 3.6 Appendix to Chapter 3

### 3.6.1 Existence of $G$ -invariant maximally entangled states

Here we prove the result stated in Remark 1.

**Definition 10.** A state  $\omega$  of a  $G$ -representation is *invariant up to a phase* if  $g \cdot \omega = \theta(g)\omega$  for some homomorphism  $\theta : G \rightarrow U(1)$ .

**Lemma 7.** *Let  $A, B$  be  $G$ -representations of identical dimension. A maximally entangled pure state  $\omega \in A \otimes B$  invariant up to a phase exists iff  $A \simeq \theta \otimes B^*$  for some  $\theta : G \rightarrow U(1)$ .*

*Proof.* Suppose the representation  $A$  is the dual of  $B$  up to a character  $\theta$ . Then let  $\omega$  be the unit  $\eta : \mathbb{1} \rightarrow \theta^* \otimes A \otimes B$  witnessing the duality  $\theta^* \otimes A \simeq B^*$ . In the other direction, suppose there exists a state stabilised up to a phase. Any maximally entangled state is of the form

$$\sum_i |i\rangle \otimes X |i\rangle$$

for some orthonormal basis  $\{|i\rangle\}$  and unitary  $X$ . Working in that basis we have the following, for all  $g \in G$ , and where  $\rho_A(g)^T$  is the transpose in the basis  $\{|i\rangle\}$ :

$$\begin{aligned} g \cdot \sum_i |i\rangle \otimes V |i\rangle &= \sum_i \rho_A(g) |i\rangle \otimes \rho_B(g) V |i\rangle \\ &= \sum_i |i\rangle \otimes \rho_B(g) V \rho_A(g)^T |i\rangle \end{aligned}$$

It follows that  $\rho_B(g) V \rho_A(g)^T = \theta(g) V$ , and therefore that  $\rho_B(g) = \theta(g) V \rho_A(g)^* V^\dagger$  for all  $g$ , where  $\rho_A(g)^*$  is the complex conjugate matrix. The result follows by definition of the dual representation.  $\square$

# Chapter 4

## Perfect and tight teleportation schemes for compact Lie transformation groups

### 4.1 Introduction

The main issue with the perfect tight scheme described in the last chapter is that it is not applicable to all groups. In particular, equivariant unitary error bases do not exist for infinite compact Lie groups, which occur more commonly in physical implementations such as ground-to-satellite teleportation. In this chapter we show how the perfect tight scheme for finite groups can be used to define two new schemes, possible for any compact Lie group, which are in general either perfect *or* tight; we call the *perfect scheme* and the *tight scheme*. (Recall that a *tight* teleportation scheme is one where, to teleport a  $d$ -dimensional quantum state, one uses a maximally entangled state of two  $d$ -dimensional systems and communicates one of  $d^2$  classical messages.) As with prior alignment schemes, an unspeakable channel is used for communication, although the set of configurations will now generally be continuous. (We will show how the constructions of unspeakable channels in Section 3.4 can be extended to the continuous case.)

The key property differentiating both our schemes from previous methods for teleportation in the case of reference frame misalignment is that they require no initial alignment phase, and may be applied in situations where prior alignment is unfeasible; in particular, in situations where the reference frame alignment is changing rapidly. We now briefly describe the main properties of the two schemes.<sup>1</sup>

---

<sup>1</sup>In this discussion we use the same terminology as in Chapter 3, with the goal of the scheme

- *Tight scheme.* This scheme has improved purity in general compared to the standard teleportation protocol, and possesses the following desirable properties, all of which are shared with the standard teleportation protocol when reference frame alignment is assumed.
  - *Dynamical robustness (DR).* The scheme is not affected by changes in reference frame alignment during transmission of the classical message from Alice to Bob.
  - *Minimal entanglement (ME).* The parties only require a  $d$ -dimensional maximally entangled resource state.
  - *Minimal communication (MC).* Only 2 dits of unspeakable classical information are communicated from Alice to Bob.
  - *Minimal operations (MO).* Alice performs a  $d^2$ -valued measurement in a fixed orthonormal basis, and Bob performs corrections from a fixed basis of  $d^2$  unitaries. Neither party realigns their frame either actively or passively, or performs any computations.
  - *No reference frame leakage (NL).* No information about either party’s reference frame alignment is transmitted.<sup>2</sup>
- *Perfect scheme.* This scheme performs perfect teleportation, up to a global phase, while retaining properties (DR) and (ME) of the tight scheme. It violates (MC), (MO) and (NL); in particular, it requires a classical channel capable of communicating full reference frame information. Its key advantage over prior alignment schemes is the (DR) property.

**Technical outline.** The essential idea of our schemes is to consider a finite subgroup  $H \subset G$  with an  $H$ -equivariant unitary error basis, and bootstrap the previous results to obtain a protocol that is immune to errors arising from the subgroup  $H$ .

With no prior knowledge of the reference frame transformation relating Alice’s and Bob’s frames, the effective channel<sup>3</sup> for a conventional protocol will be a uniform average over the unitary channels corresponding to each possible misalignment. More formally, let  $i$  be Alice’s measurement result, let  $dg$  be the uniform Haar probability measure on the group  $G$ , let  $\mathcal{T}_{i,g} : B(V) \rightarrow B(V)$  be the unitary channel induced by

---

being for Alice to teleport the quantum state of a  $d$ -dimensional quantum system to Bob.

<sup>2</sup>This has cryptographic significance in some scenarios [13, 49, 56].

<sup>3</sup>The *effective channel* is the channel taking Alice’s original state onto the density matrix encoding Bob’s knowledge about his final state, given his lack of knowledge about Alice’s reference frame alignment.

a conventional teleportation scheme with reference frame misalignment  $g \in G$ , and let  $\sigma \in B(V)$  be the state to be teleported. Then the effective channel superoperator  $\mathcal{T}_i : B(V) \rightarrow B(V)$  is given as follows, as a function of the measurement result  $i$ :

$$\mathcal{T}_i(\sigma) = \int_G dg \mathcal{T}_{i,g}(\sigma) \quad (4.1)$$

The effect of our tight scheme is to replace the uniform probability measure  $dg$  in this expression with a weighted measure  $dg p_i(g)$ , which is peaked around the identity  $g = 1_G$  where the reference frame uncertainty is zero. This has the effect in practice of increasing the fidelity of the overall superoperator  $\mathcal{T}_i$ . Numerical results (see Table 4.1) show that this can for some groups more than double the purity compared to the standard protocol, while in other cases the improvement is more modest.

The factor  $p_i(g) : G \rightarrow \mathbb{R}$  in the new probability measure depends on the subgroup  $H$ , the unspeakable channel, and the encoding scheme used, in such a way that it is peaked around the identity (see Figure 4.1). Explicitly, the unspeakable channel has a space of readings  $C$ , which carries a smooth measure-preserving action of the group  $G$  describing how a change in reference frame affects the readings sent through the channel. If Alice measures result  $i$ , she will send a reading from a certain *encoding subset*  $E_i$  associated to that value. Bob, for his part, will perform the correction corresponding to  $i$  if the reading  $g \cdot i$  he receives lies in a certain *decoding subset*  $D_i$ . The factor  $p_i(g) = \mu_C(D_i \cap g \cdot E_i)$  is the measure in  $C$  of the intersection of the image  $g \cdot E_i$  of the encoding region  $E_i$  under the reference frame transformation  $g$  and the decoding region  $D_i$ . For an important class of unspeakable channels, the factor  $p_i(g)$  will be derived from a *fundamental domain*  $F$  for the subgroup  $H \subset G$ . (See Figure 4.1 for  $G = U(1)$ .)

For our perfect scheme, additional reference frame information is transmitted by Alice, reducing reference frame uncertainty exactly to the finite group  $H$ ; the measurement result is simultaneously communicated, so that the previous results [95, 96] can be applied to perform perfect teleportation. Our techniques allow us to ‘fold’ the measurement result in with the reference frame information, obviating the need to communicate it through a separate channel, and most importantly, maintaining the novel dynamical robustness property.

**Constructions and calculations.** Our schemes have two requirements: an  $H$ -equivariant unitary error basis and a compatible unspeakable classical channel. The existence of  $H$ -equivariant unitary error bases was addressed in the last chapter. Here we show how the construction of compatible unspeakable channels from shared

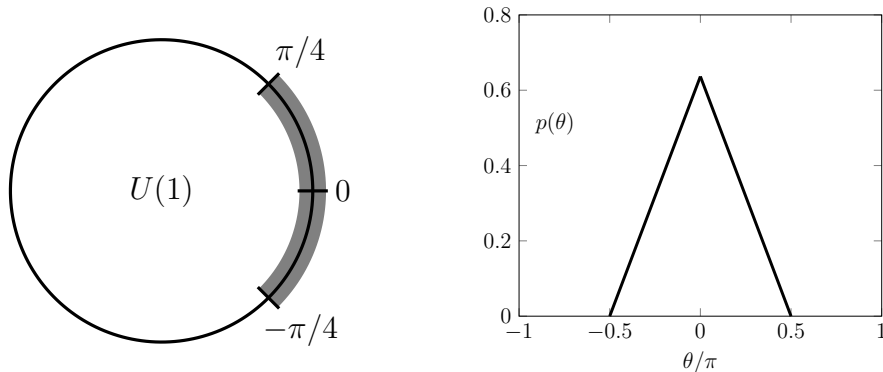


Figure 4.1: The reference frame transformation group  $U(1)$  is parameterised by a single angle variable  $\theta \in [-\pi, \pi)$ , and has cyclic subgroup  $\mathbb{Z}_4 \subset U(1)$  with fundamental domain  $F = (-\pi/4, \pi/4)$ , highlighted in the left subfigure. The effective channel for a conventional protocol is a uniform average over all  $\theta \in [-\pi, \pi)$ ; the effect of our tight scheme with a reference frame channel is to reduce this to a weighted average with factor  $p(\theta)$  shown in the right subfigure.

reference frame systems given in Section 3.4 can be extended to the case of continuous spaces and infinite groups.

We derive an expression for the effective channel induced by our tight teleportation scheme, which we use to calculate channel purity<sup>4</sup> for a variety of groups and unspeakable channels. In particular, we consider  $G = U(1)$ , arising in teleportation with polarised photons and energy eigenstates of different eigenvalues; and  $G = SU(2)$ , arising in teleportation with spin- $\frac{1}{2}$  particles. Comparing this with the purity for a standard protocol, where an unspeakable channel is not used, we numerically confirm improved purity in each case. The results are shown in Table 4.1.

**Criticism.** Compared to conventional teleportation, our tight scheme shows only a small improvement for the group  $U(1)$ , for which there already exist experimental methods for dealing with misalignment in optical systems [34, 93] (although these existing methods, based on decoherence free subspaces, are not tight.) Improvements for  $SU(2)$  are more substantial. Also, we emphasise that both our tight scheme and

---

<sup>4</sup>We define channel purity as the normalised purity of the Choi-Jamiołkowski state associated to the quantum channel induced by the protocol, where we take a convex sum over all frames  $g \in G$ , weighted by the Haar measure. Where figures are numerical estimates we give an error range in the reported figure.

Transformation group	Conventional purity	New tight scheme purity
U(1)	0.59	0.62 (reference frame channel)
SU(2)	0.21	0.32 $\pm$ 0.02 (reference frame channel) 0.44 $\pm$ 0.03 (rod channel)

Table 4.1: A comparison of the purity achieved by conventional teleportation and our new tight scheme. The numbers shown are purity values for the effective channel, calculated in Section 4.8. For SU(2), the purity is given for two different unspeakable channels which could be used to implement our scheme.

our perfect scheme require an unspeakable classical channel on which the reference frame acts nontrivially; by comparison, previous schemes based on prior alignment make use of an unspeakable *quantum* channel [9, 14, 50, 51, 81, 90].

**Outlook.** Our approach may be applicable to other multi-party protocols in the case of reference frame uncertainty; these include quantum key distribution [17, 40], where reference frame-independent protocols correspond to equivariant complementary orthonormal bases. It may also be possible to generalise our teleportation schemes to continuous variable systems [82]. Such a generalisation would allow us to extend our results to locally compact groups such as the Poincaré group, for which the Haar measure still exists but irreducible representations are in general no longer finite dimensional.

**Related work.** Chiribella et al [25] showed that perfect reference frame-independent teleportation can be achieved only if the state to be teleported is itself invariant under the group action. This result does not apply to our schemes, since we make use of an unspeakable classical channel, a possibility that this previous work did not consider.

Imperfect teleportation with an infinite group of reference frame transformations has been considered by other authors. Chiribella et al [25] considered perfect teleportation with vanishing error in the limit of infinite entangled resources; Marzolino and Buchleitner [69] considered teleportation of identical particles under a particle number superselection rule<sup>5</sup>; and Kitaev et al [56] showed that a shared quantum reference system could be used to approximate perfect quantum protocols. All these approaches require the size of the shared entangled resource to increase; in contrast,

---

<sup>5</sup>Here both parties use a particle reservoir to perform operations, and the phase difference in the reservoirs corresponds to the action of a U(1) transformation group.

our schemes have the same entanglement requirements as standard quantum teleportation. Our schemes also apply to arbitrary compact Lie groups, whereas the approach of Marzolino and Buchleitner [69] is specific to  $U(1)$  uncertainty.

**Outline.** In Section 4.2 we give an informal example of our schemes in the case of continuous spatial reference frame uncertainty. In Section 4.3 we provide a framework for sending classical information through an unspeakable classical channel with an continuous space of readings. In Section 4.4 we specify operational procedures underlying our two schemes. In Section 4.5 we show how a shared reference frame system may be used to construct compatible encodings for any equivariant unitary error basis. In Section 4.6 we finally define our tight and perfect teleportation schemes. In Section 4.7 we give another example in the case of phase reference frame uncertainty, which uses the formalism we have developed. In Section 4.8 we derive numerical results for the tight scheme, shown in Table 4.1. In the appendices we recall the effect of reference frame transformations on states and operations, and prove Theorem 6 and some technical results about Voronoi cells.

## 4.2 Example

We begin with an informal example, using the same scenario as in Section 3.2. Alice and Bob are spatially separated, and their qubits are spin- $\frac{1}{2}$  particles. Alice plans to teleport a state  $\sigma$  to Bob. They each possess half of the following maximally entangled pair<sup>6</sup>:

$$|\eta\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

However, they do not have a shared spatial reference frame: the Cartesian frame according to which Alice’s  $x$ -,  $y$ - and  $z$ -spin axes are defined is related to Bob’s by some unknown three-dimensional rotation. The reference frame transformation group is  $SU(2)$ , which acts on a qubit Hilbert space  $H$  by its standard matrix representation  $\rho : SU(2) \rightarrow B(H)$ . The transformation  $g(t) \in SU(2)$  which relates Alice’s and Bob’s frames at time  $t$  is unknown, and may vary on timescales shorter than the message transmission time between the parties.

---

<sup>6</sup>Note that the entangled state is invariant under changes in reference frame, so both parties’ frames may shift arbitrarily following its creation without affecting the quality of the entangled resource.



**Conventional scheme.** We first suppose that Alice and Bob use the entangled state  $|\eta\rangle$  to attempt a standard teleportation protocol [18], based on the Pauli unitary error basis:

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad U_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad U_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad U_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (4.2)$$

Alice measures the state  $\sigma$  together with her entangled qubit in the maximally entangled orthonormal basis  $|\phi_i\rangle = (\mathbb{1} \otimes -i(U_i U_2)^T) |\eta\rangle$ , and communicates the measurement result to Bob through an ordinary classical channel. Bob then applies the correction  $U_i$  to his half of the entangled state. Should both parties' reference frames be aligned, Bob's system will finish in the state  $\sigma$ .

However, if Bob's frame is related to Alice's by a nontrivial transformation  $g \in \text{SU}(2)$ , then from the perspective of Alice's frame, Bob will not perform the intended correction  $U_i$ , but rather the conjugated unitary

$$\rho(g)^\dagger U_i \rho(g). \quad (4.3)$$

Since the conjugation action of  $\text{SU}(2)$  has kernel  $\{\pm I\}$ , we only consider the quotient  $\text{SO}(3)$  in the following analysis. The transformation  $g$  is unknown, so we must average over the whole of  $\text{SO}(3)$  to find the effective channel, which for measurement result  $i$  yields the following expression:

$$\mathcal{T}_i(\sigma) = \int_{\text{SO}(3)} dg [\rho(g)^\dagger U_i \rho(g) U_i^\dagger](\sigma) \quad (4.4)$$

Here  $dg$  is the Haar measure on  $\text{SO}(3)$ , and we have used the notation  $[X](\sigma)$  for the conjugation  $X\sigma X^\dagger$ . Averaging over the four equiprobable measurement results, we find (Section 4.8.3) that the effective channel purity is approximately 0.21.

**Tight scheme.** Alice considers a cube centered at the origin of her frame, oriented so that the  $x$ -,  $y$ - and  $z$ -axes form normal vectors to its faces; we call the faces intersected by the  $x$ -,  $y$ - and  $z$ -axes the 1-, 2- and 3-faces respectively. She measures in the basis  $\{|\phi_i\rangle\}$ , and transmits her measurement result using the encoding scheme given in Table 4.2, and illustrated in Figure 4.2, which we summarize as follows. If Alice receives measurement result 0, she sends a spherically symmetric object (in other words, a sphere) to Bob. Otherwise, if she receives measurement result  $n \in \{1, 2, 3\}$ , she prepares a rigid rod in an arbitrary orientation in space, centred at the origin of her frame, such that it intersects the  $n$ -faces of the cube. She then sends this object through space to Bob by parallel transport.

Measurement result	Classical transmission
0	Featureless sphere
1	Rod oriented along any axis intersecting the 1-faces
2	Rod oriented along any axis intersecting the 2-faces
3	Rod oriented along any axis intersecting the 3-faces

Table 4.2: Tight encoding scheme for the rod channel. Alice chooses the precise orientation of the rod uniformly at random from the set of all orientations satisfying the intersection condition.

When Bob receives the object from Alice, he performs the reverse of Alice’s encoding scheme. If he receives the spherically symmetric object he performs correction  $U_0$ . If he receives a rod, he moves it by parallel transport to his origin, and observes which faces of the cube it intersects. Bob’s cube will of course in general be oriented differently to Alice’s, and so he may observe a different intersection than that encoded by Alice. Having observed an intersection with the  $n$ -faces, he then performs correction  $U_n$ .

We emphasise that since Alice performs one of 4 actions, and Bob receives one of 4 messages, the scheme transmits precisely 2 bits of classical information. Bob can observe the exact orientation of the rod in his frame, but this conveys no further information, since Alice’s measurement result was uniformly random, and so any rod orientation was equally possible.

To see why this encoding scheme leads to increased overall purity for the final state, consider the octahedral subgroup  $\text{Oct} \subset \text{SO}(3)$  preserving the cube. The Pauli UEB is *equivariant* for the action of this subgroup, and is permuted inversely to the labels on the cube’s faces under reference frame transformations in this subgroup. By Theorem 2, teleportation is therefore perfect if the reference frame misalignment is in the group  $\text{Oct} \subset \text{SO}(3)$ . It follows from our later analysis (Theorem 6) that, for reference frame error uniformly distributed in  $\text{SO}(3)$ , the expression (4.4) for the effective channel under the tight scheme just described becomes the following, where the new probability measure  $dg p_i(g) : G \rightarrow \mathbb{R}$  is proportional to the spherical measure of the intersection of the spherical projections of the  $i$ -faces with their image under the rotation  $g \in \text{SO}(3)$ :

$$\mathcal{T}_i(\sigma) = \int_{\text{SO}(3)} dg p_i(g) [\rho(g)^\dagger U_i \rho(g) U_i^\dagger] (\sigma). \quad (4.5)$$

This changes the effective probability distribution over possible misalignments from the uniform distribution to a distribution which is peaked around the identity, where

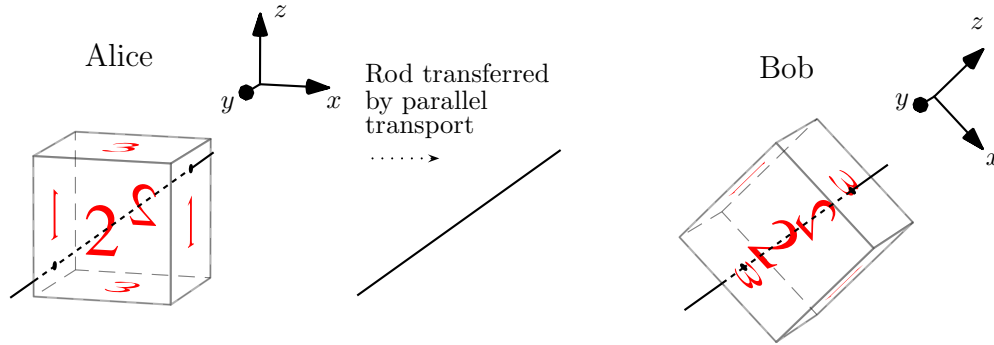


Figure 4.2: Tight encoding scheme for the rod channel. Alice measures 1, chooses at random an orientation of the rod which intersects the 1-faces of the cube in her frame, and communicates the rod to Bob by parallel transport along a straight path. In Bob's frame, related to Alice's by a  $\pi/4$ -rotation around the  $y$ -axis, the rod intersects the 3-faces; he therefore performs the correction  $U_3$ .

the induced errors will be less pronounced. In Section 4.8.3 we describe a numerical calculation of the purity of the effective channel as  $0.44 \pm 0.03$ , approximately double the value for a conventional scheme.

Finally, this scheme is indeed *tight*. We illustrate the properties of the procedure that we claimed in Section 4.1:

- (ME), (ML). Immediate.
- (DR). The effective channel (4.5) is unaffected by changes in reference frame orientation during execution, as long as Bob's reference frame does not change between observing the rod in his lab and performing the corresponding correction.
- (NL). To an observer outside Alice's lab, the information she communicates is uniformly random. This follows from the fact that her measurement outcomes are equiprobable, and given the measurement outcome  $i$  all directions through the corresponding face pair of the cube are equiprobable. Therefore, nothing can be deduced from her transmission about her reference frame orientation.
- (MC). There are four messages Bob can receive: a spherically symmetric object, or a rod oriented through the  $i$ -faces for some  $i \in \{1, 2, 3\}$ . All four messages are equiprobable. He therefore obtains precisely two bits of classical information.

Measurement result	Alice's rotation $r^A$	Bob's observation $r^B$
0	()	() or (234) or (243)
1	(132)	(142) or (132) or (12)(34)
2	(123)	(13)(24) or (123) or (143)
3	(134)	(134) or (124) or (14)(23)

Table 4.3: Type C encoding scheme for the reference frame channel.

**Perfect scheme.** We now give an example of our scheme for perfect teleportation. We call the following family of unitary matrices the *tetrahedral* qubit unitary error basis:

$$\begin{aligned}
V_0 &= \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix} & V_2 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2}e^{2\pi i/3} \\ \sqrt{2} & e^{5\pi i/3} \end{pmatrix} \\
V_1 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2}e^{4\pi i/3} \\ \sqrt{2}e^{4\pi i/3} & e^{5\pi i/3} \end{pmatrix} & V_3 &= \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2} \\ \sqrt{2}e^{2\pi i/3} & e^{5\pi i/3} \end{pmatrix}
\end{aligned} \tag{4.6}$$

This UEB is equivariant for the tetrahedral subgroup  $\text{Tet} \subset \text{SO}(3)$  preserving a regular tetrahedron centred at the origin with vertices:

$$v_0 = \hat{z} \quad v_1 = \frac{1}{3}(\sqrt{8}\hat{x} - \hat{z}) \quad v_2 = \frac{1}{3}(-\sqrt{2}\hat{x} + 2\sqrt{3}\hat{y} - \hat{z}) \quad v_3 = \frac{1}{3}(-\sqrt{2}\hat{x} - 2\sqrt{3}\hat{y} - \hat{z})$$

We identify the elements of  $\text{Tet} \cong A_4$  with the permutation they induce on these vertices.

Alice again measures in the basis  $\{|\phi_i\rangle\}$ , where  $|\phi_i\rangle = (\mathbb{1} \otimes -i(V_i U_2)^T) |\eta\rangle$ . To perform the classical communication, Alice uses a completely asymmetric classical object whose orientation exactly determines a frame of reference. In order to transmit the measurement result  $i$ , she aligns the asymmetric object so that the frame determined by its orientation matches her own Cartesian frame. She then rotates the object by an element  $r^A \in \text{Tet}$ , according to the prescription in Table 4.3, and sends it to Bob. Bob observes the orientation of the object according to his own Cartesian frame, and realigns his frame (actively or passively) by the smallest possible angle so that the rotation  $r^B$  taking his frame onto that determined by the orientation of the asymmetric object is in  $\text{Tet}$ . He then uses Table 4.3 to decide which measurement result  $j$  to correct for, and performs — in his own frame — the correction  $V_j$ .

It will be shown in Proposition 23 that this procedure results in perfect teleportation. Of the properties considered in Section 4.1, it possesses the (DR) property, since the parties' reference frame orientation may change arbitrarily during the measurement and transmission phases, and need only remain constant between Bob's

receipt of the classical information and his performance of the corresponding correction; it clearly also uses an entangled resource of minimal dimension, and so satisfies (ME). However, the procedure violates (MC), (NL) and (MO), since Bob must realign his frame in order for the protocol to be successful, and he gains information about Alice’s reference frame alignment from the orientation he receives.

## 4.3 Encoding schemes for continuous channels

### 4.3.1 Continuous unspeakable channels

In this section we extend the previous definition of unspeakable channels (Definition 3) to the case of a continuous space of readings.

**Definition 11.** We say that a classical channel *communicates unspeakable information* [81], or is an *unspeakable channel*, if its space of readings  $C$  is itself described with respect to the reference frame, carrying a nontrivial smooth measure-preserving action of the reference frame transformation group  $G$ .

A channel whose space of readings is not described with respect to the reference frame, and which therefore carries a trivial  $G$ -action, is called a *speakable channel*.

Throughout this paper we make the simplifying assumption that there is no channel noise; whatever reading Alice sends through the channel will be received unaltered by Bob, although his description of it may be different. A channel is therefore fully described by its space of readings and the  $G$ -action on that space; for this reason we conflate the channel and its space of readings, using the same letter  $C$  for both.

*Example 4.* The channels used in Section 4.2 were unspeakable channels for the group  $G \simeq \text{SU}(2)$  of spatial rotations.

*Example 5.* If  $G \simeq \text{U}(1)$  is the group of time translations of a quantum system<sup>7</sup>, so that a frame corresponds to a choice of a ‘zero of time’  $t_0$ , then a channel through which a signal is sent to arrive at a fixed time, and whose space of readings corresponds to the time of arrival of the signal with respect to the period, is an unspeakable channel. (This is the continuous version of Example 2.)

### 4.3.2 Compatible encoding schemes for continuous actions

We now specify a framework for encoding of measurement values in an unspeakable channel with a continuous space of readings, which allows us to extend the notion of

---

<sup>7</sup>This reference frame transformation group naturally occurs when the states  $|0\rangle$  and  $|1\rangle$  of a qubit are energy eigenstates with different eigenvalues.

a compatible channel to the continuous setting.

**Definition 12** (Encoding scheme). Let  $C$  be an unspeakable channel and  $I$  be a finite set of values to be sent through it. An *encoding scheme* for  $I$  is:

- A space of subsets  $\{E_i \subset C \mid i \in I\}$ , the *encoding subsets*, where  $E_i$  are disjoint open sets.
- A space of subsets  $\{D_i \subset C \mid i \in I\}$ , the *decoding subsets*, where  $D_i$  are disjoint open sets which cover  $C$  up to a set of measure zero.

The encoding subset  $E_i$  is the set of all possible readings Alice can send in order to transmit the value  $i \in I$ . The decoding subset  $D_i$  is the set of all possible readings upon receipt of which Bob will record the value  $i \in I$ .

As before, the success of our protocol depends on encoding schemes which are compatible with the right action of  $H$  on the index set of the UEB. We define a general notion of compatibility of an encoding scheme with a right action.

**Definition 13** (Compatible channel). Let  $C$  be an unspeakable channel for a finite group  $H$ . Let  $\sigma : I \times H \rightarrow I$  be a right action of  $H$  on an index set  $I$ . We say that an encoding scheme for  $I$  is *compatible with  $\sigma$*  if:

- The decoding subsets  $\{D_i\}_{i \in I}$  and the encoding subsets  $\{E_i\}_{i \in I}$  are permuted under the action of  $H$  on  $C$ , inducing left actions  $\tau_D, \tau_E : H \times I \rightarrow I$ .
- The left actions  $\tau_D, \tau_E : H \times I \rightarrow I$  are equal and inverse to the action  $\sigma : I \times H \rightarrow I$  of  $H$  on  $I$ . That is, for all  $i \in I$ ,

$$\tau_D(i, -) = \tau_E(i, -) = \sigma^{-1}(i, -).$$

In other words, given a right action of the reference frame transformation group on a set, a compatible encoding scheme for that set induces the inverse left action on the values sent through the channel.

## 4.4 Two teleportation procedures

In this section we define the operational procedures which Alice and Bob will follow in our teleportation schemes.

Our approach depends on the existence of a compatible encoding scheme for the action  $\sigma : I \times H \rightarrow I$  induced by the right conjugation action of the finite subgroup

$H \subset G$  on an equivariant UEB with index set  $I$ . In Section 4.5, we will show, using an unspeakable classical channel corresponding to a shared reference frame system, a compatible encoding scheme for any *transitive* right action  $\sigma$  of  $H$  may be constructed.

As in the finite case (Section 3.4), to ensure that our procedures can be applied to nontransitive actions, we use the orbit splitting of  $I$  under the  $H$ -action. Alice will first communicate, through a speakable channel, the orbit  $O \subset I$  of her measurement result; she will then communicate the measurement index  $i \in O$  using an unspeakable classical channel with the set of messages  $O$ , compatible with the restricted action  $\sigma|_O : O \times H \rightarrow O$ , which is transitive and therefore amenable to our construction in Section 4.5. As before, this does not affect any of the desirable properties of the teleportation schemes. Of course, if one can find an equivariant UEB with a single orbit under the  $H$ -action [96], such as the tetrahedral UEB for  $\text{BTet} < \text{SU}(2)$  in Section 4.2, or combine different orbits in a single physical channel, as in Section 4.7, this prior speakable communication of the orbit label is unnecessary.

Throughout this section and the rest of the chapter, let  $H \subset G$  be a finite subgroup, let  $\{U_i\}_{i \in I}$  be an equivariant UEB for  $H$ , let  $\sigma : I \times H \rightarrow I$  be the corresponding right action of  $H$  on the index set of the UEB, let  $I_k \subset I$  be the orbits of  $I$  under  $\sigma$ , where  $k$  is some index for the orbits, and let  $\sigma_k : I_k \times H \rightarrow I_k$  be the corresponding transitive restricted actions.

#### 4.4.1 Teleportation without realignment

We first detail a procedure which satisfies the (MO) property, and which will form the basis of our tight scheme.

**Procedure 3** (Teleportation procedure without realignment). Let  $C$  be an unspeakable channel for  $G$  (and therefore also for  $H$ ), and let  $(D_i^k, E_i^k)_{i \in I}$  be encoding schemes for  $I_k$  compatible with  $\sigma_k : I_k \times H \rightarrow I_k$ .

Alice measures in the basis  $\{|\phi_i\rangle\}_{i \in I}$  as in a standard teleportation protocol (2.2). Let her measurement result be  $i \in I_k$ . The result is transmitted as follows.

1. Alice transmits the orbit label  $k$  through a speakable channel.
2. Alice sends a reading  $x$  chosen uniformly at random from the region  $E_i^k$ .
3. Bob receives  $g \cdot x \in D_j^k$  and performs the correction  $U_j$ .

Here  $g$  is the reference frame transformation taking Alice's frame at the time of measurement onto Bob's frame at the time of receipt.

We derive an explicit expression for the effective channel obtained using Procedure 3 for a general encoding scheme.

**Theorem 6** (Effective channel for Procedure 3). *Suppose that Alice measures some result  $i \in I_k$ . Then the channel induced by Procedure 3 is as follows:*

$$\mathcal{T}_k(\rho) = \frac{|I_k|}{\mu_C(E_0^k)} [\pi(c_i)] \circ \int_G \left( dg p(g) [\pi(g)^\dagger U_0 \pi(g) U_0^\dagger] \right) \circ [\pi(c_i)^\dagger] (\rho) \quad (4.7)$$

Here  $0 \in I_k$  is any element of the orbit; the normalising factor  $\mu_C(E_0^k)$  is the measure of  $E_0^k$  in  $C$ ;  $p(g) = \int_{E_0^k \subset C} dx \mathbb{1}_{D_0^k}(g \cdot x)$ , where  $\mathbb{1}_{D_0^k}$  is a continuous approximation to the indicator function for  $D_0^k \subset C$ ; and  $\{c_i\}_{i \in I_k}$ ,  $c_i \in H$  are such that  $c_i \cdot E_0^k = E_i^k$ .

*Proof.* The proof is somewhat technical, so has been placed in Section 4.9.1.  $\square$

**Proposition 16.** *Procedure 3 satisfies (ME), (DR) and (MO).*

*Proof.* (ME) and (MO) are clear, since the entangled resource, measurements and corrections are exactly as in a conventional teleportation protocol; only the classical communication step has changed.

(DR) is also satisfied. Since the orbit is unaffected by reference frame transformations, we need only consider the second and third stages of the procedure. In Alice's frame, reference frame misalignment affects Bob's reading of the transmitted measurement result, and his unitary correction. Since the interval between both of these events is limited only by Bob's apparatus, we may assume that his reference frame alignment does not change between these steps. Otherwise, the effective channel (4.7) is unaffected by unknown arbitrary changes in reference frame alignment throughout the rest of the procedure, since it involves an average over all misalignments in any case.  $\square$

In general Procedure 3 communicates an infinite amount of reference frame information.

**Proposition 17.** *Suppose Alice measures  $i \in I_k$ , performs Procedure 3, and Bob receives  $y \in C$ . Bob now knows that the reference frame misalignment  $g_{AB} \in G$  lies in the subset*

$$\{g \in G \mid g^{-1} \cdot y = x \text{ for some } x \in \sqcup_j E_j^k\}. \quad (4.8)$$



## 4.4.2 Teleportation with realignment

We now detail a teleportation procedure which involves realignment, and will form the basis of our perfect scheme. For simplicity, we assume that Alice's encoding subsets are singleton sets, as will be the case for our perfect scheme.

**Procedure 4** (Teleportation procedure with realignment). Let  $C$  be an unspeakable channel for  $G$  (and therefore also for  $H$ ), and let  $(D_i^k, E_i^k)_{i \in I}$  be encoding schemes for  $I_k$  compatible with  $\sigma_k : I_k \times H \rightarrow I_k$ . Let  $E_i^k = \{x_i^k\}$ , where  $x_i^k$  is a single reading in  $C$ .

Alice measures in the basis  $\{|\phi_i\rangle\}_{i \in I}$  as in a standard teleportation protocol (2.2). Let her measurement result be  $i \in I_k$ . The result is transmitted as follows.

1. Alice transmits the orbit label  $k$  through a speakable channel.
2. Alice sends the reading  $x_i^k$ .
3. Bob receives  $y = g \cdot x_i^k \in D_j^k$  and performs the correction  $\rho(r_j(y))U_j\rho(r_j(y))^\dagger$ , where  $r_j(y) \in G$  is any element such that  $r_j(y) \cdot x_j^k = y$ .

In words, Bob realigns his frame (actively or passively) so that the reading he receives is  $x_j^k$ , and then performs the correction  $U_j$ . Here  $g$  is the reference frame transformation taking Alice's frame at the time of measurement onto Bob's frame at the time of receipt.

We derive an explicit expression for the effective channel obtained using Procedure 4 for a general encoding scheme.

**Proposition 18** (Effective channel for Procedure 4). *Suppose that Alice measures some result  $i \in I_k$ . Then the channel induced by Procedure 4 is as follows:*

$$\mathcal{T}_i(\sigma) = \int_{\text{Stab}_G(x_i)} ds [\rho(s)^\dagger U_i \rho(s) U_i^\dagger](\sigma) \quad (4.9)$$

Here  $ds$  is the Haar measure on  $\text{Stab}_G(x_i^k)$ .

*Proof.* Alice measures  $i \in I_k$  and communicates  $x_i^k$  to Bob, who receives  $y \in D_j$ , where  $y = g \cdot x_i^k = (r_j(y)h_{ij}s) \cdot x_i^k$  for  $h_{ij} \in H$  such that  $h_{ij} \cdot x_i^k = x_j^k$  and some  $s \in \text{Stab}_G(x_i^k)$ .

The distribution over  $\text{Stab}_G(x_i^k)$  is uniform. We therefore have the following expression for the effective channel:

$$\begin{aligned}
\mathcal{T}_k(\rho) &= \int_{\text{Stab}_G(x_i^k)} ds [\rho(r_j(y)h_{ij}s)^\dagger \rho(r_j(y))U_j \rho(r_j(y))^\dagger \rho(r_j(y)h_{ij}s)U_i^\dagger] (\sigma) \\
&= \int_{\text{Stab}_G(x_i^k)} ds [\rho(h_{ij}s)^\dagger U_j \rho(h_{ij}s)U_i^\dagger] (\sigma) \\
&= \int_{\text{Stab}_G(x_i^k)} ds [\rho(s)^\dagger U_i \rho(s)U_i^\dagger] (\sigma)
\end{aligned}$$

At each step, we used the fact  $\rho$  is a representation. To get the final equality, we used equivariance of the unitary error basis.  $\square$

**Proposition 19.** *Procedure 4 satisfies (ME) and (DR).*

*Proof.* Exactly as in Proposition 16.  $\square$

## 4.5 Continuous reference frame channels

We now show that the construction from reference frame systems given in Section 3.4 can be extended to the continuous setting.

### 4.5.1 Continuous reference frame channels

**Definition 14.** A *reference frame system* is a classical system described according to a reference frame, on whose space of configurations the reference frame transformation group  $G$  acts freely and transitively.

These systems were already considered in the finite case; the construction here will be a straightforward extension to the infinite case.

*Example 6.* The set of orientations of a totally asymmetric solid object in  $n$  dimensions is a reference frame system for the group of  $n$ -dimensional spatial rotations, as in Section 3.2.

*Example 7.* The set of orientations of a single vector of fixed length in the plane, specifying the positive  $x$ -direction, is a reference frame system for the two-dimensional spatial rotation group  $U(1)$ , since the orientation of the positive  $y$ -direction is determined by perpendicularity and parity.

*Example 8.* The classical system of Example 5, where the set of configurations is the time of arrival of the signal, is a reference frame system for the group of periodic time translations  $U(1)$ .

Again, Alice and Bob will use their shared reference frame system to communicate messages, using the well-known fact that any free and transitive left  $G$ -space is isomorphic to the group  $G$  considered as a left  $G$ -space under left multiplication.<sup>8</sup> As before, they associate each of the configurations of the system to an element of  $G$  using a *labelling*, obtained by choosing an element  $x_e \in C$  such that  $l(x_e) = e$ . Again, we assume that there is a canonical procedure (agreed by both parties beforehand) to choose an element  $x_e \in C$  based on one's own frame configuration  $f \in \mathcal{F}$ , where  $\mathcal{F}$  is the space of reference frame configurations, corresponding to a map  $\epsilon : \mathcal{F} \rightarrow C$  satisfying the naturality condition 3.4. We use the same notation as before for labellings and their inverses.

*Example 9.* For the channel of Example 6, one can define  $\epsilon$  by aligning marked orthogonal points on the object with one's own Cartesian frame. For the channel of Example 7, one can define  $\epsilon$  by aligning the vector with one's own  $x$ -axis. For the channel of Example 2, one can define  $\epsilon$  by timing the signal to arrive at one's own zero of time, with respect to the period.

**Proposition 20.** *Let  $\mathcal{F}$  be the space of reference frame configurations, and let Alice and Bob have different frame configurations  $f_A \in \mathcal{F}$  and  $f_B = g_{AB} \cdot f_A$ , which they use to label a reference frame system by fixing  $[e]_A = \epsilon(f_A)$  and  $[e]_B = \epsilon(f_B)$ . Then:*

$$[g]_A = [gg_{AB}^{-1}]_B \quad (4.10)$$

*Proof.* The  $G$  labelling of the channel is defined as  $[g]_A = g \cdot (x_e)_A$ ; we have  $(x_e)_A = \epsilon(f_A)$ , so  $[g]_A = g \cdot \epsilon(f_A) = \epsilon(g \cdot f_A) = \epsilon(g \cdot g_{AB}^{-1} \cdot f_B) = (gg_{AB}^{-1}) \cdot (x_e)_B = [gg_{AB}^{-1}]_B$ .  $\square$

We have seen how labelling of a shared reference frame system allows us to construct an unspeakable channel whose set of messages is the set of elements of  $G$ , and which carries the action (4.10). We call this a *reference frame channel*. As an example of the utility of such a channel, we give a procedure whereby it can be used to transfer full reference frame information in a single shot.

**Procedure 5** (Reference frame information transfer). Alice arranges with Bob to send the reading  $[e]_A$  which is the identity in her labelling. Bob receives it and sees that it is labelled  $[g_{AB}^{-1}]_B$  in his own frame. He thus learns that the reference frame transformation taking Alice's frame *at the time of transmission* onto his own is  $g_{AB}$ .

---

<sup>8</sup>Manifolds on which  $G$  acts freely and transitively are usually known as *principal homogeneous spaces*, or *torsors*.

## 4.5.2 Encoding schemes for continuous reference frame channels

We now use reference frame channels to construct compatible encoding schemes (Definition 13) for any transitive right action of any finite subgroup  $H \subset G$ . In order to characterise the possible transitive right actions of  $H$ , we recall the following well-known fact.

**Lemma 8.** *Let  $H$  be a finite group. Any finite transitive right  $H$ -set is isomorphic to a right coset space  $(H/L)_R$  for some subgroup  $L \subset H$  under the right action  $(Lh_2) \cdot h_1 = Lh_2h_1$ .*

Recall from Proposition 20 that the  $G$ -labelling of  $C$  carries the left action  $[g]_A = [gg_{AB}^{-1}]_B$ . As the first step in defining the encoding scheme for a given transitive right  $H$ -set, we now show how a labelled channel  $C$  may be divided into regions  $[R_h]$  labelled by elements of  $H$ , which, for reference frame changes  $h_{AB} \in H$ , are permuted as  $[R_h]_A = [R_{hh_{AB}^{-1}}]_B$ . To this end, we first recall the definition of a fundamental domain.

**Definition 15.** A *fundamental domain* for the action of  $H$  on  $G$  is an open subset  $F \subset G$  such that the  $H$ -translates  $Fh$  have empty intersection and cover  $G$  up to a set of measure zero.

*Remark 3.* We are trying to approximately limit the domain of possible reference frame transformations to  $F$ . It is therefore sensible to pick  $F$  so that all the readings in it are as close to the identity as possible under some metric. To make this precise one can use Voronoi cells (Definition 26).

Having fixed some fundamental domain  $F$ , we now define the regions  $[R_h]$ .

**Definition 16.** Fix a subgroup  $H \subset G$ , and a fundamental domain  $F$  for  $H$  in  $G$ . Then the regions  $[R_h]$  for  $h \in H$  are defined as

$$[R_h] = [Fh] = \{[fh] \mid f \in F\}.$$

These regions are indeed permuted in the desired way.

**Lemma 9.** *Let Bob's reference frame configuration  $f_B \in \mathcal{F}$  be related to Alice's configuration  $f_A \in \mathcal{F}$  by  $f_B = h_{AB} \cdot f_A$  for  $h_{AB} \in H$ . Then*

$$[R_h]_A = [R_{hh_{AB}^{-1}}]_B.$$

*Proof.* By (4.10) the labelling on the readings transforms as  $[g]_A = [gg_{AB}^{-1}]_B$ ; so

$$[R_h]_A = \{[fh]_A \mid f \in F\} = \{[fhh_{AB}^{-1}]_B \mid f \in F\} = [R_{hh_{AB}^{-1}}]_B.$$

This completes the proof.  $\square$

We now show how to use the above division to obtain compatible encoding schemes  $(D_i^k, E_i^k)_{i \in I_k}$  for each  $(I_k, \sigma_k)$ . We know from Lemma 8 that  $(I_k, \sigma_k)$  is isomorphic as a right  $H$ -set to the right coset space  $(H/L_k)_R$ . Let  $\alpha_k : I_k \rightarrow (H/L_k)_R$  be an isomorphism, where for notational convenience we treat  $\alpha_k$  as a map onto coset representatives rather than onto cosets themselves. That is, we have  $\alpha_k(i) = c_i$  for  $i \in I_k$  and representatives  $c_i \in H$  of the cosets  $L_k c_i$ .

**Definition 17.** Let  $L_k, H$  and  $c_i$  be as above. The *tight reference frame encoding scheme* is defined as:

$$[D_i^k] = \bigsqcup_{l \in L_k} [R_{lc_i}] \qquad [E_i^k] = [D_i^k]$$

The *perfect reference frame encoding scheme* is defined as:

$$[D_i^k] = \bigsqcup_{l \in L_k} [R_{lc_i}] \qquad [E_i^k] = \{[c_i]\}$$

It is clear that these subsets are disjoint and open and that the  $\{[D_i^k]\}_{i \in I_k}$  cover the channel up to a set of measure zero; this is therefore an encoding scheme. We now show compatibility.

**Proposition 21.** *The encoding schemes of Definition 17 are compatible with  $(I_k, \sigma_k)$ . That is, the subsets  $(D_i^k, E_i^k)_{i \in I_k}$  carry the following action of  $H$  under reference frame changes  $h_{AB} \in H$ :*

$$[D_i^k]_A = [D_{\sigma^{-1}(h_{AB}, i)}^k]_B \qquad [E_i^k]_A = [E_{\sigma^{-1}(h_{AB}, i)}^k]_B$$

*Proof.* We have

$$\begin{aligned} [D_i]_A &= \sqcup_{k \in K} [F(kc_i)]_A = \sqcup_{k \in K} [F(kc_i h_{AB}^{-1})]_B = \sqcup_{k \in K} [F(k\alpha(\sigma^{-1}(h_{AB}, i)))]_B \\ &= \sqcup_{k \in K} [F(kc_{\sigma^{-1}(h_{AB}, i)})]_B = [D_{\sigma^{-1}(h_{AB}, i)}]_B. \end{aligned}$$

The result for  $[E_i^k]$  in the perfect encoding follows similarly.  $\square$

## 4.6 Teleportation schemes for compact Lie transformation groups

We now define our teleportation schemes. The tight scheme may be performed with any unspeakable channel, whereas the perfect scheme requires a reference frame channel.

### 4.6.1 Tight teleportation scheme

**Definition 18** (Tight encoding scheme). We say that an encoding scheme  $(D_i^k, E_i^k)_{i \in I_k}$  is *tight* if the encoding subsets  $\{E_i^k\}_{i \in I_k}$  cover the space of readings for all  $k$ .

*Remark 4.* Since the encoding subsets  $\{E_i^k\}_{i \in I_k}$  are permuted transitively under the action of  $H$ , it follows that they all have the same measure.

*Example 10.* The tight encoding scheme for a reference frame channel (Definition 17) is tight. The first encoding scheme in Section 4.2 was tight.

With a tight encoding scheme, Procedure 3 leaks no reference frame information.

**Proposition 22.** *When the encoding scheme is tight, Procedure 3 additionally satisfies (MC) and (NL).*

*Proof.* For a tight encoding scheme, Alice is equally likely to send any reading in the channel, since Alice has an equal probability of measuring any  $i \in I_k$  and chooses a reading with uniform probability from the subsets  $\{E_i^k\}_{i \in I}$ , which have equal measure and cover the space of readings up to a set of measure zero. It follows that the procedure communicates no reference frame information, since without prior knowledge of the reading Alice sent, nothing can be learned from the reading that is received. The (NL) property is therefore satisfied.

The only useful information Bob learns from the message he receives is which of his decoding subsets  $\{D_i^k\}_{i \in I_k}$  the reading he receives lies in; there are  $\sum_k |I_k| = |I| = d^2$  possible messages, which are equiprobable. In total, therefore, he receives two dits of classical information. The (MC) property is therefore also satisfied.  $\square$

We therefore define our tight teleportation scheme as follows.

**Definition 19.** Our *tight teleportation scheme* uses Procedure 3 together with a tight encoding scheme for every orbit  $I_k$ .

## 4.6.2 Perfect teleportation scheme

**Proposition 23.** *Procedure 4 with the perfect encoding scheme on a reference frame channel (Definition 17) induces a perfect teleportation channel.*

*Proof.* Immediate from Proposition 18 and the fact that the stabiliser of any reading in the channel is trivial.  $\square$

We therefore define our perfect teleportation scheme as follows.

**Definition 20.** Our *perfect teleportation scheme* uses Procedure 4 together with a perfect encoding scheme on a reference frame channel for every orbit  $I_k$ .

## 4.7 Phase reference frame uncertainty revisited

Finally, we return to the example of phase uncertainty, which we saw in Section 2.1.3 in the context of ground-to-satellite teleportation. Alice and Bob have an optical link along a line of sight, through which they can perform quantum or classical communication mediated by individual photons or classical beams of light. The axis of this link can be treated as a shared  $z$ -direction. However, there is no shared  $xy$ -frame in the perpendicular plane.

Alice intends to transfer one half of a polarisation-entangled pair of photons to Bob, which can be used to teleport the state of a qubit in her possession. However, reference frame uncertainty may arise from rotation of the devices [61]; if Bob's device rotates around the axis of the optical link, his description of the polarisation state of the transmitted photon will change.

Recall that the reference frame transformation group here is the 2D rotation group  $U(1)$ . If  $\theta \in [0, 2\pi)$  is the angle of a clockwise rotation of the 2D Cartesian frame, we have the following action on the state of the photon:

$$\theta \mapsto \rho(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2i\theta} \end{pmatrix} \quad (4.11)$$

The deleterious effect of this uncertainty on the teleportation channel was shown in (2.4).

**Unspeakable channel and encoding scheme.** We consider how our schemes can be used to improve performance. We propose that Alice use the polarisation of a classical beam of light to communicate the measurement result. We note first that because the action (4.11) has kernel  $\{0, \pi\}$ , we can consider the reduced reference

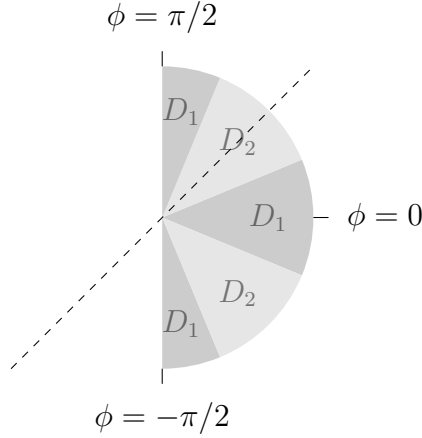


Figure 4.3: The decoding subsets  $[D_1]$  and  $[D_2]$ . The polarisation axis of a beam of light linearly polarised at angle  $\theta = \pi/4$  is shown in the figure.

frame transformation group  $U(1)/\mathbb{Z}_2 \simeq U(1)$ , with parametrisation  $[-\pi/2, \pi/2)$ . The orientation of the polarisation axis of a linearly polarised light beam carries a free and transitive action of this reduced reference frame transformation group and therefore serves as a reference frame channel.

From the results of our previous paper [96, Theorem 4.1], the largest subgroup of  $G$  with an equivariant UEB is  $\mathbb{Z}_4$ ; the equivariant UEB is the set of Pauli matrices (4.2). We choose the fundamental domain in  $G$  as the Voronoi cell of the identity for the metric  $\mu(\theta_1, \theta_2) = |\theta_1 - \theta_2|$  (see Appendix 4.9.2). We define the map  $\epsilon : F \rightarrow C$  by stipulating that the reading labelled by the identity should be the orientation of the  $x$ -axis of the labeller's Cartesian frame.

Under the action of  $\mathbb{Z}_4$ , the only orbit of the Pauli UEB which is not a singleton is  $i \in \{1, 2\}$ . We use the machinery of Section 4.5.2 to define tight and perfect encoding schemes for this orbit. The tight encoding scheme is:

$$\begin{aligned} [D_1] = [E_1] &:= \{[\phi] \mid \phi \in (12\pi/8, 13\pi/8] \cup (15\pi/8, \pi/8] \cup (3\pi/8, 4\pi/8]\} \\ [D_2] = [E_2] &:= \{[\phi] \mid \phi \in (13\pi/8, 15\pi/8] \cup (\pi/8, 3\pi/8]\} \end{aligned} \quad (4.12)$$

The angles here are the polar angles of the polarisation axis with the labeller's  $x$ -axis; the regions  $[D_1]$  and  $[D_2]$  are shown in Figure 4.3. The perfect encoding scheme has  $[D_1]$  and  $[D_2]$  as in (4.12), with  $[E_1] := \{[e]\}$  and  $[E_2] := \{[\pi/4]\}$ .

**Tight scheme.** Following Procedure 3, Alice sends her measurement result as follows. If Alice measures 0 or 3, she transmits a beam of clockwise or anticlockwise



circularly polarised light respectively. Since the direction of circular polarisation is preserved under reference frame transformations, Bob will receive the measurement result as it was sent. However, if she measures 1 or 2, she sends the measurement result encoded in the polarisation axis of a beam of linearly polarised light, using the regions specified in (4.12). If she measures 1, she sends the light linearly polarised along an axis selected uniformly at random from the region  $[E_1]_A$ . If she measures 2, she sends the light linearly polarised along an axis selected uniformly at random from the region  $[E_2]_A$ . Bob then uses  $[D_1]_B$  and  $[D_2]_B$  to decode. By Theorem 6 we calculate the effective channel for measurement result 1 as

$$4 \int_{-\pi}^{\pi} d\theta p(\theta) [\rho(\theta)^\dagger U_1 \rho(\theta) U_1^\dagger](\sigma) \quad (4.13)$$

where  $p(\theta)$  is the modulus of a sawtooth wave:

$$p(\theta) = \left| \frac{(\theta + \pi/2)}{\pi} - \left\lfloor \frac{1}{2} + \frac{(\theta + \pi/2)}{\pi} \right\rfloor \right| \quad (4.14)$$

This integral is straightforward to evaluate for an arbitrary input density matrix. The channel for result 2 is similar. Averaging over the possible measurement outcomes, we find that the tight scheme has the following action on an input density matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & \frac{b}{2} \left( \frac{1}{\pi^2} + 1 \right) \\ \frac{c}{2} \left( \frac{1}{\pi^2} + 1 \right) & d \end{pmatrix} \quad (4.15)$$

We see that the quality of the channel has increased slightly, despite the fact that no reference frame information has been transmitted. In particular, the final state is now asymmetric; our protocol teleports unspeakable information even when values 1 and 2 are measured.

**Perfect scheme.** We now outline our perfect scheme. If Alice measures 0 or 3, she transmits a beam of left or right circularly polarised light respectively; regardless of his reference frame orientation, Bob will receive the polarisation direction transmitted, and perform the required correction. If she measures 1 or 2, she transmits light linearly polarised along the direction  $[0]_A$  or  $[\pi/4]_A$  respectively. Bob observes the polarisation of the light he receives with respect to his own frame. If the polarisation direction is in the region  $[D_1]_B$ , he rotates his frame either actively or passively so that the light is polarised along the direction  $[0]_B$ , and performs the correction  $U_1$ . If the polarisation direction is in the region  $[D_2]_B$ , he rotates his frame either actively or passively so that the light is polarised along the direction  $[\pi/4]_B$ , and performs the correction  $U_2$ . By Proposition 23, this results in perfect dynamically robust teleportation.

## 4.8 Channel purity calculations for tight scheme

In this section we assess our tight scheme in the specific cases of  $U(1)$  and  $SU(2)$  reference frame uncertainty on a qubit, and compute its average purity, comparing this to the purity obtained by the conventional teleportation scheme. Of course, we give no calculations for our perfect scheme, since that yields purity 1 in all cases.

### 4.8.1 Map purity

We begin by introducing the measure we use to evaluate the success of the protocol, the *map purity*  $P(\rho_{\mathcal{T}})$  [85, 86, 105]. We first recall the definition of the Choi-Jamiołkowski (CJ) state of a channel.

**Definition 21.** The *Choi-Jamiołkowski state*  $\rho_{\mathcal{T}}$  of a channel  $\mathcal{T}$  on a Hilbert space of dimension  $d$  is

$$\rho_{\mathcal{T}} = \frac{1}{2}(\mathbb{1} \otimes \mathcal{T})(\omega),$$

where  $\omega$  is the density matrix of the state  $\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$ .

**Definition 22.** The *normalised map purity*  $P(\mathcal{T})$  of a channel  $\mathcal{T}$  on a Hilbert space of dimension  $d$  is the normalised purity of its CJ state; that is,

$$P(\mathcal{T}) = 1 + \frac{\text{Tr}(\rho_{\mathcal{T}} \ln(\rho_{\mathcal{T}}))}{\ln(d^2)} \quad (4.16)$$

For the specific problem of optimising the conventional protocol over the space of all qubit UEBs, we use the normalised linear map purity for ease of calculation.

**Definition 23.** The *linear map purity*  $P(\mathcal{T})$  of a channel  $\mathcal{T}$  on a Hilbert space of dimension  $d$  is defined as the normalised linear purity of its CJ state; that is,

$$P^L(\mathcal{T}) = \text{Tr}(\rho_{\mathcal{T}}^2).$$

The map purity, whether linear or not, is easy to calculate and very similar to minimum purity over pure state inputs in the qubit case [86], which we consider here.

In this work there are two situations in which we need to calculate the map purity. The first situation is optimisation of the linear map purity for standard teleportation over the space of all qubit UEBs. We first note that all our channels are random unitary channels.

**Definition 24.** A *random unitary channel* is a channel of the form

$$\sigma \mapsto \int_X dx [U(x)](\sigma)$$

for some label space and probability measure  $(X, dx)$ , where each  $U(x)$  is a unitary matrix.

In our case, the channel is of the form

$$\sigma \mapsto \sum_i \int_G dg p(i)q(g)[U(i, g)](\sigma)$$

where  $U(i, g)$  are the unitaries, the label space is  $I \times G$ , and the probability measure on the label space is  $dg p(i)q(g)$ ; this is the product of the Haar measure, the probability  $p(i)$  of measurement result  $i$  (which is uniform), and the p.d.f.  $q(g)$  over the set of reference frame alignments. We have the following useful expression for the map purity of these channels.

**Proposition 24** (Map purity of a random unitary channel). *Let  $\mathcal{T}$  be a random unitary channel on a Hilbert space of dimension  $d$ . Let  $I = \{0, \dots, n-1\}$  be a discrete index for the random unitary matrices with probability distribution  $p(i), i \in I$ , and  $g \in G$  be a continuous index with p.d.f.  $q(g)dg$ , such that the probability of a given unitary is  $p(i)q(g)dg$ . Then:*

$$P^L(\mathcal{T}) = \frac{1}{d^2} \sum_{i,j=0}^{n-1} \int_{G \times G} p(i)p(j)q(g)q(g')dgdg' |\text{Tr}(U(i, g)^\dagger U(j, g'))|^2 \quad (4.17)$$

*Proof.* This is a straightforward unpacking of the definition of  $P^L(\mathcal{T})$  for a random unitary channel.  $\square$

We will also need to calculate the map purity from the matrix expression of the superoperator for a given channel. Recall that a superoperator, as a linear map on the space of density matrices, can be written as a  $d^2 \times d^2$  matrix [73, 106]. The density matrix of the CJ state can be obtained by ‘reshuffling’ the entries of this superoperator matrix and multiplying by a scale factor [85], illustrated here for  $d = 2$ :

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{pmatrix} \mapsto \frac{1}{2} \begin{pmatrix} A_{11} & A_{12} & A_{21} & A_{22} \\ A_{13} & A_{14} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{41} & A_{42} \\ A_{33} & A_{34} & A_{43} & A_{44} \end{pmatrix}$$

### 4.8.2 Calculations for U(1)

Here we consider the case  $G = \text{U}(1)$ , where the group of reference frame transformations acts on the qubit state as follows:

$$\theta \mapsto \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (4.18)$$

**Conventional scheme.** We begin by finding the UEB which optimises linear map purity for a conventional protocol. A general qubit UEB may be expressed as  $U\mathcal{E}V$ , where  $U, V$  are arbitrary unitary matrices and  $\mathcal{E} = \{X_0, X_1, X_2, X_3\}$  is the Pauli UEB (4.2). Since we ignore global phase, we need only consider unitaries up to their induced rotation of the Bloch sphere. Let  $R_{\hat{n}}(\theta)$  be a Bloch sphere rotation through an angle  $\theta$  around the  $\hat{x}$  axis; let  $X_i$  be a Pauli rotation (that is, a rotation through an angle  $\pi$  around the  $x$ -,  $y$ - or  $z$  axis); and let  $\hat{x}, \hat{y}$  be two unit vectors which correspond to the choice of UEB. Then the equiprobable unitaries are as follows:

$$U_{ig} = gV^\dagger X_i U^\dagger g^\dagger U X_i V \quad (4.19)$$

$$\sim V g V^\dagger X_i U^\dagger g^\dagger U X_i \quad (4.20)$$

$$= R_{\hat{x}}(\theta) R_{X_i(\hat{y})}(-\theta) \quad (4.21)$$

We write  $\sim$  to indicate that replacing unitaries (4.19) with unitaries (4.20) will yield a channel with the same purity, because of cyclicity of the trace in (4.17). The second equality follows by the fact that conjugating a rotation  $R_{\hat{x}}(\theta)$  by another rotation  $Q$  gives  $Q R_{\hat{x}}(\theta) Q^{-1} = R_{Q(\hat{x})}(\theta)$ . By Lemma 24 we therefore have the following expression for the effective channel:

$$P(\mathcal{T}) = \frac{1}{256\pi^2} \sum_{i,j} \int_0^{2\pi} \int_0^{2\pi} d\theta_1 d\theta_2 |\text{Tr}[R_{X_j(\hat{y})}(-\theta_2) R_{X_i(\hat{y})}(\theta_1) R_{\hat{x}}(\theta_2 - \theta_1)]|^2 \quad (4.22)$$

Here the choice of UEB corresponds to a choice of two unit vectors  $(\hat{x}, \hat{y})$  or equivalently a choice of angles  $(\psi_{\hat{x}}, \psi_{\hat{y}}, \phi_{\hat{x}}, \phi_{\hat{y}}) \in [0, \pi]^2 \times [0, 2\pi]^2$ . The factor in front of the integral is a product of the normalisation factors for the parameterisation of U(1) and the  $1/4$  probabilities for measurement results  $i$  and  $j$ . The simplicity of the integral allows us to numerically evaluate it for given  $\hat{x}, \hat{y}$  with negligible error. We performed Nelder-Mead maximisation over  $\hat{x}, \hat{y}$  and found optimality of the Pauli UEB, corresponding to angles  $(0, 0, 0, 0)$ . The normalised map purity for this UEB is

$$1 + \frac{1}{\ln(4)} (0.75 \ln(0.75) + 0.25 \ln(0.25)) \simeq 0.59.$$

**Tight scheme.** To employ our approach we must choose a finite subgroup  $H \subset U(1)$  for which an equivariant UEB exists. Since the region of integration will be the fundamental domain of such a group, we should choose the largest such subgroup possible; in previous work [96] this was shown to be  $H \simeq \mathbb{Z}_4$ , for which there exists a two-parameter family of equivariant UEBs, all with the same orbit type:

$$U_0 = R_{\hat{z}}(\theta - \pi) \quad U_1 = R_{\hat{z}}(\phi)XR_{\hat{z}}(-\phi) \quad U_2 = R_{\hat{z}}(\phi)YR_{\hat{z}}(-\phi) \quad U_3 = R_{\hat{z}}(\theta)$$

Here  $X$  and  $Y$  are the Pauli matrices, and  $R_{\hat{n}}(\theta)$  is the unitary matrix (we ignore phase) which rotates the Bloch sphere through an angle  $\theta$  about the axis  $\hat{n}$ . The Pauli UEB is the member of this family with parameters  $\theta = \pi, \phi = 0$ . The tight reference frame encoding scheme for this family of UEBs was given in (4.12).

We use Theorem 6 to calculate the superoperator for the effective channel. Because the group is abelian, conjugation by  $\pi(c_i)$  is irrelevant, so the channel will be identical for measurements 1 and 2. For a similar reason we need only consider the Pauli UEB, since all UEBs in the family yield identical channels. It is easy to derive an analytic expression for  $p(g)$ ; we stated it at the end of Section 4.7. There we also stated the action on an input density matrix for measurement results 1 and 2. The normalised map purity for the effective channel is

$$1 + \frac{1}{\ln(4)} \left( \frac{1 + 3\pi^2}{4\pi^2} \ln \left( \frac{1 + 3\pi^2}{4\pi^2} \right) + \frac{-1 + \pi^2}{4\pi^2} \ln \left( \frac{-1 + \pi^2}{4\pi^2} \right) \right) \simeq 0.62.$$

### 4.8.3 Calculations for SU(2)

We now consider the case  $G = \text{SU}(2)$ , acting on a qubit state by its defining representation.

**Conventional scheme.** We have a channel of the form (4.17), which involves integration over  $\text{SU}(2)$ . In order to obtain a parametrisation and measure for the integral, we use the isomorphism between  $\text{SU}(2)$  and the unit quaternions. These quaternions, being diffeomorphic to the 3-sphere  $S^3$ , may be parametrised by hyperspherical coordinates  $(\theta, \psi, \phi) \in D$ , where  $D = [0, \pi] \times [0, \pi] \times [0, 2\pi]$ . This parametrisation is inherited by  $\text{SU}(2)$ , along with the Haar measure  $d\Omega$  on  $S^3$ , as follows:

$$g(\theta, \psi, \phi) = \begin{pmatrix} \cos(\theta) + i \sin(\theta) \sin(\psi) \sin(\phi) & (\cos(\psi) + i \cos(\phi) \sin(\psi)) \sin(\theta) \\ -(\cos(\psi) - i \cos(\phi) \sin(\psi)) \sin(\theta) & \cos(\theta) - i \sin(\phi) \sin(\psi) \sin(\theta) \end{pmatrix}$$

$$d\Omega = \frac{1}{2\pi^2} \sin^2(\theta) \sin(\psi) d\theta d\psi d\phi$$

We consider the integrand. Expanding the UEB elements in the form  $U\mathcal{E}V$ , where  $U, V$  are arbitrary unitary matrices and  $\mathcal{E} = \{X_0, X_1, X_2, X_3\}$  is the Pauli UEB, we see that the unitaries of the channel will be, for all  $Y \in \text{SU}(2)$  and  $i \in I = \{1, \dots, 4\}$ ,

$$\begin{aligned} U(Y, i) &= YV^\dagger X_i^\dagger U^\dagger Y^\dagger U X_i V \\ &\sim VYV^\dagger X_i^\dagger U^\dagger Y^\dagger U X_i \end{aligned}$$

where the equivalence is again a consequence of the cyclicity of the trace in (4.17). We therefore obtain the following equation for the map purity:

$$P(\mathcal{T}) = \frac{1}{32} \int_{D \times D} d\Omega_1 d\Omega_2 |\text{Tr}[X_i Y_1 X_i \tilde{U} Y_1^\dagger Y_2 \tilde{U}^\dagger X_j Y_2^\dagger X_j]|^2 \quad (4.23)$$

Here we performed a change of variables from  $Y_i$  to  $\tilde{Y}_i = VY_iV^\dagger$ , using the invariance of the measure; we omit the tilde on the new variable. We also wrote  $\tilde{U} := VU$ ; note that this is the the only significant element in our choice of UEB.

There are only three relevant angle variables in the choice of UEB, corresponding to a choice of a single unitary  $\tilde{U} := VU$ . We performed random sampling of 100 angle triples and computed the linear map purity of the effective channel for the corresponding UEB using (4.23). None of these UEBs outperformed the Pauli matrices. For these the normalised map purity is

$$1 - \frac{1}{2 \ln(4)} \left( \ln \left( \frac{1}{2} \right) + \ln \left( \frac{1}{6} \right) \right) \simeq 0.21.$$

**Tight scheme with rod channel.** The action on the rod channel considered in Section 3.2 can be most easily expressed using the inner product-preserving isomorphism of  $\text{SU}(2)$ -spaces

$$\begin{aligned} S^2 \subset \mathbb{R}^3 &\xrightarrow{\alpha} B(\mathbb{C}^2) \\ (n_x, n_y, n_z) &\mapsto \frac{I + (n_x, n_y, n_z) \cdot (X, Y, Z)}{2}, \end{aligned} \quad (4.24)$$

where  $I, X, Y$  and  $Z$  are the Pauli matrices,  $S^2$  carries the obvious quotient left action of  $\text{SU}(2)$ , and  $B(\mathbb{C}^2)$  carries the left action of  $\text{SU}(2)$  by conjugation. The encoding and decoding regions are then made up of Voronoi cells for the cardinal points under the metric derived from the Hilbert-Schmidt inner product.

Using the above identification, we calculated  $p(g)$  and the integral (4.4) using Monte Carlo integration with rejection sampling [83], took the average over the four measurement results, and found normalised map purity  $0.44 \pm 0.03$ .

**Tight scheme with reference frame channel.** Again, we choose the largest possible subgroup  $H \subset \text{SU}(2)$  for which an equivariant UEB exists; in previous work [96] this was shown to be  $H \simeq \text{BOct}$ , where  $\text{BOct}$  is the binary octahedral group, which has order 48. The group  $\text{BOct} \subset \text{SU}(2)$  is the symmetry group of a cube centered at the origin of the Bloch sphere and whose center-to-face axes we take to be the  $x$ -,  $y$ - and  $z$ -axes. The Pauli UEB is, up to phase, the unique UEB equivariant for this subgroup.

We show in Appendix 4.9.2 that the Frobenius distance function (Definition 27) is an invariant distance function for  $\text{SU}(2)$  such that the Voronoi cell of the identity of any subgroup in  $\text{SU}(2)$  is a fundamental domain (Proposition 25). Let  $F$  be the Voronoi cell of the identity element of the subgroup  $H = \text{BOct}$ .

The channel is perfect for measurement result 0. However,  $\{U_1, U_2, U_3\}$  is a 3-orbit up to a phase under the conjugation action, isomorphic as a right  $H$ -set to the right coset space obtained by taking the quotient of  $H$  by a certain subgroup  $K = \text{Stab}(U_1) \subset H$ . We choose right coset representatives of  $K$  in  $H$  as follows:

$$c_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad c_2 = \frac{1}{2} \begin{pmatrix} 1-i & -1-i \\ 1-i & 1+i \end{pmatrix} \quad c_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}$$

The channel expression is given by Theorem 6. We evaluated the integral using Monte Carlo integration with rejection sampling, took the average over the four measurement results, and found the normalised map purity of the effective channel to be  $0.32 \pm 0.02$ .

## 4.9 Appendix to Chapter 4

### 4.9.1 Proof of Theorem 6

We now provide the postponed proof of this theorem.

**Theorem 7** (Effective channel for a general encoding scheme). *Suppose that Alice measures some result  $i \in I_k$ . Then the channel induced by Procedure 3 is as follows:*

$$\mathcal{T}_k(\rho) = \frac{|I_k|}{\mu_C(E_0^k)} [\pi(c_i)] \circ \int_G \left( \text{d}g p(g) [\pi(g)^\dagger U_0 \pi(g) U_0^\dagger] \right) \circ [\pi(c_i)^\dagger] (\rho) \quad (4.25)$$

Here  $0 \in I_k$  is any element of the orbit; the normalising factor  $\mu_C(E_0^k)$  is the measure of  $E_0^k$  in  $C$ ;  $p(g) = \int_{E_0^k \subset C} \text{d}x \mathbb{1}_{D_0^k}(g \cdot x)$ , where  $\mathbb{1}_{D_0^k}$  is a continuous approximation to the indicator function for  $D_0^k \subset C$ ; and  $\{c_i\}_{i \in I_k}$ ,  $c_i \in H$  are such that  $c_i \cdot E_0^k = E_i^k$ .

*Proof.* We define  $U(x) = U_j \mid x \in D_j^k$ . Then, in Alice's frame, Bob's correction will be:

$$\pi(g_{AB})^\dagger U(g_{AB} \cdot x) \pi(g_{AB}),$$

where  $x \in E_i^k$  is the direction sent by Alice. Since both  $g_{AB} \in G$  and  $x \in E_i^k$  are unknown and uniformly distributed, we must average over both. When Alice measures  $i \in I_k$ , the channel is as follows for input state  $\sigma$ :

$$\mathcal{T}_i^k(\sigma) = \frac{1}{\mu_C(E_i^k)} \int_{G \times C} dg dx \mathbb{1}_{E_i^k}(x) [\rho(g)^\dagger U(g \cdot x) \rho(g) U_i^\dagger] (\sigma) \quad (4.26)$$

Here  $\mathbb{1}_{E_i^k}$  is a continuous approximation to the indicator function for the region  $E_i \subset C$ .

First we show that  $\mathcal{T}_i^k = [\rho(c_i)] \circ \mathcal{T}_0^k \circ [\rho(c_i)^\dagger]$ ; that is, every measurement result in a given orbit produces a similar channel. Indeed, since the product measure  $dg d\phi$  is invariant under the left  $G$ -action  $g_1 \cdot (g_2, x) = (g_2 g_1^{-1}, g_1 \cdot x)$  on  $G \times C$ , we can make the change of variables  $(g, x) \mapsto (g c_i^{-1}, c_i \cdot x)$ :

$$\begin{aligned} \mathcal{T}_i^k(\sigma) &= \frac{1}{\mu_C(E_i^k)} \int_{G \times C} dg dx \mathbb{1}_{E_i^k}(c_i \cdot x) [\rho(c_i) \rho(g)^\dagger U(g \cdot x) \rho(g) \rho(c_i)^\dagger U_i^\dagger \rho(c_i) \rho(c_i)^\dagger] (\sigma) \\ &= \frac{1}{\mu_C(E_0^k)} [\rho(c_i)] \circ \int_{G \times C} dg dx \mathbb{1}_{E_0^k}(x) [\rho(g)^\dagger U(g \cdot x) \rho(g) U_1^\dagger] \circ [\rho(c_i)^\dagger] (\sigma) \\ &= [\rho(c_i)] \circ \mathcal{T}_0^k \circ [\rho(c_i)^\dagger] \end{aligned}$$

To obtain the first equality we changed variables and used the fact that  $\rho$  is a representation. For the second equality we used  $\mathbb{1}_{E_i^k}(c_i \cdot x) = \mathbb{1}_{E_0^k}$ , linearity, and the fact that the action of  $G$  on  $C$  is measure-preserving. We can therefore restrict our attention to the channel where Alice measures the index  $0 \in I_k$ .

We will now express the integral for the channel  $\mathcal{T}_0^k$  as a sum over integrals where Bob performs a definite correction. The action  $\nu : (g, x) \mapsto g \cdot x$  is continuous; it follows that the preimages of the open sets  $D_i^k$  under  $\nu$  are open and therefore measurable. That the open sets  $\nu^{-1}(D_i^k)$  cover  $G \times C$  up to a set of measure zero follows immediately from the fact that the  $D_i^k$  cover  $C$  up to a set of measure zero and  $\nu$  is a submersion. We may therefore split the domain of integration over the  $\nu^{-1}(D_i^k)$ :

$$\mathcal{T}_0^k(\sigma) = \frac{1}{\mu_C(E_0^k)} \sum_{i \in I_k} \int_{G \times C} dg dx \mathbb{1}_{E_0^k}(x) \mathbb{1}_{D_i^k}(g \cdot x) [\rho(g)^\dagger U_i \rho(g) U_0^\dagger] (\sigma)$$



Now we observe that the integrals over  $\nu^{-1}(D_i^k)$  are identical for all  $i \in I_k$ :

$$\begin{aligned} \mathcal{T}_0^k(\sigma) &= \frac{1}{\mu_C(E_0^k)} \sum_{i \in I_k} \int_{G \times C} dg dx \mathbb{1}_{E_0^k}(x) \mathbb{1}_{D_i^k}(g \cdot x) [\rho(c_i^{-1}g)^\dagger U_0 \pi(c_i^{-1}g) U_0] (\sigma) \\ &= \frac{|I_k|}{\mu_C(E_0^k)} \int_{G \times C} dg dx \mathbb{1}_{E_0^k}(x) \mathbb{1}_{D_0^k}(g \cdot x) [\rho(g)^\dagger U_0 \rho(g) U_0] (\sigma) \end{aligned}$$

The first equality uses that  $U_i = \rho(c_i) U_0 \rho(c_i)^\dagger$ , while in the second we performed the change of variables  $(g, x) \mapsto (c_i g, x)$  and noted that  $\mathbb{1}_{D_i^k}((c_i g) \cdot x) = \mathbb{1}_{D_0^k}(g \cdot x)$ . By Fubini's theorem this may be evaluated as an iterated integral, where  $x$  is integrated over first:

$$\mathcal{T}_0^k(\sigma) = \frac{|I_k|}{\mu_C(E_0^k)} \int_G dg \int_C dx \mathbb{1}_{E_0^k}(x) \mathbb{1}_{D_0^k}(g \cdot x) [\rho(g)^\dagger U_0 \rho(g) U_0] (\sigma)$$

This produces a weighting for  $g \in G$  which is precisely the measure in  $C$  of the set  $D_0^k \cap (g \cdot E_0^k)$ . The result follows.  $\square$

## 4.9.2 Voronoi cells

**Definition 25.** We say that  $G$  has an invariant distance function if there is some distance function  $\mu : G \times G \rightarrow \mathbb{R}$  which makes  $G$  into a metric space and is invariant under translation, i.e.  $\mu(g_1, g_2) = \mu(gg_1, gg_2) = \mu(g_1g, g_2g)$  for all  $g_1, g_2, g \in G$ .

**Definition 26.** If  $G$  has an invariant distance function, we define the *Voronoi cells*  $\{V_h \mid h \in H\}$  as follows:

$$V_h = \{g \in G \mid \mu(h, g) < \mu(\tilde{h}, g) \forall \tilde{h} \neq h\}$$

That is, the Voronoi cell of  $h \in H$  is the set of all  $g \in G$  which are closer to it than to any other element of  $H$ .

It is often possible to use the Voronoi cell  $V_e$  of the identity as a fundamental domain. In our calculations for  $SU(2)$  uncertainty in Section 4.8, we use the Voronoi cell of the identity under the Frobenius distance function as a fundamental domain for  $B\text{Oct} \subset SU(2)$ . We now define the Frobenius distance function and show that the Voronoi cell of the identity for this distance function on  $SU(2)$  is indeed a fundamental domain.

**Definition 27.** For a matrix Lie group embedded in  $M(n)$ , one may consider the matrices within  $G$  as forming a submanifold of  $\mathbb{C}^{n^2}$ ; the Euclidean distance on that space induces a metric on  $G$  by restriction, which we call the *Frobenius distance function*:

$$\mu_F(M_1, M_2) = \sqrt{\frac{1}{d} \text{Tr}[(M_1 - M_2)^\dagger (M_1 - M_2)]}$$

In order to show that the Voronoi cell of the identity is a fundamental domain, we first prove a simple lemma.

**Lemma 10.** *Let  $G$  be a compact Lie group with invariant distance function  $\mu$ , and let  $H \subset G$  be a finite subgroup. Then the Voronoi cells  $V_h$  are the  $H$ -translates  $V_e h$ . Moreover, the Voronoi cell of the identity  $V_e$  is a fundamental domain if for every  $h \in H$ ,  $h \neq e$ , the set*

$$\{g \in G \mid \mu(g, e) = \mu(g, h)\} \tag{4.27}$$

*has measure zero.*

*Proof.* It is easy to see that the Voronoi cells are all  $H$ -translates of the Voronoi cell of the identity. Indeed, for  $x \in V_e$  we have that  $\mu(e, x) < \mu(h, x)$  for all  $h \neq e$ . We therefore see that  $xh \in V_h$ , since  $\mu(h_2, xh) = \mu(h_2 h^{-1}, x)$ , which is minimised when  $h_2 h^{-1} = e$ , that is, when  $h_2 = h$ . Therefore  $V_h = V_e h$ .

For the first statement, the  $\{V_h\}_{h \in H}$  clearly cover  $G$  except for some subset of the union

$$\bigcup_{h_1, h_2 \in H} \{g \in G \mid \mu(h_1, g) = \mu(h_2, g)\}$$

of sets of points equidistant from two elements of  $H$ . If this is of measure zero then  $V_e$  will be a fundamental domain. Now note that  $\mu(h_1, g) = \mu(h_2, g) \Leftrightarrow \mu(e, g^{-1}h_1) = \mu(g, h_2)$ . Let  $\bar{g} = g^{-1}h_1$ . We have

$$\begin{aligned} \bigcup_{h_1, h_2 \in H} \{g \in G \mid \mu(h_1, g) = \mu(h_2, g)\} &= \bigcup_{h_1, h_2 \in H} \{(\bar{g} \in G \mid \mu(e, \bar{g}) = \mu(h_1 \bar{g}^{-1}, h_2)\} \\ &= \bigcup_{h_1, h_2 \in H} \{(\bar{g} \in G \mid \mu(e, \bar{g}) = \mu(h_2^{-1} h_1, \bar{g})\} \\ &= \bigcup_{h \in H} \{(\bar{g} \in G \mid \mu(e, \bar{g}) = \mu(h, \bar{g})\}, \end{aligned}$$

so the union of sets of points equidistant from two elements of  $H$  has measure zero if and only if the union of sets of points equidistant from the identity and one other element of  $H$  does.  $\square$

Finally, we show for  $SU(2)$  under the Frobenius distance function that the Voronoi cell of the identity is a fundamental domain.

**Proposition 25.** *For any  $h \in SU(2)$ , the subset  $\{g \in G \mid \mu(g, e) = \mu(g, h)\}$  has measure zero, where  $\mu$  is the Frobenius distance function.*

*Proof.* We have:

$$\begin{aligned}\mu(g, h)^2 &\sim |\mathrm{Tr}[(g - h)^\dagger(g - h)]| \\ &= |\mathrm{Tr}[2 \cdot \mathbb{1} - (h^\dagger g + g^\dagger h)]| \\ &= 2|2 - \mathrm{Re}(\mathrm{Tr}[gh^\dagger])|\end{aligned}$$

For  $\mu(g, e) = \mu(g, h)$  it is therefore necessary that

$$|2 - \mathrm{Re}(\mathrm{Tr}[gh^\dagger])| = |2 - \mathrm{Re}(\mathrm{Tr}[g])| \quad (4.28)$$

Note that  $\mathrm{Re}(\mathrm{Tr}[u]) = \mathrm{Tr}[u] = 2 \cos(\theta_u/2)$  for any  $u \in SU(2)$ , where  $\theta_u$  is the angle of the corresponding rotation of the Bloch sphere. Now we have<sup>9</sup> the following equation for the angle of rotation  $\theta_{12}$  of the composition  $R_{\hat{n}_2}(\theta_2) \circ R_{\hat{n}_1}(\theta_1)$  of two special unitary matrices which are rotations of the Bloch sphere through angles  $\theta_1, \theta_2$  around the axes  $\hat{n}_1, \hat{n}_2$  respectively:

$$c_{12} = c_1 c_2 - s_1 s_2 \hat{n}_1 \cdot \hat{n}_2 \quad (4.29)$$

Here  $c_{12} = \cos(\theta_{12}/2)$ ,  $c_i = \cos(\theta_i/2)$  and  $s_i = \sin(\theta_i/2)$ . Suppose we have some  $g = R_{\hat{n}_1}(\theta_1)$ ,  $h = R_{\hat{n}_2}(\theta_2)$  for which Equation 4.28 holds. Then we have  $c_{12} = c_2$ . We consider small changes in  $c_1$ . Locally parametrising  $SU(2)$  by the angle of rotation  $\theta_1$  and the spherical polar angles  $\phi_1 \in [-\pi, \pi)$ ,  $\psi_1 \in [0, \pi)$  determining  $\hat{n}_1$ , it is easy to check that there is no point at which  $\frac{\partial c_{12}}{\partial \theta_1} = \frac{\partial c_{12}}{\partial \phi_1} = \frac{\partial c_{12}}{\partial \psi_1} = 0$ . Therefore, we can always change the value of  $c_{12}$  in Equation 4.29 by a small change in  $c_1$ . It follows that the set has measure zero, since the Haar measure on  $SU(2)$  is induced by a Riemannian metric.  $\square$

---

<sup>9</sup>See Exercise 4.15 of [79].

## Part II

# Quantum pseudo-telepathy

# Chapter 5

## Pseudo-telepathy and noncommutative mathematics

**Nonlocal games in quantum information theory.** Bell showed [15] that the experimental predictions of quantum mechanics violate those of classical mechanics. *Nonlocal games* are a family of scenarios in which these violations are clearly observed. In these games two or more non-communicating parties, possibly sharing an entangled state, must perform a task for which guaranteed success would ordinarily require communication.

For a two-player game, the general set-up is as follows. The players Alice and Bob communicate with a third party called the verifier. The game is defined by four sets  $X_A, X_B, Y_A, Y_B$  (Alice's input set, Bob's input set, Alice's output set, and Bob's output set) and a subset  $R \subset X_A \times X_B \times Y_A \times Y_B$ . Alice and Bob know this information, but may not communicate once the game has begun. When the game starts, the referee sends Alice and Bob elements  $x_A \in X_A, x_B \in X_B$  respectively, and they must return elements  $y_A \in Y_A, y_B \in Y_B$  respectively; they win the game if  $(x_A, x_B, y_A, y_B) \in R$ . (See Figure 5.1.) They may share some classical randomness before the game begins; while allowing for probabilistic mixtures of classical strategies may improve the winning probability, the classical correlations Alice and Bob share are necessarily independent of the vertices  $x_A, x_B$  they each receive from the verifier.

This is not the case when the two non-communicating players share a pair of entangled quantum systems, since one player's measurements on their half of the entangled state will affect the outcomes of the other player's measurements on the other half. Since quantum mechanics does not permit superluminal signalling, Alice and Bob cannot use these correlations to communicate; they can nevertheless use the correlations to coordinate their responses to the verifier, thereby increasing their

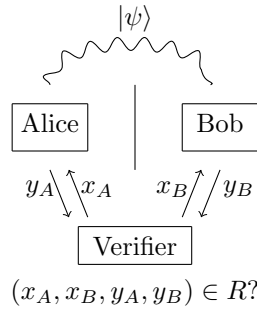


Figure 5.1: The setup for a two-player nonlocal game. While Alice and Bob may not communicate, they may share an entangled state  $|\psi\rangle$  which they can use to coordinate their response to the verifier.

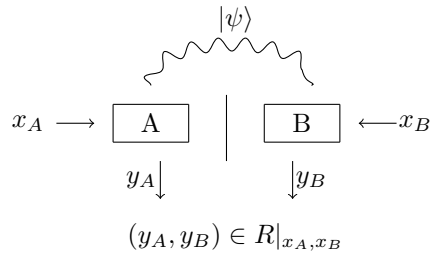


Figure 5.2: An application of quantum pseudo-telepathy to distributed quantum computation. Using shared entanglement, two unconnected nodes compute the relation  $R$  on a given input.

success probability for some games. This phenomenon has been called *quantum pseudo-telepathy* [22], because Alice and Bob’s success makes it seem as though they have communicated, even though no communication has occurred.

This phenomenon has been usefully applied to distributed quantum computation [21], zero-error communication [32] and device-independent quantum cryptography [2]. We briefly describe the first of these. Suppose that a distributed computer contains two unconnected nodes  $A, B$ , which can each receive data from sets  $X_A, X_B$ , and transmit data from sets  $Y_A, Y_B$ . (See Figure 5.2.) A strategy for the nonlocal game is then precisely a strategy allowing  $A, B$  to compute the relation  $R$ . That is, whenever  $x_A, x_B$  are received by the nodes, they will transmit  $y_A, y_B$  such that  $(x_A, x_B, y_A, y_B) \in R$ . In general, shared entanglement allows the relation to be computed with higher probability.

It is very natural to ask which nonlocal games have *perfect* strategies with shared entanglement (that is, strategies where Alice and Bob win the game with probability

1), but not without it. In this case, algebraic and combinatorial techniques become much more relevant.

**Two approaches to quantisation.** In particular, a remarkable connection to noncommutative mathematics has recently been identified [65, 76]. Noncommutative mathematics studies noncommutative, or ‘quantum’, analogues of structures in classical mathematics. The approach is as follows: instead of a finite set  $X$ , one considers the finite-dimensional commutative  $C^*$ -algebra  $\mathbb{C}X$  of complex functions  $f : X \rightarrow \mathbb{C}$ , where multiplication in the  $C^*$ -algebra is pointwise multiplication of functions and  $*$  is complex conjugation. It is easy to check that a function  $f : X \rightarrow Y$  induces a  $*$ -homomorphism  $f : \mathbb{C}Y \rightarrow \mathbb{C}X$ . Going the other way, one can obtain a set from a commutative  $C^*$ -algebra by taking its *spectrum*, and a  $*$ -homomorphism between  $C^*$ -algebras contravariantly induces a function between spectra. In categorical language, there is a duality between the category of finite sets and functions and the category of finite-dimensional  $C^*$ -algebras and  $*$ -homomorphisms, called *Gelfand duality*.

Structures on the finite set  $X$  induce dual structures on  $\mathbb{C}X$ . For instance, a group structure on  $X$  (a multiplication function  $m : X \times X \rightarrow X$ , an inversion map  $i : X \rightarrow X$ , and a map  $e : \{\cdot\} \rightarrow \mathbb{X}$  picking out the identity element, obeying the conditions defining a group) induces a  $*$ -homomorphism  $\tilde{m} : \mathbb{C}X \rightarrow \mathbb{C}X \otimes \mathbb{C}X$ , called the *comultiplication*, a homomorphism  $\tilde{i} : \mathbb{C}X \rightarrow \mathbb{C}X$ , called the *antipode*, and a homomorphism  $\tilde{e} : \mathbb{C}X \rightarrow \mathbb{C}$ , called the *counit*. The equations making  $(X, m, i, u)$  into a group imply that  $(\mathbb{C}X, \tilde{m}, \tilde{i}, \tilde{e})$  is a *Hopf  $*$ -algebra* (for a definition, see [66]), which is commutative, since multiplication of functions is commutative. Going the other way, the structure of a Hopf  $*$ -algebra on a commutative finite-dimensional  $C^*$ -algebra induces the structure of a group on its spectrum. One may therefore identify finite groups with finite-dimensional commutative Hopf algebras.

Once a structure has been formulated in terms of a commutative  $C^*$ -algebra, it is easy to ‘quantise’ it: one simply drops the commutativity condition on the  $C^*$ -algebra. A *finite quantum set*, therefore, is simply a general (i.e. possibly noncommutative) finite-dimensional  $C^*$ -algebra. (We generally conflate sets with their associated algebras, simply referring to finite dimensional  $C^*$ -algebras as quantum sets, rather than ‘function algebras on complex sets’.) A *finite quantum group* is a general (i.e. possibly noncommutative) finite-dimensional Hopf  $*$ -algebra. The theory of these quantum structures may be developed analogously to the classical theory, although there is generally no obvious structure on the other side of the duality. These arguments extend from finite sets to compact topological spaces; a *compact quantum topological space* is a  $C^*$ -algebra, and a *compact quantum group* is

a Hopf  $*$ -algebra.

It is also possible to quantise functions. Since functions between sets induce  $*$ -homomorphisms between their corresponding algebras, we may take  $*$ -homomorphisms between quantum sets to correspond to ordinary functions. However, the  $*$ -homomorphisms between two  $C^*$ -algebras form an ordinary set, not a quantum set. One is therefore led to seek a definition of *quantum functions*. There are several ways to obtain this: for instance, one involves a universal construction in the category of  $C^*$ -algebras and  $*$ -homomorphisms [92], while another is motivated by diagrammatic calculus and topology [76]. They all result in the same definition in the finite-dimensional case: a quantum function  $A \rightarrow B$  is a  $*$ -homomorphism  $\mathbb{C}B \rightarrow \mathbb{C}A \otimes B(H)$ , where  $H$  is some auxiliary finite-dimensional Hilbert space. A notion of *quantum bijection* then can be defined [76], and from there a notion of *quantum graph isomorphism* [76].

It is not obvious that this has anything to do with quantum information theory. However, there is a deep and surprising connection to nonlocal games, at least in the setting of perfect strategies. This is because we can also define a notion of quantisation using nonlocal games: one finds a nonlocal game whose perfect classical strategies are all the instances of a certain type of mathematical object. One can then define the quantum analogue of that type of mathematical object to be the thing whose instances are the perfect quantum strategies (i.e. those using a shared entangled state). We now introduce the particular example we consider in this thesis.

**Definition 28** ([6]). The graph isomorphism game is defined by two graphs  $\Gamma, \Gamma'$  with vertex sets  $V_\Gamma, V_{\Gamma'}$  respectively. The verifier sends vertices  $v_A, v_B \in V_\Gamma$  to Alice and Bob respectively, and they return vertices  $w_A, w_B \in V_{\Gamma'}$  to the verifier. Alice and Bob win the game if the relationship between  $w_A$  and  $w_B$  — i.e. ‘same’, ‘connected’ or ‘disconnected’ — is the same as the relationship between  $v_A$  and  $v_B$ .

In a deterministic classical strategy, the vertices Alice and Bob return depend only on the vertices they receive. This corresponds to a function  $f : V_\Gamma \rightarrow V_{\Gamma'}$ , where Alice and Bob return vertices  $f(v_A)$  and  $f(v_B)$  respectively. (To see that they both use the same function  $f_A = f_B = f$ , note that if the verifier sends the same vertex  $x$  to Alice and Bob then they must both return the same vertex, implying  $f_A(x) = f_B(x)$  for all  $x$ .) It is straightforward to check that, for a perfect classical strategy,  $f$  must be a graph isomorphism [6, Sec.3.1].

It turns out that these two approaches to quantisation produce identical definitions of quantum graph isomorphism. One may therefore use the tools of noncommutative topology to construct and classify instances of quantum pseudo-telepathy in the graph isomorphism game.



**The Morita theory of quantum graph isomorphisms.** In the paper [77], the present author and collaborators showed that one can completely classify the finite-dimensional quantum isomorphisms out of a given graph  $\Gamma$  (that is, the strategies for the graph isomorphism game with graphs  $(\Gamma, \Gamma')$  for any graph  $\Gamma'$  which use a finite-dimensional entangled resource), as well as the graphs quantum isomorphic to that graph (that is, the isomorphism classes of graphs  $\Gamma'$  for which the quantum graph isomorphism game with graphs  $(\Gamma, \Gamma')$  can be won with a finite-dimensional entangled resource), in terms of structures in the ‘category of finite-dimensional quantum elements’ of the quantum automorphism group of that graph. We review these results in some detail in Chapter 6, but will give a rough overview now.

The definition of quantum elements of a quantum group can be motivated by observing that the isomorphism classes of irreducible representations of the commutative Hopf  $*$ -algebra  $\mathbb{C}G$ , for some finite group  $G$ , are all one-dimensional, and correspond to the elements of the group.<sup>1</sup> We can therefore analogously define the finite-dimensional ‘quantum elements’ of an (imagined) compact quantum group to be the finite-dimensional representations of its Hopf  $C^*$ -algebra of functions.

We classify finite-dimensional quantum graph isomorphisms out of  $\Gamma$  by considering the finite-dimensional quantum elements of the automorphism group of  $\Gamma$  (these are finite-dimensional *quantum automorphisms*, each corresponding to a strategy for the graph isomorphism game with graphs  $(\Gamma, \Gamma)$  using a finite-dimensional entangled state). Indeed, in the category of finite-dimensional quantum automorphisms of  $\Gamma$ , some of the quantum automorphisms carry an algebraic structure — a *simple dagger Frobenius algebra* — which indicates that they have been obtained by composing a quantum graph isomorphism with its dual (the quantum equivalent of the inverse). We show that any quantum automorphism carrying an algebraic structure of this kind can be split to obtain a quantum graph isomorphism out of the graph, and that, moreover, any quantum isomorphism out of the graph produces such a quantum automorphism by composition with its dual. We therefore obtain a correspondence between  $*$ -isomorphism classes of simple dagger Frobenius algebras in the category of quantum automorphisms of a graph, and quantum isomorphisms out of that graph.

For the graph isomorphism game, we are only really interested in the graphs which are quantum isomorphic, and not the quantum isomorphisms themselves. This is where Morita theory comes in; it allows us to classify the simple dagger Frobenius

---

<sup>1</sup>This can be seen immediately, since the matrix algebra  $B(H)$  has only one irreducible representation, of dimension  $\dim(H)$ ; a commutative  $C^*$  algebra has only one-dimensional factors (which in this case correspond to elements of the group); and the representations of a direct sum of algebras are direct sums of representations of the factors.

algebras which correspond to quantum isomorphisms from the same graph. We say that two algebras are *Morita equivalent* if there is a *dagger bimodule* between them in the category of elements of the quantum automorphism group. This notion of equivalence of simple dagger Frobenius algebras is weaker than  $*$ -isomorphism. We obtain a correspondence between Morita equivalence classes of simple dagger Frobenius algebras in the category of quantum automorphisms of a graph, and quantum isomorphic graphs.

**Constructing quantum graph isomorphisms.** Although this classification is fully general, the category of quantum automorphisms of a given small graph is in general poorly understood. In order to construct isomorphisms, we therefore restrict our attention to the *classical subcategory* of quantum automorphisms generated by the ordinary automorphisms of the graph. (A classical automorphism can be considered as a quantum automorphism with a one-dimensional Hilbert space, and these generate a subcategory under direct sum; see Section 6.3.3.) Perhaps surprisingly, this classical subcategory contains simple dagger Frobenius algebras which split to give nontrivial quantum bijections out of the graph.

In the Chapter 7 we discuss the construction of quantum graph isomorphisms from these algebras in the classical subcategory. First, we classify the algebras, and show that they correspond to subgroups of the automorphism group of the graph of *central type*. These groups generalise the Pauli matrices: like  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , they are groups which have a faithful projective representation as a basis of orthogonal unitary matrices (a *unitary error basis*).

For any one of these algebras which gives rise to a *classical* quantum isomorphic graph (this requires an additional group-theoretical condition, since there are such things as quantum graphs) we explicitly construct the new graph, and the quantum isomorphism giving the strategy for the graph isomorphism game, and consider when this new graph will be isomorphic. We also discuss the connection to the linear constraint system games such as the Mermin-Peres magic square game. It is to be hoped (and is a matter for further computational investigation) that these central type groups will give rise to a large number of new instances of nonlocal games that may be won perfectly using shared entanglement, but not without it.

# Chapter 6

## Quantum bijections and quantum isomorphisms

### 6.1 Introduction

#### 6.1.1 Background

##### Pseudo-telepathy and the graph isomorphism game

Quantum pseudo-telepathy [22] is a well studied phenomenon in quantum information theory, where parties can use non-signalling correlations from pre-shared entanglement to perform tasks classically impossible without communication. These tasks are generally formulated as games; in these games, players are provided with inputs by a verifier, and must each return outputs satisfying some winning condition. One such game is the graph isomorphism game [6], which generalises the linear constraint system games studied intensively in recent years [27, 28, 91].

**Definition 29** ([6]). The graph isomorphism game is defined by two graphs  $\Gamma, \Gamma'$  with vertex sets  $V_\Gamma, V_{\Gamma'}$  respectively. Two non-communicating players, Alice and Bob, communicate with a verifier. The verifier sends vertices  $v_A, v_B \in V_\Gamma$  to Alice and Bob respectively; they return vertices  $w_A, w_B \in V_{\Gamma'}$  to the verifier. Alice and Bob win the game if the relationship between  $w_A$  and  $w_B$  — i.e. ‘same’, ‘connected’ or ‘disconnected’ — is the same as the relationship between  $v_A$  and  $v_B$ .

In a deterministic classical strategy, the vertices Alice and Bob return depend only on the vertices they receive. This corresponds to a function  $f : V_\Gamma \rightarrow V_{\Gamma'}$ , where Alice and Bob return vertices  $f(v_A)$  and  $f(v_B)$  respectively. (To see that they both use the same function  $f_A = f_B = f$ , note that if the verifier sends the same vertex  $x$  to

Alice and Bob then they must both return the same vertex, implying  $f_A(x) = f_B(x)$  for all  $x$ .) A strategy is *perfect* if, using it, Alice and Bob win the game for any input  $x_A, x_B$  sent by the verifier. It is easy to see that, for a perfect classical strategy,  $f$  must be a graph isomorphism [6, Sec.3.1].

We can also consider *quantum strategies*. While Alice and Bob may share an entangled bipartite quantum state and use the non-signalling correlations to synchronise their outputs.

A *quantum graph isomorphism* is a set of projective measurements on a Hilbert space  $H$  of dimension  $d$ , indexed by elements of  $V_\Gamma$  and with outcome set  $V_{\Gamma'}$ , satisfying certain orthogonality conditions. A quantum graph isomorphism defines a quantum strategy, where Alice and Bob perform these measurements their half of a maximally entangled pair of  $d$ -dimensional quantum systems. (More general classes of quantum measurements and entangled states could be considered, but all strategies are quantum graph isomorphisms up to convex combination; this is true of all *synchronous games* [47].)

Quantum pseudo-telepathy in the graph isomorphism game is exhibited by pairs of non-isomorphic graphs which are quantum isomorphic. The only known examples come from quantum but not classically satisfiable linear constraint systems; the smallest known of these has 24 vertices [65], and is obtained from the quantum solution to the well-known Mermin-Peres magic square [72].

## A compositional approach

To find new examples of quantum pseudo-telepathy in the graph isomorphism game and other synchronous games, we propose a new approach. In [76], the author and collaborators show how quantum isomorphisms fit into a general theory of *quantum functions*. A quantum function between classical sets  $X \rightarrow Y$  is an  $X$ -indexed family of projective measurements with outcomes in  $Y$ ; this is a matrix of projectors  $\{P_{x,y}\}_{x \in X, y \in Y}$  on a finite-dimensional Hilbert space  $H_P$  such that each row  $\{P_{x,y}\}_{y \in Y}$  forms an orthonormal decomposition of the identity operator on  $H_P$ .

Quantum functions  $P : X \rightarrow Y$  and  $Q : Y \rightarrow Z$  can be composed, giving a quantum function  $Q \circ P : X \rightarrow Z$ ; explicitly, this is defined as  $(Q \circ P)_{x,z} := \sum_{y \in Y} Q \otimes P$  on the Hilbert space  $H_{Q \circ P} := H_Q \otimes H_P$ . This generalises the ordinary composition of functions. On the other hand, unlike classical functions, for quantum functions  $P, Q : X \rightarrow Y$  with underlying Hilbert spaces  $H_P$  and  $H_Q$  we can consider compatible linear maps  $f : H_P \rightarrow H_Q$  fulfilling  $fP_{x,y} = Q_{x,y}f$  for all  $x \in X, y \in Y$ . These *intertwiners* imply that the quantum functions between two sets form, not a set, but a *category*.

Using this compositional framework, we define notions of quantum bijection and quantum graph isomorphism, recovering the game-theoretical definition and placing it within a broader setting of noncommutative set theory which includes the noncommutative graphs considered in zero-error quantum communication [36]. We also make contact with compact quantum group theory; the category  $\text{QPerm}(A)$  of quantum permutations of a set, and the category  $\text{QAut}(\Gamma)$  of quantum automorphisms of a graph, are finite dimensional representation categories of certain well-studied Hopf  $C^*$ -algebras.

## Quantum bijections from classical symmetries

This framework can be applied to classify and construct quantum bijections. We show in [77] that the quantum bijections into a set  $A$  can be completely classified in terms of algebraic structures in the category  $\text{QPerm}(A)$ . Indeed, any bijection into a set gives a *simple dagger Frobenius monoid* in  $\text{QPerm}(A)$ , and two equivalent quantum bijections give rise to  $*$ -isomorphic Frobenius monoids. Going in the other direction, we can *split* any simple dagger Frobenius monoid in order to obtain the corresponding quantum bijection.

Although a general  $*$ -isomorphism classification of simple dagger Frobenius monoids in  $\text{QPerm}(A)$  currently seems unfeasible, we can focus on the subcategory generated by classical permutations, where the algebraic classification reduces to a group-theoretical one. In this thesis we will focus on this group-theoretical construction of quantum bijections. The relevance for quantum graph isomorphisms is that a graph structure on a set  $A$  can be uniquely ‘pulled back’ along a quantum bijection to make it a quantum isomorphism; this new graph need not be classically isomorphic.

### 6.1.2 Overview of this chapter

In this chapter we will give an accessible overview of the relevant results from the two papers [76, 77]. In the next chapter we will use these results to consider constructions of quantum bijections from group theoretical data, applicable to quantum pseudo-telepathy.

**Contents of this chapter.** In Section 6.2 we introduce Gelfand duality, the basis of our approach to quantum functions. In Section 6.3 we define quantum bijections and explain their various properties. In Section 6.4 we show how quantum graph isomorphisms fit into our framework. In Section 6.1.4 we give a brief overview of the graphical calculus we use to derive many of these results.

### 6.1.3 Notation and conventions.

In this chapter and the next we assume some basic notions in category theory, of the sort that could be found in an introductory course [19, 98].

We make use of the graphical calculus for tensor categories; a brief overview is given in Section 6.1.4. We read diagrams from bottom to top.

All the sets and quantum sets we consider are finite, and all the Hilbert spaces we consider are finite-dimensional.

For a group  $L$ , we write  $Z_L(S)$  and  $N_L(S)$  for the centraliser and normaliser of a subset  $S \subset L$  in  $L$ , respectively. We denote the commutator of two group elements  $a, b \in L$  by  $[a, b] := aba^{-1}b^{-1}$ , and define the commutator of two subsets similarly. We write  $S_n$  for the symmetric group on  $n$  points.

### 6.1.4 The graphical calculus of string diagrams

We make use of the graphical calculus of monoidal dagger categories [29, 88]. Mostly, this will be the graphical calculus of the category **Hilb** of finite-dimensional Hilbert spaces and linear maps. Before commencing the mathematical material, we briefly review this calculus.

In the graphical calculus, morphisms are displayed as *string diagrams*, which we read from bottom to top. In these diagrams of strings and nodes, strings are labelled with objects, and nodes are labelled with morphisms. The string for the monoidal unit  $I$  is not drawn. Composition and tensor product are depicted as follows:

$$\begin{array}{ccc}
 \begin{array}{c} C \\ \circlearrowleft g \\ B \\ \circlearrowleft f \\ A \end{array} & \begin{array}{cc} C & D \\ | & | \\ \circlearrowleft f & \circlearrowleft g \\ | & | \\ A & B \end{array} & (6.1) \\
 gf : A \rightarrow C & f \otimes g : A \otimes B \rightarrow C \otimes D &
 \end{array}$$

In a monoidal dagger category, given a morphism  $f : A \rightarrow B$ , we express its  $\dagger$ -adjoint  $f^\dagger : B \rightarrow A$  as a reflection of the corresponding diagram across a horizontal axis.

Restricting attention to the category **Hilb**, we note that all finite-dimensional Hilbert spaces  $V$  have dual spaces  $V^* = \text{Hom}(V, \mathbb{C})$ , represented in the graphical calculus as an oriented wire with the opposite orientation as  $V$ . Duality is characterized by the following linear maps, here called *cups and caps*:

$$\begin{array}{cccc}
 \begin{array}{c} \curvearrowright \\ V^* \quad V \end{array} & \begin{array}{c} V \quad V^* \\ \curvearrowleft \end{array} & \begin{array}{c} \curvearrowright \\ V \quad V^* \end{array} & \begin{array}{c} V^* \quad V \\ \curvearrowleft \end{array} & (6.2) \\
 f \otimes v \mapsto f(v) & 1 \mapsto \mathbb{1}_V & v \otimes f \mapsto f(v) & 1 \mapsto \mathbb{1}_V &
 \end{array}$$

To define the second and fourth map, we have identified  $V \otimes V^* \cong V^* \otimes V \cong \text{End}(V)$ . It may be verified that these maps fulfill the following *snake equations*:

$$\begin{array}{c} \curvearrowright \end{array} = \begin{array}{c} | \\ \uparrow \end{array} = \begin{array}{c} \uparrow \\ \curvearrowleft \end{array} \quad \begin{array}{c} \curvearrowleft \end{array} = \begin{array}{c} | \\ \downarrow \end{array} = \begin{array}{c} \downarrow \\ \curvearrowright \end{array} \quad (6.3)$$

Together with the swap map  $\sigma_{V,W} : v \otimes w \mapsto w \otimes v$ , depicted as a crossing of wires, this leads to a very flexible topological calculus, allowing us to untangle arbitrary diagrams and straighten out any twists:

$$\begin{array}{c} \text{tangled wires} \end{array} = \begin{array}{c} | \\ | \\ | \\ | \end{array} \quad \begin{array}{c} \text{crossing} \end{array} = \begin{array}{c} | \\ \uparrow \end{array} = \begin{array}{c} \downarrow \\ | \end{array} \quad (6.4)$$

A closed circle evaluates to the dimension of the corresponding Hilbert space:

$$\begin{array}{c} \bigcirc \end{array} = \begin{array}{c} \bigcirc \end{array} = \dim(H) \quad (6.5)$$

## 6.2 Frobenius monoids and Gelfand duality

Our framework for quantum functions puts finite set theory into the setting of linear algebra. In this way, we are able to formulate functions as linear maps, allowing us to generalise the definition to quantum functions of a higher dimension, and also to quantum functions between quantum sets.

To do this we use *Gelfand duality* for finite sets; in particular, a Frobenius algebraic formulation admitting a diagrammatic calculus whose convenience will soon become clear.

### 6.2.1 Frobenius monoids

#### Definitions

Finite sets correspond to certain Frobenius monoids in the category **Hilb** of finite-dimensional Hilbert spaces and linear maps. We first recall the definition of a Frobenius monoid.

**Definition 30.** In a monoidal category, a *monoid* is an object  $M$  with multiplication and unit morphisms, depicted as follows:

$$\begin{array}{ccc}
 \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array} & & \begin{array}{c} | \\ \circ \end{array} \\
 m : M \otimes M \rightarrow M & & u : I \rightarrow M
 \end{array} \tag{6.6}$$

These morphisms are *associative* and *unital*:

$$\begin{array}{ccc}
 \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ \text{---} \\ \circ \\ | \end{array} = \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array} & & \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array} = | = \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array}
 \end{array} \tag{6.7}$$

Analogously, a *comonoid* is an object  $C$  with a coassociative comultiplication  $\delta : C \rightarrow C \otimes C$  and counit  $\epsilon : C \rightarrow I$ . The  $\dagger$ -adjoint 6.1.4 of a monoid in a monoidal dagger category is a comonoid.

For all these multiplication, comultiplication, unit and counit morphisms we draw white nodes rather than labelled boxes, to be concise; we can easily distinguish the morphisms by their type.

**Definition 31.** A *dagger Frobenius monoid* in a monoidal dagger category is a monoid where the monoid and  $\dagger$ -adjoint comonoid structures are related by the Frobenius equation:

$$\begin{array}{ccc}
 \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array} & = & \begin{array}{c} \circ \\ \text{---} \\ \circ \\ | \end{array} & = & \begin{array}{c} \circ \\ \text{---} \\ \circ \\ | \end{array}
 \end{array} \tag{6.8}$$

A dagger Frobenius monoid is *special* if equation (6.9a) holds. In **Hilb**, such a monoid is moreover *symmetric* or *commutative* if one of (6.9b) or (6.9c) holds.

$$\begin{array}{ccc}
 \begin{array}{c} | \\ \circ \\ \text{---} \\ \circ \\ | \end{array} = | & & \begin{array}{c} \circ \\ \text{---} \\ \circ \\ \text{---} \\ \circ \\ | \end{array} = \begin{array}{c} \circ \\ \text{---} \\ \circ \\ | \end{array} & & \begin{array}{c} \circ \\ \text{---} \\ \circ \\ \text{---} \\ \circ \\ | \end{array} = \begin{array}{c} \circ \\ \text{---} \\ \circ \\ | \end{array}
 \end{array} \tag{6.9}$$

a) special                      b) symmetric                      c) commutative

By (6.7) and (6.8), the following cups and caps fulfil the snake equations (6.3):

$$\begin{array}{ccc}
 \begin{array}{c} \circ \\ \text{---} \\ \circ \end{array} := \begin{array}{c} \circ \\ \text{---} \\ \circ \end{array} & & \begin{array}{c} \text{---} \\ \circ \end{array} := \begin{array}{c} \text{---} \\ \circ \end{array}
 \end{array} \tag{6.10}$$

There is also a notion of morphism between dagger Frobenius monoids.



**Definition 32.** A *\*-homomorphism*  $f : A \rightarrow B$  between dagger Frobenius monoids  $A$  and  $B$  is a morphism  $f : A \rightarrow B$  satisfying the following equations:

$$\begin{array}{c} \text{---} \\ \circ f \\ \text{---} \\ \cup \\ \text{---} \end{array} = \begin{array}{c} \cup \\ \text{---} \\ \circ f \\ \text{---} \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ f \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad (6.11)$$

A *\*-cohomomorphism*  $f : A \rightarrow B$  is a morphism  $f : A \rightarrow B$  satisfying the following equations:

$$\begin{array}{c} \cup \\ \text{---} \\ \circ f \\ \text{---} \end{array} = \begin{array}{c} \cup \\ \text{---} \\ \circ f \\ \text{---} \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ f \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ f \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad (6.12)$$

A *\*-isomorphism* is a *\*-homomorphism* which is also a *\*-cohomomorphism*.

It can be shown that the dagger of a *\*-homomorphism* is a *\*-cohomomorphism*; every *\*-isomorphism* is unitary; and every unitary *\*-homomorphism* between dagger Frobenius monoids is a *\*-isomorphism*.

We refer to Frobenius monoids in **Hilb** as Frobenius *algebras*. One important example is the endomorphism algebra of a Hilbert space.

**Definition 33.** The *endomorphism algebra* of a Hilbert space  $H$  is defined to be the following special symmetric dagger Frobenius algebra on  $H \otimes H^*$  (where  $n = \dim(H)$ ):

$$\begin{array}{c} \cup \\ \text{---} \\ \circ \frac{1}{\sqrt{n}} \\ \text{---} \end{array} = \begin{array}{c} \cup \\ \text{---} \\ \circ \frac{1}{\sqrt{n}} \\ \text{---} \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ \sqrt{n} \\ \text{---} \\ \bullet \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ \text{---} \\ \circ \sqrt{n} \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \circ \frac{1}{\sqrt{n}} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \frac{1}{\sqrt{n}} \\ \text{---} \\ \bullet \\ \text{---} \end{array} \quad (6.13)$$

## 6.2.2 Gelfand duality for finite sets

We now recall how finite sets and functions may be identified with Frobenius algebras and their cohomomorphisms, using the framework established by Coecke, Pavlović and Vicary [30].

*Example 11.* Let  $\{|i\rangle\}_{1 \leq i \leq n}$  be an orthonormal basis of a Hilbert space  $H$ . The following multiplication and unit maps and their adjoints form a special commutative

dagger Frobenius algebra on  $H$ :

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \circ \\ \diagup \quad \diagdown \\ \text{---} \end{array} & := & \sum_{i=1}^n \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 & & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 m : |i\rangle \otimes |j\rangle & \mapsto & \delta_{i,j} |i\rangle
 \end{array}
 \qquad
 \begin{array}{ccc}
 \begin{array}{c} \text{---} \\ | \\ \circ \\ | \\ \text{---} \end{array} & := & \sum_{i=1}^n \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 & & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 u : 1 & \mapsto & \sum_{i=1}^n |i\rangle
 \end{array}
 \tag{6.14}$$

In fact, every special commutative dagger Frobenius algebra  $A$  comes from an orthonormal basis of  $A$ ; the basis vectors are given by the copyable elements of  $A$ , defined as follows.

**Definition 34.** A *copyable element* of a special commutative dagger Frobenius algebra  $A$  is a vector  $|\psi\rangle \in A$ , such that the following hold:

$$\begin{array}{ccc}
 \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \circ \\ | \\ \text{---} \end{array} & = & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 & & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 \begin{array}{c} \circ \\ | \\ \text{---} \end{array} & = & \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \circ \\ \diagup \quad \diagdown \\ \text{---} \end{array} \\
 \begin{array}{c} \circ \\ | \\ \text{---} \end{array} & = & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \\
 \begin{array}{c} \circ \\ | \\ \text{---} \end{array} & = & \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \begin{array}{c} \circ \\ | \\ \text{---} \end{array}
 \end{array}
 \tag{6.15}$$

**Theorem 8** ([30, Theorem 5.1.]). *The copyable elements of a special commutative dagger Frobenius algebra  $A$  are an orthonormal basis of  $A$  for which the monoid is defined as in in Example 11.*

Every special commutative dagger Frobenius algebra in **Hilb** is therefore defined by Example (6.14) for some orthonormal basis on a Hilbert space. This gives a correspondence between sets (which can be considered as orthonormal bases of some Hilbert space) and special commutative dagger Frobenius algebras in **Hilb**.

We develop a similar correspondence for functions. For a special commutative dagger Frobenius algebra  $A$ , let  $\widehat{A}$  be its set of copyable elements. It can be shown that function  $\widehat{A} \rightarrow \widehat{B}$  gives rise to a  $*$ -cohomomorphism between  $A$  and  $B$ , and, conversely, every  $*$ -cohomomorphism  $A \rightarrow B$  comes from such a function.

**Corollary 3** ([30, Corollary 7.2.]). *The category of special commutative dagger Frobenius algebras and  $*$ -cohomomorphisms in **Hilb** is equivalent to the category of finite sets and functions.*

This equivalence takes a special commutative dagger Frobenius algebra  $A$  to the set of copyable elements  $\widehat{A}$ , and a set  $X$  to the algebra associated to the orthonormal basis  $\{|x\rangle \mid x \in X\}$  of  $\mathbb{C}^{|X|}$ . We therefore consider the category of finite sets as ‘contained within **Hilb**’ using the following identification.

Set	Hilb
sets of cardinality $n$	special commutative dagger Frobenius algebras of dimension $n$
elements of the set	copyable states of the Frobenius algebra
functions	*-cohomomorphisms
bijections	*-isomorphisms
the one element set $\{*\}$	the one-dimensional Frobenius algebra $\mathbb{C}$

We also broaden our analysis to include noncommutative Frobenius algebras, as is common in noncommutative topology. In noncommutative topology, one identifies finite sets  $X$  with commutative special symmetric dagger Frobenius algebras<sup>1</sup>  $\mathbb{C}X$  of functions  $X \rightarrow \mathbb{C}$ . Structures on  $X$  correspond to dual algebraic structures on the  $\mathbb{C}X$ ; for instance, a monoid structure on  $X$  induces a comonoid structure on the algebra  $\mathbb{C}X$ .

By analogy, one then considers general (i.e. possibly noncommutative) special symmetric dagger Frobenius algebras<sup>2</sup> as dual to finite *quantum sets*. The dual algebraic structures on function algebras  $\mathbb{C}X$  can usually be extended to general special symmetric dagger Frobenius algebras also, giving a method of quantisation. For instance, a comonoid structure on such an algebra could be thought of as dual to a *quantum monoid*.

**Definition 35** (Quantum set). A *quantum set* is defined to be a special symmetric dagger Frobenius algebra (equivalently, a finite-dimensional  $C^*$ -algebra.)<sup>3</sup>

## 6.3 Quantum bijections

### 6.3.1 Definition

We now define the correct notion of a quantum bijection between quantum sets. The simplest approach is based on the fact that an ordinary bijection is a \*-cohomomorphism which is also a \*-homomorphism. We define a quantum bijection analogously, adding an additional Hilbert space wire corresponding to the quantum resource used to perform the bijection.<sup>4</sup>

<sup>1</sup>These are precisely commutative finite-dimensional  $C^*$ -algebras [97, Theorem 4.6 and 4.7].

<sup>2</sup>These are precisely finite-dimensional  $C^*$ -algebras [97, Theorem 4.6 and 4.7].

<sup>3</sup>Properly, this is the function algebra dual to the quantum set, but we conflate the two notions.

<sup>4</sup>For a detailed explanation of our quantisation procedure, see [76, Introduction].

**Definition 36.** A *quantum bijection* between quantum sets  $A$  and  $B$  is a pair  $(H, P)$ , where  $H$  is a Hilbert space and  $P$  is a linear map  $H \otimes A \rightarrow B \otimes H$  satisfying the following:

$$(6.16)$$

**Definition 37.** The *dimension* of a quantum bijection  $(H, P)$  is the dimension of  $H$ , its underlying Hilbert space.

*Remark 5.* A one-dimensional quantum bijection (an *ordinary bijection*) is an ordinary  $*$ -isomorphism of Frobenius algebras, by comparison of (6.11-6.12) with (6.16).

**Definition 38.** We call ordinary bijections from a quantum set to itself *permutations*, and denote the group of permutations of a quantum set  $A$  by  $\text{Perm}(A)$ .

The underlying Hilbert space gives a notion of morphism between quantum bijections.

**Definition 39.** An *intertwiner* of quantum bijections  $(H, P) \rightarrow (H', P')$  is a linear map  $f : H \rightarrow H'$  such that the following holds:

$$(6.17)$$

An equivalent way to define a quantum bijection is as a *dagger-dualisable quantum function* [76, Def. 4.6]. Dualisability is a kind of weak invertibility which is standard in category theory. Here all we need of this definition is its following consequence.

**Theorem 9** ([76, Theorem 4.8]). *For every quantum bijection  $(H, P) : A \rightarrow B$  between quantum sets, there exists a quantum bijection  $(H^*, \bar{P}) : B \rightarrow A$ , whose underlying linear map  $\bar{P} : H^* \otimes B \rightarrow A \otimes H^*$  fulfils equations (6.19) and (6.20), which express that the cups and caps (6.2) are intertwiners.*

$$(6.18)$$

$$\text{Diagram (6.19)} \quad (6.19)$$

$$\text{Diagram (6.20)} \quad (6.20)$$

### 6.3.2 Quantum bijections between classical sets

For the graph isomorphism game, we are particularly interested in quantum bijections between classical sets. In this case, we will now see that Definition 36 reduces to the definition of a controlled projective measurement we saw in the introduction.

**Theorem 10.** *A quantum bijection  $X \rightarrow Y$  between classical sets  $X$  and  $Y$  is a family of projectors  $\{P_{x,y}\}_{x \in X, y \in Y}$  on a Hilbert space  $H$  such that the following holds, for all  $x \in X$  and  $y_1, y_2 \in Y$ :*

$$P_{x,y_1} P_{x,y_2} = \delta_{y_1,y_2} P_{x,y_1} \quad \sum_{y \in Y} P_{x,y} = \mathbb{1}_H \quad (6.21)$$

$$P_{x_1,y} P_{x_2,y} = \delta_{x_1,x_2} P_{x_1,y} \quad \sum_{x \in X} P_{x,y} = \mathbb{1}_H \quad (6.22)$$

*Proof.* The elements of the set  $X$  form a basis of copyable elements of the corresponding algebra (Definition 34). We expand the linear map  $P : H \otimes X \rightarrow Y \otimes H$  in this basis: :

$$P_{x,y} := P$$

As an example, the first equation of (6.16), expanded in the classical basis, becomes  $\delta_{y,y'} P_{x,y} = P_{x,y} P_{x,y'}$ :

$$\delta_{y,y'} P_{x,y} = P_{x,y} P_{x,y'} \stackrel{(6.16)}{=} \dots = P_{x,y} P_{x,y'}$$

The other equations are obtained similarly from (6.16). □

Considering these projectors as arranged in an  $|X| \times |Y|$  matrix, equation (6.21) states that the projectors along each row form a complete orthogonal family, while equation (6.22) requires this for each column also. Matrices of projectors obeying both the row and the column equations have been called *magic unitaries* [12] and *projective permutation matrices* [6] (PPMs). We here adopt the latter terminology.

*Remark 6.* For matrices of projectors, composition of quantum bijections  $P : X \rightarrow Y$  and  $Q : Y \rightarrow Z$  takes the form

$$(Q \circ P)_{x,z} = \sum_{y \in Y} Q_{y,z} \otimes P_{x,y}.$$

A linear map  $f : H \rightarrow H'$  is an intertwiner  $f : (H, P) \rightarrow (H', P')$  if

$$fP_{x,y} = P'_{x,y}f.$$

Quantum bijections only exist between classical sets of the same cardinality.

**Proposition 26** ([76, Prop. 4.17]). *If there is a quantum bijection  $X \rightarrow Y$ , between classical sets, then  $|X| = |Y|$ . (Every projective permutation matrix is square.)*

### 6.3.3 The direct sum of quantum bijections

Quantum bijections  $A \rightarrow B$  between two quantum sets do not just form a set, but rather a *category*  $\text{QBij}(A, B)$ , whose objects are quantum bijections and whose morphisms are intertwiners. This category behaves much like the category of representations of a finite group.<sup>5</sup> In particular, there is a notion of *direct sum* of quantum bijections.

**Definition 40.** The *direct sum* of quantum bijections  $(H, Q)$  and  $(H', P)$  is defined as  $(H \oplus H', Q \oplus P)$ , where  $Q \oplus P$  is the direct sum of the underlying linear maps:

$$\begin{array}{c} B \\ \swarrow \quad \searrow \\ \textcircled{Q \oplus P} \\ \swarrow \quad \searrow \\ H \oplus H' \quad A \end{array} = \begin{array}{c} B \\ \swarrow \quad \searrow \\ \textcircled{Q} \\ \swarrow \quad \searrow \\ H \quad A \end{array} \oplus \begin{array}{c} B \\ \swarrow \quad \searrow \\ \textcircled{P} \\ \swarrow \quad \searrow \\ H' \quad A \end{array} \quad (6.23)$$

If  $(H, P)$  and  $(H', Q)$  are quantum bijections  $A \rightarrow B$  between classical sets, then the direct sum has underlying Hilbert space  $H \oplus H'$ , and projectors:

$$(P \oplus Q)_{a,b} = P_{a,b} \oplus Q_{a,b} \quad (6.24)$$

---

<sup>5</sup>In fact, we showed that  $\text{QBij}(A, B)$  is the category of representations of a certain  $C^*$ -algebra [76, Sec. 3.4].

**Definition 41.** A quantum bijection  $P$  is *simple* if it cannot be decomposed as direct sum of two nonzero quantum bijections.

*Remark 7.* Every ordinary bijection is a simple quantum bijection, by dimensional considerations. However, not all simple quantum bijections are ordinary bijections, in general.

**Theorem 11** ([76, Thm. 6.4]). *For any pair of quantum sets  $A$  and  $B$ ,  $\text{QBij}(A, B)$  is a semisimple category.*

We do not fully state the definition of semisimplicity here (see [76, Def. 6.19]), but rather draw out its two main consequences for this work.

1. Every quantum bijection decomposes as a finite direct sum of a unique multiset of simple quantum bijections.
2. In the category  $\text{QBij}(A, B)$ , all idempotents split.

*Remark 8.* There are usually an infinite number of simple quantum bijections between two quantum sets.

### 6.3.4 The category $\text{QPerm}(A)$

We now focus in particular on the category  $\text{QPerm}(A) = \text{QBij}(A, A)$  of quantum permutations of a quantum set  $A$ .

We first observe that these categories have already been considered in finite non-commutative topology. Indeed, Wang introduced ‘quantum symmetry groups of finite spaces’ [100] as non-commutative versions of the symmetric groups  $S_n$ .

**Proposition 27** ([76, Prop. 4.12]). *For a quantum set  $B$ ,  $\text{QPerm}(B)$  is the category of finite-dimensional representations of Wang’s ‘quantum permutation group’ algebra  $A_{\text{aut}}(B)$ .*

The categories  $\text{QPerm}(A)$  are monoidal categories, where monoidal product is composition. As discussed in Section 6.3.3, they also have a direct sum and are semisimple.

**Definition 42.** The *classical subcategory* of  $\text{QPerm}(A)$  is the full semisimple monoidal subcategory of quantum permutations decomposing as a direct sum of ordinary permutations.

A quantum permutation  $(H, P) : A \rightarrow A$  in the classical subcategory has the following form. Here  $\{|i\rangle\}$  is an orthonormal basis decomposing the Hilbert space  $H$  into one-dimensional subspaces  $H \cong \bigoplus_i \mathbb{C} |i\rangle$ , and  $f_i : \Gamma \rightarrow \Gamma$  are ordinary permutations:

$$\begin{array}{c}
 \begin{array}{c}
 \text{V}_\Gamma \quad \text{H} \\
 \swarrow \quad \searrow \\
 \text{P} \\
 \swarrow \quad \searrow \\
 \text{H} \quad \text{V}_\Gamma
 \end{array}
 = \sum_i \begin{array}{c}
 \text{H} \quad \uparrow \\
 \swarrow \quad \searrow \\
 \text{f}_i \\
 \swarrow \quad \searrow \\
 \uparrow \quad \text{H}
 \end{array}
 \end{array}
 \tag{6.25}$$

A quantum permutation of a classical set is in the classical subcategory if and only if all projectors in its PPM are commuting [77, Prop. 6.9].

The classical subcategory has a very convenient description. For a finite group  $G$ , let  $\mathbf{Hilb}_G$  denote the category of finite-dimensional  $G$ -graded Hilbert spaces. The objects of this category are finite-dimensional Hilbert spaces  $H$ , with a Hilbert space decomposition  $H = \bigoplus_{g \in G} H_g$ . The morphisms are grading-preserving linear maps. This is a semisimple monoidal dagger category: the dagger is the Hilbert space adjoint of a graded linear map, and the monoidal product is defined as follows:

$$(H \otimes H')_g := \sum_{a,b \in G, ab=g} H_a \otimes H'_b
 \tag{6.26}$$

The simple objects in this category are one-dimensional  $G$ -graded Hilbert spaces. As a category,  $\mathbf{Hilb}_G$  is generated by the elements of the group  $G$  — which correspond to isomorphism classes of one-dimensional  $G$ -graded Hilbert spaces. Tensor product is induced by group multiplication.

**Proposition 28.** *Let  $A$  be a quantum set. The classical subcategory of  $\mathbf{QPerm}(A)$  is equivalent to  $\mathbf{Hilb}_{\text{Perm}(A)}$ .*

*Proof.* The classical subcategory is a semisimple monoidal dagger category generated from the ordinary permutations of the quantum set  $A$ . There is an obvious monoidal dagger equivalence, which takes a permutation  $g \in \text{Perm}(A)$  to the one-dimensional Hilbert space with grading  $g$ .  $\square$

There is in particular a full inclusion  $\mathbf{Hilb}_{\text{Perm}(A)} \subseteq \mathbf{QPerm}(A)$ . In general (for classical sets of dimension greater than or equal to four [100], for instance) the inclusion is strict; there will be simple quantum permutations which are *not* one-dimensional.



### 6.3.5 Splitting in $\mathbf{QPerm}(A)$

Theorem 9 implies that every quantum bijection into  $A$  gives rise to a Frobenius monoid in  $\mathbf{QPerm}(A)$ .

**Proposition 29.** *A quantum bijection  $(H, P) : B \rightarrow A$  gives rise to a special dagger Frobenius monoid in  $\mathbf{QPerm}(A)$ . The underlying object of this algebra is the composition  $(H \otimes H^*, P \circ \bar{P})$ , and the underlying algebra structure is the endomorphism algebra (6.13):*

(6.27)

*Proof.* This follows from the fact that the structural morphisms of the endomorphism algebra (6.13) are intertwiners for  $P \circ \bar{P}$ ; this is immediate from (6.19) and (6.20).  $\square$

We abstract the relevant property of these monoids.

**Definition 43.** Let  $B$  be a quantum set. A *simple dagger Frobenius monoid* in  $\mathbf{QPerm}(B)$  is a special dagger Frobenius monoid  $(H, P)$  whose underlying dagger Frobenius algebra in  $\mathbf{Hilb}^6$  is  $*$ -isomorphic to an endomorphism algebra (6.13).

The main result of [77] is that the converse is also true: simple dagger Frobenius monoids in  $\mathbf{QPerm}(A)$  can be *split* to obtain quantum bijections  $(H, P) : B \rightarrow A$ .

**Theorem 12** ([77, Thm. 3.4]). *Let  $A$  be a quantum set and let  $X$  be a simple dagger Frobenius monoid in  $\mathbf{QPerm}(A)$ . Then there exists a quantum set  $B$  and a quantum bijection  $(H, P) : B \rightarrow A$  such that  $X$  is  $*$ -isomorphic to  $(H \otimes H^*, P \circ \bar{P})$ .*

We sketch how the quantum set  $B$  and the quantum bijection  $B \rightarrow A$  are defined from  $X$ . Firstly,  $X$  is a quantum bijection  $(H \otimes H^*, X) : A \rightarrow A$ . The endomorphism algebra (6.13) is an intertwiner for this algebra. This makes the following linear map  $x \in \text{End}(H^* \otimes A \otimes H)$  a dagger idempotent (i.e. self-adjoint and fulfilling  $x^2 = x$ ):

(6.28)

---

<sup>6</sup>This is formally defined by the forgetful functor  $F : \mathbf{QPerm}(B) \rightarrow \mathbf{Hilb}$ , which takes a quantum bijection  $(H, P)$  to the Hilbert space  $H$  and an intertwiner to the underlying linear map.

Here  $n = \dim(H)$  is the dimension of the Hilbert space  $H$ . By splitting the idempotent, we obtain a new Hilbert space  $B$  and an isometry  $i : B \rightarrow H^* \otimes V_\Gamma \otimes H$ . This gives a map  $P : H \otimes B \rightarrow A \otimes H$  by bending wires. It follows that  $X$  is of the form (6.27).

To define the structure of a quantum set on  $B$ , we use the following shorthand notation:

Now we define an algebra structure on  $B$  (depicted as grey nodes) using the algebra structure on  $A$  (depicted as white nodes):

We show in [77] that  $B$  is a quantum set, and  $(H, P)$  is a quantum bijection  $B \rightarrow A$ .

### 6.3.6 Classification of quantum bijections

Simple dagger Frobenius algebras in  $\text{QPerm}(A)$  can be split to produce quantum bijections  $(H, P) : B \rightarrow A$  from some quantum set  $B$ . Likewise, a quantum bijection  $(H, P) : B \rightarrow A$  gives rise to a simple dagger Frobenius algebra  $P \circ \bar{P}$  in  $\text{QPerm}(A)$ . This yields a correspondence between *equivalence classes* of quantum bijections  $B \rightarrow A$  and *\*-isomorphism classes* of simple dagger Frobenius algebras in  $\text{QPerm}(A)$ .

**Definition 44.** We say that quantum bijections  $(H, P) : B \rightarrow A$  and  $(H', P') : B' \rightarrow A$  are *equivalent* when there is an ordinary bijection  $\epsilon : B \rightarrow B'$  and a unitary map  $U : H \rightarrow H'$  satisfying the following equation:

For quantum bijections between classical sets, this comes down to the following condition on projective permutation matrices.

**Corollary 4.** *Two projective permutation matrices  $\{P_{x,y}\}_{x \in [m], y \in [n]}$  and  $\{P'_{x',y}\}_{x' \in [m'], y \in [n]}$  on Hilbert spaces  $H$  and  $H'$  are equivalent quantum bijections if there is an ordinary bijection  $\epsilon : [m] \rightarrow [m']$  and a unitary  $U : H \rightarrow H'$  such that*

$$P_{x,y} = U^\dagger P'_{\epsilon(x),y} U$$

for all  $y \in [n]$  and  $x \in [m]$ .

**Theorem 13** ([77, Rem. 3.9]). *Let  $A$  be a quantum set. Proposition 29 and Theorem 12 induce a bijection between the following sets:*

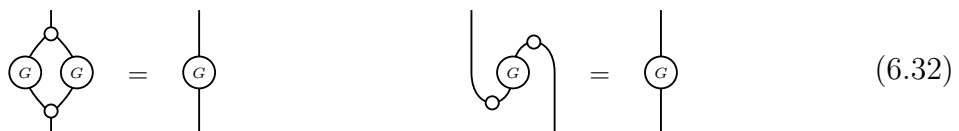
- Quantum bijections  $B \rightarrow A$  up to the equivalence relation (6.31).
- $*$ -isomorphism classes of simple dagger Frobenius monoids in  $\text{QBij}(A, A)$ .

## 6.4 Quantum graph theory

Finally, we show how (quantum) graphs and their isomorphisms can be brought into our compositional framework.

### 6.4.1 Quantum graphs

**Definition 45.** A *quantum graph* is a pair  $(A, \Gamma)$  of a quantum set  $A$  and a self-adjoint linear map  $\Gamma : A \rightarrow A$  (the *quantum adjacency matrix*) satisfying the following equations:



$$\begin{array}{c} \text{Diamond with } G \text{ nodes} \\ \text{Loop on } G \text{ node} \end{array} = \begin{array}{c} G \\ G \end{array} \quad (6.32)$$

For a classical set  $A = V_\Gamma$ , this reduces to the definition of an adjacency matrix  $\{\Gamma_{v,w}\}_{v,w \in V_\Gamma}$ ; from left to right, the conditions state that  $\Gamma_{v,w}^2 = \Gamma_{v,w}$  and  $\Gamma_{v,w} = \Gamma_{w,v}$ .

A quantum graph is *reflexive* or *irreflexive* if one of the following additional equations holds:



$$\begin{array}{c} \text{Loop on } G \text{ (reflexivity)} \\ \text{Loop on } G \text{ (irreflexivity)} \end{array} = \begin{array}{c} \text{Line} \\ 0 \end{array}$$

For classical graphs this corresponds to  $\Gamma_{v,v} = 1$  or  $\Gamma_{v,v} = 0$ , respectively. For a classical set, the definition of an irreflexive quantum graph therefore reduces to the standard definition of an adjacency matrix of a simple graph.

*Remark 9.* There are many related definitions of noncommutative or quantum graphs in the literature [36, 60, 101, 102]. These have applications in quantum error correction [102] and zero-error communication [36]. In [76, Sec.7], we show how our quantum graphs correspond to these previous definitions. In particular:

- Our reflexive quantum graphs coincide with Weaver’s finite-dimensional quantum graphs [102], defined in terms of symmetric and reflexive quantum relations [60, 101].
- Our reflexive quantum graphs  $(\text{Mat}_n, G)$  on matrix algebras coincide with Duan, Severini and Winter’s noncommutative graphs [36].

## 6.4.2 Quantum graph isomorphisms

**Definition 46.** An *isomorphism* of quantum graphs  $\Gamma$  and  $\Gamma'$  is an ordinary bijection of quantum sets  $f : V_\Gamma \rightarrow V_{\Gamma'}$  intertwining the quantum adjacency matrices (i.e.  $f\Gamma = \Gamma'f$ ). We denote the group of automorphisms of a quantum graph  $\Gamma$  by  $\text{Aut}(\Gamma)$ .

For classical graphs, this coincides with the usual notion of graph isomorphism, and the group  $\text{Aut}(\Gamma)$  is the usual automorphism group. We quantise this definition to obtain a notion of quantum graph isomorphism.

**Definition 47.** Let  $(A, \Gamma)$  and  $(A', \Gamma')$  be quantum graphs. A *quantum isomorphism*  $(H, P) : (A, \Gamma) \rightarrow (A', \Gamma')$  is a quantum bijection  $(H, P) : A \rightarrow A'$  fulfilling the following additional equation:

$$(6.33)$$

For quantum isomorphisms between irreflexive classical graphs, in terms of their underlying projective permutation matrix  $\{P_{v,w}\}_{v \in V_\Gamma, w \in V_{\Gamma'}}$  the condition (6.33) becomes:

$$\text{If } (v \sim_\Gamma v' \text{ and } w \not\sim_{\Gamma'} w') \text{ or } (v \not\sim_\Gamma v' \text{ and } w \sim_{\Gamma'} w') \Rightarrow P_{v',w'} P_{v,w} = 0 \quad (6.34)$$

These quantum graph isomorphisms between classical graphs are precisely those considered in the graph isomorphism game considered in the introduction (Definition 29).

**Proposition 30** ([6, Theorem 5.4]). *For classical graphs  $\Gamma$  and  $\Gamma'$ , a perfect quantum strategy for the graph isomorphism game exists if and only if there is a nonzero family of projectors  $\{P_{v,w}\}_{v \in V_\Gamma, w \in V_{\Gamma'}}$  fulfilling equations (6.21), (6.22) and (6.34). Equivalently, a quantum strategy exists if and only if there is a nonzero quantum isomorphism  $(H, P) : (V_\Gamma, \Gamma) \rightarrow (V_{\Gamma'}, \Gamma')$ .*

The categories of quantum graph isomorphisms  $\text{QGraphIso}((A, \Gamma), (A', \Gamma'))$  are also semisimple (recall Section 6.3.3), with the direct sum of the underlying quantum bijections. A quantum graph isomorphism is simple precisely when its underlying quantum bijection is.

**Proposition 31** ([76, Prop. 6.13]). *A quantum graph isomorphism  $Q : (A, \Gamma) \rightarrow (A', \Gamma')$  is simple if and only if its underlying quantum bijection  $Q : A \rightarrow A'$  is simple. Moreover, let  $Q : (A, \Gamma) \rightarrow (A', \Gamma')$  be a quantum isomorphism whose underlying quantum bijection has a decomposition  $Q \cong \bigoplus_i f_i$ , where  $f_i$  are simple quantum bijections. Then each  $f_i$  is a quantum isomorphism  $(A, \Gamma) \rightarrow (A, \Gamma')$ .*

# Chapter 7

## A group-theoretical construction of quantum pseudo-telepathy

### 7.1 Introduction

#### 7.1.1 Overview

In the last chapter we saw that *quantum bijections* between classical sets  $A \rightarrow A'$  are precisely projective permutation matrices (PPMs). These are quantum strategies for two-player nonlocal games such as the graph isomorphism game, where  $A$  is the set of inputs received from the verifier and  $A'$  the set of outputs returned.

In Section 6.3.6 we gave a classification of quantum bijections: for any quantum set  $A$ , equivalence classes of quantum bijections  $A \rightarrow A'$ , where  $A'$  is any other quantum set, correspond to simple dagger Frobenius monoids in the category  $\text{QPerm}(A)$  of quantum elements of the quantum permutation group of  $A$ . This implies a classification of projective permutation matrices in the case where  $A$  is classical, provided that we impose an additional classicality condition on the monoids in order that  $A'$  also be classical (Theorem 19). This classification is constructive — given the monoid, we can build the PPM.

Unfortunately, there is no good understanding of all simple dagger Frobenius monoids in the categories  $\text{QPerm}(A)$ , even when  $A$  is classical. However, we know that  $\text{QPerm}(A)$  always contains a subcategory generated by the elements of the ordinary permutation group  $\text{Perm}(A)$ ; in the case where  $A$  is a classical set with  $n$  elements, these are just the elements of  $S_n$ . In this chapter, we restrict our consideration to the simple dagger Frobenius monoids in this subcategory, thereby obtaining a group-theoretical construction of projective permutation matrices. We then con-

sider how these quantum strategies can be used to exhibit pseudo-telepathy in the graph isomorphism and linear constraint system games.

### 7.1.2 Summary

**Technical background.** In this group-theoretical setting, the mathematics mostly comes down to projective representation theory. We review all the necessary technical material in Section 7.2.

**Simple dagger Frobenius algebras from ordinary permutations.** Our first main result (Theorem 18) is a classification of all  $*$ -isomorphism classes of simple dagger Frobenius monoids in the category of ordinary permutations of a quantum set  $A$ . To do this, we observe that this category is isomorphic to the category of  $\text{Perm}(A)$ -graded vector spaces. The simple dagger Frobenius monoids in this category are just graded matrix algebras, and so we can use the classification of Bahturin and Zaicev (Theorem 17), which shows that the interesting graded matrix algebras come from subgroups of  $\text{Perm}(A)$  of *central type*. Our group-theoretical construction of a PPM  $A \rightarrow A'$  from a classical set  $A$  is therefore based on a faithful action of a group of central type on the set  $A$ . The condition ensuring that the quantum bijective set  $A'$  is also classical is that all point stabilisers under the action must be *coisotropic* (Definition 58), a property of certain subgroups of central type groups.

**PPMs from central type groups, and composition.** In the case where  $A$  is a classical set, and the classicality condition on the monoid is obeyed, we obtain a PPM. We give an explicit construction of this PPM in terms of the action of the group of central type on the set  $A$  (Theorem 20). This construction makes use of induction and restriction of representations, generalising the usual construction of contextual measurement scenarios from eigenspaces of abelian subgroups of a group of operators (c.f. Lemma 21).

Given quantum bijections  $A \rightarrow A'$  and  $A' \rightarrow A''$ , we can compose them to obtain a quantum bijection  $A \rightarrow A''$ . In Proposition 44 we show that composition of quantum bijections (e.g. PPMs) corresponds to tensor product of the corresponding simple dagger Frobenius monoids (e.g. Cartesian product of central type groups). We observe in particular that the usual quantum strategy for the Mermin-Peres magic square game factors through quantum bijections to and from an intermediate quantum set (Example 12).

**The graph isomorphism game.** Having obtained a group-theoretical construction of projective permutation matrices, we now apply these to pseudo-telepathy in the graph isomorphism game. Given a graph  $\Gamma$  on  $A$ , a given PPM from  $A \rightarrow A'$  wins the graph isomorphism game  $(\Gamma, \Gamma')$  for at most one graph  $\Gamma'$  on  $A'$ . We identify a necessary and sufficient condition for such a graph  $\Gamma'$  to exist (Proposition 45), and give an explicit construction of  $\Gamma'$  when the PPM is obtained from the group-theoretical construction (Proposition 47). This construction simplifies considerably in the case where the stabiliser subgroups for the action of the central type group are normal (Proposition 6).

For pseudo-telepathy, we require that the graph isomorphism game for  $(\Gamma, \Gamma')$  has no perfect classical strategy. To rule out PPMs, we obtain a condition on a group-theoretical PPM which means that the PPM is possible to simulate classically (Proposition 48).

**Linear constraint system games.** Finally, we consider linear constraint system games. Most if not all examples of perfect quantum strategies exhibiting quantum pseudo-telepathy are for games of this type. It is already known that the graph isomorphism game generalises linear constraint system games, in the sense that classical and quantum strategies for a linear constraint system game correspond precisely to classical and quantum isomorphisms between two graphs.

In Proposition 50 we show that each PPM obtained from a central type group acting faithfully on a graph produces a solution to a certain linear constraint system; the variables are elements of the *orthogonal complements* of the stabiliser groups (Definition 57), and the constants for each equation are given by the 2-cocycle associated to the central type group.

It is then natural to ask which quantum solutions to linear constraint systems can be obtained from a central type group acting on a set in this way. One way to obtain a quantum solution to a linear constraint system is as a representation of the abelianisation of the solution group (Definition 72). We show that if we remove the classical redundancy from a solution obtained in this way, we arrive precisely at a projective representation of a central type group. Our central type group construction therefore in some sense captures the ‘truly quantum’ part of quantum solutions to a linear constraint system factoring through the abelianisation of the solution group; we make this precise in Proposition 54.



## 7.2 Technical background

### 7.2.1 Groups of central type

We will use various results about *groups of central type* and their projective representation theory.

**Definition 48.** Let  $L$  be a group. A function  $\psi : L \times L \rightarrow U(1)$  is a *2-cocycle* precisely when, for all  $a, b, c \in L$ ,

$$\psi(a, b)\psi(ab, c) = \psi(a, bc)\psi(b, c). \quad (7.1)$$

All the 2-cocycles we consider in this work take values in  $U(1)$ . To a 2-cocycle we associate a *form*  $\rho : L \times L \rightarrow U(1)$ , defined by

$$\rho(a, b) = \psi(a, b)\psi(aba^{-1}, a)^*. \quad (7.2)$$

**Definition 49.** For a group  $L$  and a 2-cocycle  $\psi$ , the *twisted group algebra*  $\mathbb{C}L^\psi$  is an associative unital algebra with generators  $\{\bar{a} \mid a \in L\}$  and multiplication

$$\bar{a}_1 \bar{a}_2 = \psi(a_1, a_2)\overline{a_1 a_2}.$$

(Here an overline is used to distinguish a generator  $\bar{a}$  of the twisted group algebra from the corresponding element  $a$  of the group  $L$ .)

*Remark 10.* Up to  $*$ -isomorphism of twisted group algebras, we can assume without loss of generality that  $\psi(e, h) = 1 = \psi(h, e)$  and therefore  $\bar{e} = \mathbb{1}_H$ , and that  $\psi(h, h^{-1}) = 1$  and therefore  $\bar{h}^\dagger = \bar{h}^{-1}$ .

**Definition 50** ([41, Definition 7.12.21]). A group  $L$  is *of central type* if it possesses a 2-cocycle  $\psi : L \times L \rightarrow U(1)$  such that either of the following equivalent conditions hold:

1. The associated form  $\rho$  is nondegenerate, that is,

$$\rho(a, x) = 1 \text{ for all } x \in Z_L(a) \implies a = e.$$

2. The twisted group algebra  $\mathbb{C}L^\psi$  is simple.

Simplicity of  $\mathbb{C}L^\psi$  implies that it has precisely one irreducible module, of dimension  $d := \sqrt{|L|}$ , and moreover that there is a  $*$ -isomorphism  $\mathbb{C}L^\psi \simeq M_d(\mathbb{C})$ . The matrices in the image of such an isomorphism have been considered before in quantum information theory.

**Definition 51.** The unitary matrices in the image of the isomorphism  $\mathbb{C}L^\psi \rightarrow M_d(\mathbb{C})$  are called a *nice unitary error basis* of dimension  $d$ . The group  $L$  is called the *index group* of the nice UEB.

**Proposition 32** ([57]). *The matrices of a nice unitary error basis satisfy the following condition for all  $a, b \in L$ :*

$$\mathrm{Tr}(U_a^\dagger U_b) = \dim(H) \delta_{a,b} \qquad U_a U_b = \psi(a, b) U_{ab} \qquad (7.3)$$

**Definition 52.** Because the 2-cocycle condition (7.1) implies that the phase associated to a product of more than two elements is unaffected by the bracketing of the product, we write it as  $\psi(g_1, \dots, g_n)$ .

**Lemma 11.** *Let  $(L_1, \psi_1)$  and  $(L_2, \psi_2)$  be groups of central type. Then  $(L_1 \times L_2, \psi_1 \psi_2)$  is also of central type.*

Abelian groups  $(\mathbb{Z}_p)^{(2n)}$  for  $p$  prime can be considered as vector spaces over  $\mathbb{Z}_p$ ; a nondegenerate 2-cocycle  $\psi$  is then precisely a symplectic form on the vector space  $(\mathbb{Z}_p)^{(2n)}$ .

**Proposition 33** ([11, Theorem 5]). *Abelian groups of central type are all direct products of symplectic vector spaces  $(\mathbb{Z}_p)^{(2n)}$ .*

Nonabelian groups of central type are much harder to classify. For order 121 or less, they are listed at [58].

## 7.2.2 Projective representation theory

We recall definitions and theorems from projective representation theory.

**Definition 53.** A *projective representation* of a finite group  $L$  with 2-cocycle  $\psi$  is a module over the twisted group algebra  $\mathbb{C}L^\psi$ .

The category of  $\mathbb{C}L^\psi$ -modules  $\mathbf{Mod}(\mathbb{C}L^\psi)$  is semisimple; it has a finite set of simple objects, and every object can be decomposed uniquely as a direct sum of these. We call the simple objects of this category irreducible projective representations ( $\psi$ -i.p.r.'s) of  $L$ .

**Definition 54.** Let  $V$  be a  $\mathbb{C}L^\psi$ -module, and let  $X$  be an irreducible  $\mathbb{C}L^\psi$ -module. We define the *multiplicity* of  $X$  in  $V$  to be the number of times  $X$  appears in the decomposition of  $V$  into irreducibles.

There is an obvious restriction functor  $\text{Res}_H^L : \mathbf{Mod}(\mathbb{C}L^\psi) \rightarrow \mathbf{Mod}(\mathbb{C}H^\psi)$ , where the cocycle  $\psi$  is restricted in the obvious way; for a  $\mathbb{C}L^\psi$ -module  $V$ , we write  $V_H$  for  $\text{Res}_H^L(V)$ . Likewise, there is an induction functor  $\text{Ind}_H^L : \mathbf{Mod}(\mathbb{C}H^\psi) \rightarrow \mathbf{Mod}(\mathbb{C}L^\psi)$ ; for a  $\mathbb{C}H^\psi$ -module  $W$ , we write  $W^L$  for  $\text{Ind}_H^L(W) = \mathbb{C}L^\psi \otimes_{\mathbb{C}H^\psi} W$ . These functors form an adjunction, implying the following theorem.

**Theorem 14** (Frobenius reciprocity, [54, Cor. 5.6.3]). *Let  $H < L$ , and let  $\psi : L \times L \rightarrow U(1)$  be a 2-cocycle. Let  $V$  be a  $\mathbb{C}L^\psi$ -module and let  $W$  be a  $\mathbb{C}H^\psi$ -module. Then the multiplicity of  $V$  in  $W^L$  is equal to the multiplicity of  $W$  in  $V_H$ .*

The notion of *conjugation* of a representation is closely connected to induction. Let  $H < L$ , let  $\psi : L \times L \rightarrow U(1)$  be a 2-cocycle, let  $W$  be a  $\mathbb{C}H^\psi$ -module, and consider the natural embedding of  $W$  as a submodule  $W \subset (W^L)_H$ . It is clear that for any  $g \in L$ ,  $\bar{g}W \subset W^L$  is a  $\mathbb{C}(gHg^{-1})^\psi$ -submodule of  $W$ ; we write this submodule abstractly as  $W^{(g)}$ .  $W^{(g)}$  is irreducible if  $W$  is.

**Definition 55.** We say that two  $H$ -modules  $V_1, V_2$  are *conjugate* if  $V_2 \simeq V_1^{(g)}$  for some  $g \in L$ .

This definition divides the irreducible  $\mathbb{C}H^\psi$  modules into *conjugacy classes*. There are  $|N_L(H)|/|H|$  irreducible modules in each class, where  $N_L(H)$  is the normaliser of  $H$  in  $L$ .

**Lemma 12.** *Let  $W$  be a projective representation of  $H < L$ . Then the set of  $L$ -conjugates of  $W$  is a left  $L$ -set; that is,  $(W^{(g_1)})^{(g_2)} = W^{(g_2g_1)}$ .*

A relation between different restriction functors is given by the following well-known theorem. We first make a definition.

**Definition 56.** Let  $H_i, H_j < L$ . The  $(H_i, H_j)$ -double coset  $H_i x H_j$  of an element  $x \in L$  is a subset of  $L$  defined as follows:

$$H_i x H_j := \{h_i x h_j \mid h_i \in H_i, h_j \in H_j\}$$

The  $(H_i, H_j)$ -double cosets partition  $L$ .

*Remark 11.* For any  $(H_i, H_j)$ -double coset  $X \subset L$ , the subset  $X^{-1} \subset L$  is a  $(H_j, H_i)$ -double coset.

**Theorem 15** (Mackey's subgroup theorem, [54, Theorem 5.7.2]). *Let  $H_i, H_j < L$  and let  $T$  be a set of  $(H_i, H_j)$ -double coset representatives. Let  $W$  be a  $\mathbb{C}H_i^\psi$ -module. For  $t \in T$ , let  $W_t := (W^{(t)})_{tH_i t^{-1} \cap H_j}$ . Then, as  $\mathbb{C}H_j^\psi$ -modules:*

$$(W^L)_{H_j} \cong \bigoplus_{t \in T} (W_t)^{H_j}$$

Finally, as is well-known, projective representations are ordinary representations of a central extension of the group. We now recall how one can switch between these two perspectives.

**From ordinary representations to projective representations.** Let  $C < Z(L)$  be a central subgroup of  $L$ . Pick coset representatives  $\{v_x \mid x \in L\}$  for  $L' := L/C$ . Then we have

$$v_x v_y = a(x, y) v_{xy}$$

for all  $v_x, v_y$ , for some function  $a : L \times L \rightarrow C$ . Let  $\pi : \mathbb{C}L \rightarrow GL_n(\mathbb{C})$  be an ordinary representation. Because  $C$  is central, we have that  $\pi(a(x, y)) = \alpha(x, y)\mathbb{1}$  for some  $\alpha(x, y) \in U(1)$ .

**Proposition 34** ([31, Definition 11]). *The map*

$$\begin{aligned} \tilde{\pi} : \mathbb{C}L' &\rightarrow GL_n(\mathbb{C}) \\ \bar{x} &\mapsto \pi(v_x) \end{aligned}$$

*defines a projective representation of  $L'$  with 2-cocycle  $\alpha : G \times G \rightarrow U(1)$ .*

**From projective representations to ordinary representations.** Let  $\pi : \mathbb{C}L^\psi \rightarrow GL_n(\mathbb{C})$  be a projective representation of  $L$  with cocycle  $\psi$ . We assume that the image of  $L \times L$  under  $\psi$ ,  $\text{Im}(\psi) < U(1)$ , is finite. We define a new group  $L^+ = L \times \text{Im}(\psi)$ , with multiplication

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2 \psi(a_1, a_2)).$$

The projective representation  $\pi$  becomes an ordinary representation  $\pi^+$  of this group:

$$\begin{aligned} \pi^+ : \mathbb{C}L^+ &\rightarrow GL_n(\mathbb{C}) \\ (x, a) &\mapsto a\pi(x) \end{aligned}$$

### 7.2.3 Representations of groups of central type

Observing that the form  $\rho_\psi$  associated to a 2-cocycle  $\psi : L \times L \rightarrow U(1)$  satisfies

$$\rho(a, b) = \rho(b, a)^* \quad \text{for all } b \in Z_L(a),$$

we think of it as an alternating form on the group. From this perspective, the non-degenerate 2-cocycle of a group of central type induces a nondegenerate alternating form on  $L$ .

**Proposition 35** ([41, Exercise 7.12.22.v]). *Let  $(L, \psi)$  be a group of central type and let  $x \in L$ . Then  $\rho_\psi(x, -)|_{Z_L(x)} : Z_x \rightarrow U(1)$  is a multiplicative character of the centralizer  $Z_x$ , and  $\rho_\psi(x, -)|_{Z_L(x)}$  is non-trivial for every  $x \neq e_L$ , that is:*

$$\rho_\psi(x, a) = 1 \quad \forall a \in Z_L(x) \quad \Rightarrow \quad x = e_L \quad (7.4)$$

Following [16], we define various notions based on this analogy.

**Definition 57.** Let  $H$  be a group, let  $\psi$  be a 2-cocycle on  $H$ , and let  $S \subseteq H$  be a subset. The *orthogonal complement*  $S^\perp$  of  $S$  is the following subset of  $H$ :

$$S^\perp := \{g \in H \mid \rho_\psi(g, a) = 1 \quad \forall a \in Z_H(g) \cap S\} \quad (7.5)$$

**Definition 58.** We say that a subset  $S$  is *isotropic* if  $S \subseteq S^\perp$ , and *coisotropic* if  $S^\perp \subseteq S$ .

**Lemma 13.** *Let  $H$  be a group and  $\psi$  a 2-cocycle on  $H$ . Then  $H^\perp$  is preserved under inner automorphisms of  $H$ .*

In other words,  $H^\perp$  is a union of conjugacy classes. The following result is well-known.

**Proposition 36** ([54, Sec. 7.3]). *Let  $H$  be a group with 2-cocycle  $\psi$ . The number of  $\psi$ -i.p.r.'s of  $H$  is equal to the number of conjugacy classes in  $H^\perp$ .*

Central type subgroups  $(L, \psi)$  are an example, since  $L^\perp$  is trivial by Proposition 35; they therefore have only one  $\psi$ -i.p.r. Their representation theory is also well-behaved under restriction.

**Proposition 37.** *Let  $H < L$  be a subgroup of a group  $(L, \psi)$  of central type. The number of irreducible  $\mathbb{C}H^\psi$ -modules is  $\leq |L|/|H|$ , with equality iff  $H$  is coisotropic.*

*Proof.* We show in [77, Proposition 4.12] that

$$\sum_{a \in H^\perp \cap H} |Z_H(a)| \leq |L|$$

with equality iff  $L$  is coisotropic. Recalling Lemma 13, let  $\{b\}$  be a set of representatives for the  $H$ -conjugacy classes in  $H^\perp \cap H$ , and let  $C_b$  be those conjugacy classes. We have

$$\sum_{a \in H^\perp \cap H} |Z_H(a)| = \sum_b |Z_H(b)| |C_b| = |\#\text{ conjugacy classes in } H \cap H^\perp| |H|$$

where the last equality is by the orbit-stabiliser theorem, implying that

$$|\#\text{ conjugacy classes in } H \cap H^\perp| \leq \frac{|L|}{|H|}$$

with equality iff  $H$  is coisotropic. The result follows by Proposition 36.  $\square$

**Theorem 16.** *Let  $L$  be a group of central type, and let  $V$  be the unique irreducible  $\mathbb{C}L^\psi$ -module, of dimension  $\sqrt{|L|}$ . Let  $H < L$  be a coisotropic subgroup and let  $\{W_i \mid 1 \leq i \leq |L|/|H|\}$  be the set of irreducible  $\mathbb{C}H^\psi$ -modules. Then*

$$V_H \cong \bigoplus_i W_i. \quad (7.6)$$

where the orthogonal decomposition is unique.

*Proof.* Let  $n_i$  be the multiplicity of  $W_i$  in  $V_H$  and  $d_i$  be the dimension of  $W_i$ . Since  $V$  is the only irreducible module of  $\mathbb{C}L^\psi$ , we know that  $(W_i)^L$  must be some multiple of  $V$ ; by Frobenius reciprocity (Theorem 14), this multiple will be precisely  $n_i \geq 1$ . Considering the dimension of the induced representation, we have the following equation:

$$\frac{|L|}{|H|} d_i = n_i \sqrt{|L|} \quad (7.7)$$

On the other hand, decomposing  $V_H$  into irreducible modules and taking dimensions, we obtain:

$$\sum_i n_i d_i = \sqrt{|L|}$$

Substituting in (7.7):

$$\begin{aligned} \sum_i n_i d_i = \sqrt{|L|} &\Leftrightarrow \sum_i (n_i)^2 \frac{|H|}{\sqrt{|L|}} = \sqrt{|L|} \\ &\Leftrightarrow \sum_i (n_i)^2 = \frac{|L|}{|H|}. \end{aligned}$$

By Proposition 37 there are  $|G|/|H|$   $\alpha$ -i.p.r.'s, each of which must appear at least once in the sum; this implies that  $n_i = 1$  for all  $i$ . Since no irreducible module has multiplicity greater than one, the decomposition is unique.  $\square$

We immediately obtain the following corollary by Frobenius reciprocity.

**Corollary 5.** *For all  $W_i$  we have that  $(W_i)^L \cong V$ ; moreover, all the  $W_i$  have the same dimension  $\frac{|\omega||H|}{|L|}$ .*

Let  $\{g_j \mid 1 \leq j \leq |L|/|H|\}$  be left coset representatives for  $H$  in  $L$ . Since  $(W_i)^L \cong V$ , by the discussion following Theorem 14 we obtain an orthogonal decomposition of  $W$  for each  $i$ :

$$V = \bigoplus_j \overline{g_j} W_i \cong \bigoplus_j (W_i)^{(g_j)} \quad (7.8)$$

For non-normal  $H$  this is different to the decomposition (7.6), since  $\overline{g_j} W_i \cong (W_i)^{(g_j)}$  is a  $\mathbb{C}(g_j H (g_j)^{-1})^\psi$ -module, which is not a  $\mathbb{C}H^\psi$ -module unless  $g_j \in N_L(H)$ .

## 7.2.4 Graphs with symmetry

In this final background section we review the theory of graphs with group symmetries. The fact that double cosets appear here as well as in projective representation theory (Theorem 15) will be crucial in our splitting of simple dagger Frobenius algebras to obtain quantum bijections of classical sets.

Let  $V_\Gamma$  be a vertex set, and let  $L < S_{|V_\Gamma|}$ . Let  $n$  be the number of orbits under the action of  $L$ , and let  $\{O_i \subset V_\Gamma \mid 1 \leq i \leq n\}$  be these orbits. For each orbit, pick a vertex  $v_i \in O_i$  and write  $H_i := \text{Stab}(v_i)$ . We thus obtain an isomorphism of  $L$ -sets  $O_i \cong L/H_i$  by the identification  $g \cdot v_i \mapsto \bar{g} \in L/H_i$ .

We now consider the possible graph structures  $\Gamma$  on  $V_\Gamma$  for which  $L < \text{Aut}(\Gamma)$ . Edges between orbits  $O_i$  and  $O_j$  correspond to elements of  $L/H_i \times L/H_j$ . The action of  $L$  partitions  $L/H_i \times L/H_j$  into orbits. It is clear that if one edge in an orbit is connected, all others in that orbit must be if  $L$  is to be a group of symmetries of the graph. We now characterise these orbits, and use this characterisation to give a compact description of an  $L$ -symmetric graph.

**Lemma 14.** *The set of  $L$ -orbits in  $L/H_i \times L/H_j$  is in bijection with the set of  $(H_i, H_j)$ -double cosets.*

*Proof.* Let  $(g_i \cdot v_i, g_j \cdot v_j)$  be an edge. Acting by  $g_i^{-1} \in L$ , we obtain an edge  $(v_i, (g_i^{-1} g_j) \cdot v_j)$  in the same orbit. Since  $H_i, H_j$  stabilise  $v_i, v_j$  respectively,  $(v_i, g \cdot v_j)$  is in the same orbit as  $(v_i, g_i^{-1} g_j \cdot v_j)$  precisely when  $g \in H_i g_i^{-1} g_j H_j$ .  $\square$

**Proposition 38.** *Let  $V_\Gamma, L, \{O_i\}, \{v_i\}$  and  $\{H_i\}$  be as above. Let  $\mathcal{H}_{ij}$  be the set of  $(H_i, H_j)$ -double cosets. A graph  $\Gamma$  with vertex  $V_\Gamma$  and symmetry  $L < \text{Aut}(\Gamma)$  corresponds to a set of functions*

$$\epsilon_{ij} : \mathcal{H}_{ij} \rightarrow \{0, 1\} \quad \text{for all } i, j \in I$$

satisfying

$$\epsilon_{ij}(X) = \epsilon_{ji}(X^{-1}) \quad (7.9)$$

where  $X^{-1}$  is the inverse double coset.

*Proof.* Given this data, one constructs the graph by the rule

$$v_i \sim x \cdot v_j \quad \text{iff} \quad \epsilon_{ij}(H_i x H_j) = 1$$

All other edges are obtained by symmetry:

$$g_i \cdot v_i \sim g_j \cdot v_j \quad \text{iff} \quad v_i \sim (g_i^{-1} g_j) \cdot v_j$$

The inverse double coset condition ensures that the edge relation is symmetric.  $\square$

## 7.3 Quantum bijections from classical symmetries

The  $*$ -isomorphism classes of simple dagger Frobenius monoids in the categories  $\mathbf{QPerm}(A)$  are still not characterised in general, even for classical sets of dimension greater than or equal to four. We therefore focus on the classical subcategory  $\mathbf{Hilb}_{\mathbf{Perm}(A)} \subset \mathbf{QAut}(A)$ , which we introduced in Section 6.3.4. We will give a  $*$ -isomorphism classification of the simple dagger Frobenius algebras in this subcategory, explicitly construct the corresponding quantum bijections between classical sets, and apply these to quantum pseudo-telepathy.

Wherever possible, we prove results for general quantum sets and quantum graphs, as these results may be applicable to zero-error quantum communication (see Remark 9).

### 7.3.1 Simple dagger Frobenius algebras in $\mathbf{Hilb}_G$

We will classify all the simple dagger Frobenius algebras in  $\mathbf{Hilb}_G$  up to  $*$ -isomorphism, for any finite group  $G$ . This will give us an up-to-equivalence classification of all the quantum bijections into  $A$  whose associated simple dagger Frobenius algebras lie in the classical subcategory  $\mathbf{Hilb}_{\mathbf{Perm}(A)}$ .

This result is based on a classification of graded matrix algebras by Bahturin and Zaicev [10]. The following result connects our setting with their work.

**Proposition 39.** *Any simple dagger Frobenius algebra in  $\mathbf{Hilb}_{S_n}$  is graded  $*$ -isomorphic to an  $S_n$ -graded matrix algebra with graded inner product.*



*Proof.* There is a full and faithful forgetful functor  $F : \mathbf{Hilb}_{S_n} \rightarrow \mathbf{Hilb}$  which forgets the grading. In this case, by Definition 43, the images of simple dagger Frobenius algebras under this functor are  $*$ -isomorphic to matrix algebras. We can take such a  $*$ -isomorphism and push the grading on the original algebra forward, to obtain a grading compatible with the inner product on the  $*$ -isomorphic matrix algebra.  $\square$

## A classification of graded matrix algebras

Bahturin and Zaicev's classification applies to graded matrix algebras without inner product. We now recall their results before showing that they apply in our dagger setting also.

They showed that any grading on a matrix algebra is induced from two special gradings, called *elementary* and *fine*. In what follows we write  $A_g$  to signify the homogeneous subspace of the algebra  $A$  with grading  $g \in G$ . For a homogeneous element  $v$  we write  $\text{wt}(v) \in G$  for the grading of this element.

The *fine* grading is defined by a group of central type.

**Definition 59** ([10]). Let  $L < G$  be a group of central type, and let  $d = \sqrt{|L|}$ . Then the  $*$ -isomorphism  $\mathbb{C}L^\psi \cong M_d(\mathbb{C})$  determines a *fine* grading on  $M_d(\mathbb{C})$  by the rule

$$(M_d(\mathbb{C}))_g = \text{span}(\bar{g}).$$

All the homogeneous subspaces are one-dimensional, and the algebra has support on gradings  $L < G$ .

We note a useful characterisation of the fine gradings.

**Proposition 40** ([10]). *The fine graded matrix algebras are precisely those whose homogeneous subspaces are one-dimensional.*

The *elementary* gradings are defined as follows.

**Definition 60.** Let  $V$  be a  $G$ -graded vector space of dimension  $d$ , and let  $\{v_i \mid i \in 1, \dots, d\}$  be a homogeneous basis, where  $v_i \in V_{g_i}$ . The tuple  $\mathbf{g} = (g_1, \dots, g_d)$  defines an *elementary grading* on the matrix algebra  $M_d(\mathbb{C})$ , by

$$\text{wt}(E_{ij}) = g_j^{-1}g_i.$$

The fine and elementary gradings can be mixed in the following way.

**Definition 61.** Let  $A$  be a fine  $G$ -graded matrix algebra, and let  $B$  be a  $G$ -graded matrix algebra with elementary grading determined by the tuple  $(g_1, \dots, g_d)$ . Then the *induced grading* on  $A \otimes B$  is defined by

$$\text{wt}(\bar{h} \otimes E_{ij}) = g_j^{-1} h g_i.$$

Bahturin and Zaicev showed that *every* graded matrix algebra is graded isomorphic to one whose grading is induced in this way.

**Theorem 17** ([10, Theorem 5.1]). *Let  $A \cong M_n(\mathbb{C})$  be an  $G$ -graded matrix algebra. Then there exists a decomposition  $n = pq$ , a central type subgroup  $L < G$  of order  $p^2$ , and a tuple  $(g_1, \dots, g_q) \in (G)^q$  such that, as a graded algebra,  $A \cong A_f \otimes A_e$ , where  $A_f$  is the fine graded matrix algebra associated to  $L$  and  $A_e$  is the elementary graded matrix algebra defined by the tuple.*

### Extending the classification to $\mathbf{Hilb}_G$

We now show that there is at most one graded inner product on each matrix algebra, up to graded isomorphism. By Proposition 39, this implies that the above classification holds also for graded matrix algebras with graded inner product; that is, for simple dagger Frobenius algebras in  $\mathbf{Hilb}_G$ .

**Lemma 15.** *Let  $A$  be a graded matrix algebra. There is at most one graded inner product on  $A$ , up to graded isomorphism.*

*Proof.* A graded inner product is nonzero only within homogeneous subspaces of  $A$ . Therefore, graded inner products can only differ within homogeneous subspaces. Two different graded inner products are therefore related by an isomorphism which is nontrivial only within homogeneous subspaces, and which is therefore graded.  $\square$

### Translation into the classical subcategory

We have now classified the simple dagger Frobenius algebras in  $\mathbf{Hilb}_G$  up to  $*$ -isomorphism. In Section 6.3.4, we explained the equivalence between  $\mathbf{Hilb}_{\text{Perm}(A)}$  and the classical subcategory of  $\text{QPerm}(A)$ . We now use this equivalence (6.25) to obtain a diagrammatic expression for those isomorphism classes of simple dagger Frobenius algebras in this subcategory.

**Theorem 18.** *Up to  $*$ -isomorphism, the simple dagger Frobenius algebras in the classical subcategory of  $\mathbf{QPerm}(A)$  are as follows:*

$$\begin{array}{c} \text{Diagram of } X_{L,\psi,\mathbf{g}} \end{array} = \frac{1}{q\sqrt{|L|}} \sum_{\substack{a \in L \subseteq \text{Perm}(A) \\ 1 \leq i, j \leq q}} \begin{array}{c} \text{Diagram of } E_{ij}^\dagger, U_a^\dagger, g_j^{-1}, a, g_i, E_{ij}, U_a \end{array} \quad (7.10)$$

Here  $\{U_a \mid a \in L\}$  is a nice UEB corresponding to the central type group  $(L, \psi) < \text{Perm}(A)$ ;  $E_{ij}$  are the basis elements  $|i\rangle\langle j|$  for the matrix algebra  $M_q(\mathbb{C})$ ; and  $\mathbf{g} = (g_1, \dots, g_q)$  is a tuple of elements of  $\text{Perm}(A)$ .

When  $A$  is a classical set, we can express (7.10) in terms of the matrix of projectors:

$$(X_{L,\psi,\mathbf{g}})_{v,w} = \frac{1}{q\sqrt{|L|}} \sum_{\substack{a \in L \\ 0 \leq i, j \leq q}} \delta_{ag_i(v), g_j(w)} P_{U_a} \otimes P_{E_{ij}} \quad (7.11)$$

Recall that a  $*$ -isomorphism in this picture is a change of basis; every simple dagger Frobenius algebra in  $\mathbf{Hilb}_{S_n} \subset \mathbf{QPerm}([n])$  is therefore, up to a change of basis in the underlying vector space, on a quantum permutation of the form (7.11).

### 7.3.2 Splitting the algebras

In Section 6.3.5, we sketched how every simple dagger Frobenius algebra  $X$  in  $\mathbf{QPerm}(A)$  can be *split* to produce a quantum bijection  $(H, P) : B \rightarrow A$  such that  $X = P \circ \bar{P}$ . We will now give an explicit description of this splitting for simple dagger Frobenius algebras in the classical subcategory. In particular, in the case where  $A = [n]$  is a classical set, we will characterise those algebras for which  $B$  is classical, and give the projective permutation matrix for  $(H, P)$  in this case.

#### Splitting the elementary factor

We first note that it is trivial to split the elementary factor.

**Proposition 41.** *Let  $A$  be a quantum set, and let  $A \cong A_f \otimes A_e$  be a graded matrix algebra in  $\mathbf{Hilb}_{\text{Perm}(A)} \subset \mathbf{QPerm}(A)$ , defined by central type subgroup  $(L, \psi)$  and tuple  $(g_1, \dots, g_q) \in (\text{Perm}(A))^q$ . Let  $(H, P) : B \rightarrow A$  be the splitting of the fine factor; that is,  $P \circ \bar{P} \cong A_f$ . Then the splitting of  $A$  is*

$$\frac{1}{\sqrt{q}} \left( \sum_{i=1}^q (g_i)^{-1} \right) \circ P. \quad (7.12)$$



$(H, P) : B \rightarrow A$  splits  $X_{L,\psi}$  if and only if the following holds, for all  $a \in L$ :

$$(7.15)$$

*Proof.* For *only if*, we begin with the assumption:

$$(7.16)$$

Using the shorthand notation (6.29) for the quantum bijection  $P$ , and (6.19), this is equivalent to the following:

$$(7.16)$$

Contracting the first two bottom wires with  $U_a$  for  $a \in L$  and using (7.3) completes the proof in this direction.

For *if*, note that Proposition 32 implies that the following is an orthonormal basis for  $H \otimes H^*$ :

$$\left\{ \begin{array}{c} \uparrow \\ \downarrow \\ \text{bubble } U_a^\dagger \end{array} : a \in L \right\}$$

Conjugating  $P \circ \bar{P}$  by the elements of this basis, using (7.15) and then removing the bubble shows that each element of the basis is an intertwining projector onto a classical permutation  $a^{-1}$ . The algebra therefore has support on all gradings  $a \in L$ . Because of its dimension, it must therefore be a fine  $L$ -graded matrix algebra.  $\square$

### Fine quantum bijections between classical sets

In this work, we are mostly interested in quantum bijections between classical sets for the purposes of pseudo-telepathy. We therefore specialise to the case where  $A = [n]$ , and where  $B$  is also classical.

**Theorem 19** ([77, Prop. 4.12]). *Let  $(L, \psi) < S_n$  be a central type subgroup, and let  $(H, P) : B \rightarrow [n]$  be the quantum bijection generated from the corresponding algebra. The quantum set  $B$  is classical precisely when the stabiliser  $\text{Stab}(x) < L$  is coisotropic for each  $x \in [n]$ .*

For central type subgroups  $(L, \psi) < S_n$  with coisotropic stabilisers, we now define the set  $B$  and the quantum bijection  $(H, P) : B \rightarrow [n]$  explicitly. In what follows, let  $O_i \subset [n]$  be the  $L$ -orbits, let  $x_i \in O_i$  be chosen elements in each orbit, and let  $H_i = \text{Stab}(x_i)$  the stabilisers of those elements.

**Definition 62.** The classical set  $\overline{[n]}_{L, \psi}$  is the set

$$\bigcup_i \{ \rho \mid \rho \text{ is an irreducible module of } \mathbb{C}H_i^\psi \}.$$

By Proposition 37, this classical set has precisely  $n$  elements. We label the elements of the set  $(\rho, H_i)$ , in order to distinguish the subgroup  $H_i$  of which  $\rho$  is a projective representation. We now define a quantum bijection  $P_{L, \psi} : \overline{[n]}_{L, \psi} \rightarrow [n]$  as follows.

**Definition 63.** Let  $V$  be the unique irreducible module of  $\mathbb{C}L^\psi$ . We define the following matrix of projectors:

$$(P_{L, \psi})_{((\rho, H_i), g \cdot x_j)} = \begin{cases} (\rho)^{(g)} \subset V_{H_i} & i = j \\ 0 & \text{otherwise} \end{cases}$$

Here by  $(\rho)^{(g)} \subset V_{H_i}$  we indicate the projector onto that subspace.

**Proposition 42.** *The matrix of projectors in Definition 63 is a projective permutation matrix satisfying (7.15).*

*Proof.* The rows are orthogonal and complete by (7.8), and the columns are orthogonal and complete by (7.6). Finally, note that the projector onto the subspace  $(\rho)^{(g)} \subset V_{H_i}$  is  $\bar{g}\pi_i\bar{g}^\dagger$ , where  $\pi_i$  is the projector onto  $\rho \subset V_{H_i}$ . It is then immediate that the quantum bijection satisfies (7.15).  $\square$

We summarise the above results in the following theorem.

**Theorem 20.** *Up to equivalence (Definition 44), bijections  $B \rightarrow A$  whose corresponding algebra lies in the classical subcategory of  $\text{QPerm}(A)$  are classified by pairs of a central type subgroup  $(L, \psi) < S_n$  and a tuple  $\mathbf{g} \in (S_n)^q$ .*

*The set  $B$  is classical precisely when  $L$  has coisotropic stabilisers. In this case,  $B = \overline{[n]}_{L, \psi}$  (Definition 62) and the quantum bijection is the projective permutation matrix  $P_{L, \psi} : \overline{[n]}_{L, \psi} \rightarrow [n]$  (Definition 63), followed by a normalised direct sum (7.12) of classical permutations in  $\mathbf{g}$ .*

### Note on irreducibility

It is natural to ask whether the quantum bijections arising from fine graded matrix algebras can be decomposed as a direct sum of other quantum bijections. The answer is as one would hope — they are all irreducible.

**Proposition 43.** *Let  $A$  be a quantum set, and let  $(H, P) : B \rightarrow A$  be a quantum bijection such that  $P \circ \overline{P}$  lies in the classical subcategory. Then if  $P$  decomposes, i.e.  $P = P_1 \oplus P_2$ , then  $P_1 \circ \overline{P_1}$  and  $P_2 \circ \overline{P_2}$  are also algebras in the classical subcategory.*

*Proof.* If  $P = P_1 \oplus P_2$ , then  $P \circ \overline{P} = (P_1 \circ \overline{P_1}) \oplus (P_1 \circ \overline{P_2}) \oplus (P_2 \circ \overline{P_1}) \oplus (P_2 \circ \overline{P_2})$ . Let  $\pi_i : P \rightarrow P_i$  be the projector onto the  $P_i$  factor. Now the horizontal composition  $\pi_i \otimes (\pi_i)^*$  is an intertwining projector  $P \otimes \overline{P} \rightarrow P \otimes \overline{P}$  whose image is  $P_i \otimes \overline{P_i}$ . Since idempotents split in the classical subcategory,  $P_i \otimes \overline{P_i}$  is in the classical subcategory also.  $\square$

**Corollary 7.** *If the quantum bijection  $P_{L,\psi}$  corresponding to a central type subgroup  $(L, \psi) < \text{Perm}(A)$  decomposes as  $P_{L,\psi} = \oplus_i P_i$ , then  $P_i = P_{L_i, \psi_i}$ , where  $L_i < L$  are pairwise commuting central type subgroups.*

*Proof.* By Proposition 43, the subalgebras  $P_i \circ \overline{P_i} \subset P \circ \overline{P}$  are all in the classical subcategory. Since  $P \circ \overline{P}$  has one-dimensional support on each grading, they do too; by Proposition 40, they therefore correspond to central type subgroups  $L_i < L$ . They also commute since they are separate blocks of a matrix algebra, implying that the subgroups  $L_i$  on which they have support must also therefore commute.  $\square$

**Corollary 8.** *A quantum bijection between classical sets corresponding to a central type subgroup  $(L, \psi)$  is irreducible.*

*Proof.* Let the quantum bijection be  $P = \oplus_i P_i$ , where  $P_i$  are irreducible. Then, for each  $i$ ,  $P_i \circ \overline{P_i}$  is a simple dagger Frobenius subalgebra of  $P \circ \overline{P}$  in the classical subcategory. Since the homogeneous spaces of  $P \circ \overline{P}$  are all one-dimensional, those of  $P_i \circ \overline{P_i}$  must be also; by Proposition 40, it therefore corresponds to a central type subgroup, and has support on the identity. But only one of the disjoint  $P_i \circ \overline{P_i}$  can have support on the one-dimensional homogeneous subspace of the identity; there can therefore only be one of them.  $\square$

### 7.3.3 Composition and direct product

In the next section, we will apply these quantum permutations to construct instances of quantum pseudo-telepathy. Beforehand, we observe a compositional interpretation of the direct product of central type subgroups (Lemma 11).

This observation is based on the fact that permutations commuting with every element of a central type subgroup  $L < \text{Perm}(A)$  can be pushed forward along the corresponding quantum bijection.

**Lemma 17.** *Let  $A$  be a quantum set, let  $(L, \psi) < \text{Perm}(A)$  be a central type subgroup, and let  $K < Z_{\text{Perm}(A)}(L)$  be a subgroup of the centraliser of  $L$ . Then  $K \cong K_{L,\psi}$ , where the group  $K_{L,\psi}$  is defined as follows:*

$$K_{L,\psi} := \left\{ \frac{1}{\Delta} \left( \text{bubble}(g) \right) : g \in K \right\} < \text{Perm}(A_{L,\psi}) \quad (7.17)$$

*Proof.* First observe that  $g \in K$  pulls through a double wire:

$$\begin{array}{c} \text{wire} \text{---} g \text{---} \text{wire} \\ \text{wire} \text{---} g \text{---} \text{wire} \end{array} = \sum_{a \in L} \begin{array}{c} \text{wire} \text{---} g \text{---} a \text{---} \text{wire} \\ \text{wire} \text{---} a \text{---} g \text{---} \text{wire} \end{array} = \sum_{a \in L} \begin{array}{c} \text{wire} \text{---} a \text{---} \text{wire} \\ \text{wire} \text{---} g \text{---} \text{wire} \end{array} = \begin{array}{c} \text{wire} \text{---} g \text{---} \text{wire} \\ \text{wire} \text{---} g \text{---} \text{wire} \end{array} \quad (7.18)$$

We use this to show that the elements of the set (7.17) are permutations of  $V_{\Gamma_{L,\psi}}$ . The first equation in (6.16) is proved as follows:

$$\begin{array}{c} \frac{1}{\sqrt{L}} \left( \text{wire} \text{---} \text{dot} \text{---} \text{bubble}(g) \right) \\ \text{---} \text{dot} \end{array} \stackrel{(6.16)}{=} \frac{1}{\sqrt{L}} \left( \text{bubble}(g) \right) \stackrel{(6.12)}{=} \frac{1}{\sqrt{L}} \left( \text{bubble}(g) \right) = \frac{1}{\sqrt{L}} \left( \text{bubble}(g) \right) \\ \stackrel{(6.5),(6.20-6.19)}{=} \frac{1}{(L)^{3/2}} \left( \text{bubble}(g) \right) \stackrel{(7.18)}{=} \frac{1}{L} \left( \text{bubble}(g) \right) \end{array}$$

The other equations in (6.16) may be proved similarly, by expanding the bubble and using the existing relations for  $g$ .

We write  $g_{L,\psi}$  for  $g$  surrounded by a bubble as in (7.17). It is clear from (7.18) that  $K_{L,\psi}$  is a group and that the map  $g \mapsto g_{L,\psi}$  is a homomorphism under composition



of permutations of  $A_{L,\psi}$ . (Pull  $g$  through the double wire and contract one loop.) That the map is an isomorphism is clear from the fact it has an inverse

$$\frac{1}{\Delta} \text{ (diagram) } \mapsto \frac{1}{\Delta^2} \text{ (diagram) } = g,$$

where the last equality is obtained by pulling  $g$  through the double wire and contracting the loops.  $\square$

**Proposition 44.** *Let  $A$  be a quantum set, and let  $(L_1 \times L_2, \psi_1 \times \psi_2) < \text{Perm}(A)$  be a direct product of central type subgroups. Let  $P_{L_2, \psi_2} : A_{L_2, \psi_2} \rightarrow A$  be the bijection corresponding to the subgroup  $L_2 < \text{Perm}(A)$  with cocycle  $\psi_2$ . Let  $\bar{L}_1 < \text{Perm}(A_{L_2, \psi_2})$  be the subgroup isomorphic to  $L_1$  obtained by the construction (7.17), and let  $P_{\bar{L}_1, \psi_1} : (A_{L_2, \psi_2})_{\bar{L}_1, \psi_1} \rightarrow A_{L_2, \psi_2}$  be the corresponding bijection.*

*Then  $(A_{L_2, \psi_2})_{\bar{L}_1, \psi_1} = A_{L_1 \times L_2, \psi_1 \times \psi_2}$ , and*

$$P_{L_1 \times L_2, \psi_1 \times \psi_2} = P_{\bar{L}_1, \psi_1} \circ P_{L_2, \psi_2}.$$

*Proof.* By Theorem 13, we need only show that the simple dagger Frobenius algebras  $P_{L_1 \times L_2, \psi_1 \times \psi_2} \circ \bar{P}_{L_1 \times L_2, \psi_1 \times \psi_2}$  and  $P_{\bar{L}_1, \psi_1} \circ P_{L_2, \psi_2} \circ \bar{P}_{L_2, \psi_2} \bar{P}_{\bar{L}_1, \psi_1}$  are  $*$ -isomorphic. This is seen as follows (here the white node is  $P_{L_2, \psi_2}$  and the black node is  $P_{\bar{L}_1, \psi_1}$ ):

$$\text{ (diagram) } = \frac{1}{|L_1|} \sum_{a \in L_1} \text{ (diagram) } = \frac{1}{\sqrt{|L_1||L_2|}} \sum_{\substack{a \in L_1 \\ b \in L_2}} \text{ (diagram) } = \frac{1}{\sqrt{|L_1 L_2|}} \sum_{ab \in L_1 L_2} \text{ (diagram) }$$

Here the middle equality is obtained by pulling  $a$  through the double wire, contracting the loop, and expanding the remaining algebra.  $\square$

*Remark 12.* This implies that quantum bijections corresponding to direct products of central type subgroups can always be decomposed into quantum bijections corresponding to central type subgroups which are not direct products. However, this decomposition does not preserve classicality, in the sense that there is no requirement for the stabilisers of the factors in the product to be coisotropic. A quantum bijection from a classical set may therefore decompose into quantum bijections through quantum set.

*Example 12.* In [77, Introduction], we showed that the usual quantum solution of the Mermin-Peres magic square linear constraint system is obtained from a quantum permutation of its set of partial solutions, corresponding to the direct product of central type subgroups  $(\mathbb{Z}_2 \times \mathbb{Z}_2)^2$ . It is therefore a composite of two quantum bijections from  $(\mathbb{Z}_2 \times \mathbb{Z}_2)$  subgroups. However, the intermediate quantum graph is not classical. Indeed, none of the partial solutions for the middle row or column has nontrivial stabiliser under the action of a single  $(\mathbb{Z}_2 \times \mathbb{Z}_2)$  factor, and the subgroup containing only the identity is not coisotropic.

## 7.4 Quantum pseudo-telepathy

### 7.4.1 From classical symmetries to graph isomorphisms

We have just characterised quantum bijections between classical sets  $\overline{[n]} \rightarrow [n]$  obtained by splitting simple dagger Frobenius algebras in the classical subcategory of  $\text{QPerm}([n])$ . In order to apply these to the study of quantum pseudo-telepathy, we put a relational structure — a graph — on  $[n]$ .

Given an ordinary bijection  $f : \overline{[n]} \rightarrow [n]$ , and an adjacency matrix  $\Gamma$  on  $[n]$ , there is a unique adjacency matrix  $\overline{\Gamma}$  on  $\overline{[n]}$  such that the bijection is also a graph isomorphism. This is true of quantum bijections also, provided that the corresponding algebra is a quantum *automorphism* of the quantum graph  $\Gamma$ . (Note that for a classical bijection, this is always true, since  $f \circ f = \text{id}_A$ .)

**Proposition 45.** *Let  $A$  be a quantum set, let  $\Gamma$  be an adjacency matrix on  $A$ , and let  $(H, P) : B \rightarrow A$  be a quantum bijection of dimension  $d$ , such that  $P \circ \overline{P}$  is a quantum automorphism of  $(A, \Gamma)$ . Then there is a unique adjacency matrix  $\Gamma'$  on  $B$  making  $(H, P)$  a quantum isomorphism.*

*Proof.* We define the adjacency matrix  $\Gamma'$  as follows:

$$\begin{array}{c} B \\ | \\ \textcircled{\Gamma'} \\ | \\ B \end{array} = \frac{1}{d} \begin{array}{c} \textcircled{\phantom{\Gamma}} \\ | \\ \textcircled{\Gamma} \\ | \\ \textcircled{\phantom{\Gamma}} \end{array} \begin{array}{c} \curvearrowright \\ \curvearrowleft \end{array}$$

It is easy to see using the double wire-hopping trick that this defines an adjacency matrix on  $B$  making  $P$  into a quantum isomorphism. That it is unique can be seen

from the isomorphism equation (6.33):

□

For a quantum graph  $(A, \Gamma)$ , we now consider which of the simple dagger Frobenius algebras in the classical subcategory of  $\text{QPerm}(A)$  are automorphisms.

**Proposition 46.** *Let  $(A, \Gamma)$  be a quantum graph. A simple dagger Frobenius algebra  $X_{L, \psi, \mathbf{g}}$  in the classical subcategory of  $\text{QPerm}(A)$  is a quantum automorphism of  $(A, \Gamma)$  iff  $(L, \psi) < \text{Aut}(\Gamma)$  and  $\mathbf{g} \in \text{Aut}(\Gamma)^g$ .*

*Proof.* There is an embedding of semisimple categories  $\text{QAut}(\Gamma) \subset \text{QPerm}(A)$ , which takes every quantum automorphism to its underlying quantum permutation. The part of the classical subcategory of  $\text{QPerm}(A)$  contained within  $\text{QAut}(\Gamma)$  is generated by those permutations which are classical automorphisms, and is therefore isomorphic to  $\mathbf{Hilb}_{\text{Aut}(\Gamma)}$ . The result then follows from Theorem 17. □

These algebras split as before. Again, postcomposition by a direct sum of classical automorphisms does not change the isomorphism class of the source graph, giving the following corollary.

**Corollary 9.** *The isomorphism class of the new graph  $\Gamma'$  depends only on the fine factor of the algebra.*

We therefore write  $\overline{\Gamma}_{L, \psi}$  to indicate the quantum isomorphic graph obtained from a central type subgroup  $(L, \psi) < \text{Aut}(\Gamma)$ .

## 7.4.2 The graph $\Gamma_{L, \psi}$

### General description

For quantum graph isomorphisms between classical sets  $\overline{[n]}_{L, \psi} \rightarrow [n]$  obtained from the classical subcategory, we give an explicit description of the new graph  $\overline{\Gamma}_{L, \psi}$ .

Let  $\Gamma$  be a graph on  $[n]$ , and let  $(L, \psi) < \text{Aut}(\Gamma)$  be a group of central type. Recalling Section 7.2.4, let  $\{O_i \subset [n]\}$  be the orbits under the  $L$ -action, let  $\{v_i \in O_i\}$  be chosen vertices in each orbit, let  $H_i := \text{Stab}(v_i)$ , let  $\mathcal{H}_{ij}$  be the set of  $(H_i, H_j)$ -double cosets, and let  $\{\epsilon_{ij} : \mathcal{H}_{ij} \rightarrow \{0, 1\}\}$  be the edge functions of the graph.

**Definition 64.** We define the graph structure  $\Gamma_{L,\psi}$  on the set  $\overline{[n]}_{L,\psi}$  as follows. Let  $\rho, \rho' \in \overline{[n]}_{L,\psi}$  be irreducible modules of  $\mathbb{C}H_i^\psi$  and  $\mathbb{C}H_j^\psi$  respectively. By Theorem 15, let  $X \in \mathcal{H}_{ij}$  be the unique double coset such that

$$\rho \not\sim (\rho')^{(x)} \quad \text{for all } x \in X.$$

Then

$$\rho \sim \rho' \quad \text{iff } \epsilon_{ij}(X) = 1. \quad (7.19)$$

**Proposition 47.** *The construction above defines an undirected graph  $\Gamma_{L,\psi}$ , and the quantum bijection  $P_{L,\psi} : \overline{[n]}_{L,\psi} \rightarrow [n]$  is a quantum isomorphism  $\Gamma_{L,\psi} \rightarrow \Gamma$ .*

*Proof.* The relation is clearly well-defined, since the double coset relating two representations is unique. For an undirected graph, the relation must be symmetric. We have that

$$\rho \not\sim (\rho')^{(x)} \Leftrightarrow (\rho)^{(x^{-1})} \not\sim \rho',$$

so this follows from (7.9).

We show that the quantum bijection  $P_{L,\psi} : \overline{[n]}_{L,\psi} \rightarrow [n]$  is a quantum isomorphism. Recall the quantum isomorphism condition for a projective permutation matrix (6.34):

$$\text{If } (v \sim_G v' \text{ and } w \not\sim_{G'} w') \text{ or } (v \not\sim_G v' \text{ and } w \sim_{G'} w') \quad \Rightarrow \quad P_{v',w'} P_{v,w} = 0$$

We need to check that the relevant projectors are orthogonal. For  $g_i \cdot v \in O_i$  and  $g_j \cdot w \in O_j$  we have that  $P_{\rho, g_i \cdot v} = (\rho)^{(g_i)} \subset V_{H_i}$ , and  $P_{\rho', g_j \cdot w} = (\rho')^{(g_j)} \subset V_{H_j}$ . By Theorem 15, the subspaces  $(\rho)^{(g_i)}$  and  $(\rho')^{(g_j)}$  are orthogonal if and only if the unique  $(H_i, H_j)$ -double coset  $X$  such that  $\rho \not\sim (\rho')^X$  does not contain  $(g_i)^{-1}g_j$ .

Suppose that  $\rho \not\sim \rho'$ , and  $g_i \cdot v \sim g_j \cdot w$ . That is,  $\epsilon_{ij}(X) = 0$ , and  $\epsilon_{ij}(H_i(g_i)^{-1}g_j H_j) = 1$ . But then clearly  $(g_i)^{-1}g_j \notin X$ , since the values of  $\epsilon_{ij}$  are different. Suppose on the other hand that  $\rho \sim \rho'$ , and  $g_i \cdot v \not\sim g_j \cdot w$ . That is,  $\epsilon_{ij}(X) = 1$ , and  $\epsilon_{ij}(H_i(g_i)^{-1}g_j H_j) = 0$ . But then again  $(g_i)^{-1}g_j \notin X$ , for the same reason.

The relevant projectors are therefore orthogonal and  $P_{L,\psi} \Gamma_{L,\psi} \rightarrow \Gamma$  is a quantum graph isomorphism.  $\square$

*Remark 13.* Since the quantum graph structure on  $\overline{[n]}_{L,\psi}$  for which  $P_{L,\psi}$  is a quantum isomorphism is unique, it follows that the new graph does not depend on which vertices  $\{v_i\}$  are picked. (An explicit isomorphism between the graphs for different vertex choices can easily be constructed.)

## Description for normal subgroups

In the case where all stabiliser subgroups are normal, the description of the new graph is greatly simplified. In this case, all the  $\psi$ -i.p.r.'s of the subgroup are conjugate (see the discussion after Theorem 14). The following lemma is obvious, but observe that we define a ‘funny’ left action.

**Lemma 18.** *Let  $H < (L, \psi)$  be a normal coisotropic subgroup. Pick a  $\psi$ -i.p.r.  $\rho$  of  $H$ . Let  $\{g_k\}$  be coset representatives for  $L/H$ . Then the set of all  $\psi$ -i.p.r.'s of  $H$  is  $\{\rho^{(g_k)} \mid g_k \in L/H\}$ , which is a transitive  $L$ -set under the left action  $g \cdot \rho^{(g_k)} = \rho^{(g_k g^{-1})}$ .*

By picking representations  $\rho_i$  for each  $H_i$  and coset representatives  $\{g_{i,k}\}_k$  for  $L/H_i$ , the whole set  $\overline{[n]}_{L,\psi}$  acquires an  $L$ -set structure by this left action (which is not necessarily a symmetry of the graph  $\Gamma_{L,\psi}$ ). We now define the following map:

$$\begin{aligned} \overline{[n]}_{L,\psi} &\rightarrow [n] \\ (\rho_i)^{(g_{i,k}^{-1})} &\mapsto g_{i,k} \cdot v_i \end{aligned}$$

Here  $v_i$  are chosen vertices in each orbit  $O_i \subset [n]$ . This map is an isomorphism on the individual orbits. Indeed, we have that:

$$\begin{aligned} \rho_i^{(g_{i,k_1}^{-1})} \sim \rho_i^{(g_{i,k_2}^{-1})} &\Leftrightarrow \epsilon_{i,i}(g_{i,k_1}^{-1} g_{i,k_2}) = 1 \\ &\Leftrightarrow g_{i,k_1} \cdot v_i \sim g_{i,k_2} \cdot v_i \end{aligned}$$

The difference between  $\Gamma_{L,\psi}$  and  $\Gamma$  therefore lies in the connectivity between different orbits. Let  $x_{ji} \in L$  be such that  $\rho_i \not\sim \rho_j^{(x_{ji})}$ . Then:

$$\begin{aligned} \rho_i^{(g_{i,k_1}^{-1})} \sim \rho_j^{(g_{j,k_2}^{-1})} &\Leftrightarrow \epsilon_{i,j}(g_{i,k_1}^{-1} x_{ji} g_{j,k_2}) = 1 \\ &\Leftrightarrow g_{i,k_1} \cdot v_i \sim (x_{ji} g_{j,k_2}) \cdot v_j \end{aligned}$$

The following description of  $\Gamma_{L,\psi}$  is immediate.

**Procedure 6.** Let  $\Gamma$  be a graph with an action of a central type group  $(L, \psi)$ , such that the orbits under the action have normal coisotropic stabilisers. Choose an irreducible representation  $\rho_i$  of each orbit stabiliser  $H_i$ , and for each pair  $(O_i, O_j)$  choose  $x_{ij}$  such that  $\rho_i \not\sim \rho_j$ . Then the graph  $\Gamma_{L,\psi}$  is constructed as follows:

- Draw the orbits as before, with the same internal edges.
- For  $v_i \in O_i, v_j \in O_j$ , connect  $v_i \sim_{\Gamma_{L,\psi}} v_j$  iff  $v_i \sim_{\Gamma} x_{ji} \cdot v_j$ .

*Example 13.* See the quantum isomorphic graphs arising from the Mermin-Peres magic square [6]. Here the group of central type is abelian [77, Introduction], so the stabilisers are normal and the construction is an instance of Procedure 6.

### 7.4.3 Conditions for pseudo-telepathy

Instances of pseudo-telepathy are hard to find by brute force search through all graphs. We now give representation-theoretic conditions for central type groups which characterise their suitability for pseudo-telepathy in the graph isomorphism game.

#### Quantum bijections which cannot produce pseudo-telepathic graphs.

For some quantum bijections, the graph  $\Gamma_{L,\psi}$  will never be isomorphic.

**Lemma 19.** *Let  $A$  be a quantum set and let  $P : B \rightarrow A$  be a quantum bijection. If  $P$  has a one-dimensional component, then  $\bar{\Gamma} \cong \Gamma$  for all quantum graphs  $\Gamma$  on  $A$ , where  $\bar{\Gamma}$  is the pullback of  $\Gamma$  by  $P$ .*

*Proof.* The splitting of a quantum isomorphism is identical to that of the underlying quantum bijection (Proposition 31). The quantum isomorphism therefore always has a one-dimensional component; by definition, this is a classical isomorphism.  $\square$

We know from Corollary 8 that this can never be the case for quantum bijections of classical sets arising from central type subgroups. There is however a much weaker condition than having a one-dimensional component which also means that quantum bijections cannot produce pseudo-telepathic graphs, and which is often satisfied by quantum bijections arising from central type groups. The way to interpret this condition is that it is possible to imitate the quantum bijection using a classical bijection.

**Proposition 48.** *Let  $(L, \psi) < S_n$  be a subgroup of central type with coisotropic stabilisers. Then  $\Gamma_{L,\psi} \cong \Gamma$  for any graph  $\Gamma$  on  $[n]$  if, for each orbit  $O_i$ ,  $i \in I$ , it is possible to choose a bijection of the representations  $\{\rho_{i,k}\}_{k \in K_i}$  of  $H_i$  with the coset representatives  $\{g_{i,k}\}_{k \in K_i} \in G/H_i$ , such that the following subspaces are pairwise non-orthogonal:*

$$(\rho_{i,k})^{(g_{i,k})} \not\perp (\rho_{i',k'})^{(g_{i',k'})} \quad \text{for all } i, i' \in I, k \in K_i, k' \in K_{i'} \quad (7.20)$$

*Proof.* Suppose that the condition is satisfied. Then consider the bijection  $\rho_{i,k} \mapsto g_{i,k} \cdot v_i$ . We show that this is an isomorphism. Note first that, by Proposition 47:

$$\rho_{i,k} \sim \rho_{i',k'} \Leftrightarrow \epsilon_{ii'}(X) = 1 \text{ where } \rho_{i,k} \not\perp (\rho_{i',k'})^{(X)}$$

On the other hand, in the graph  $\Gamma$ :

$$g_{i,k} \cdot v_i \sim g_{i',k'} \cdot v_{i'} \Leftrightarrow \epsilon_{ii'}(\langle (g_{i,k})^{-1} g_{i',k'} \rangle) = 1$$

Now consider the condition (7.20):

$$\begin{aligned} (\rho_{i,k})^{(g_{i,k})} \not\sim (\rho_{i',k'})^{(g_{i',k'})} &\Leftrightarrow \rho_{i,k} \not\sim (\rho_{i',k'})^{((g_{i,k})^{-1}g_{i',k'})} \\ &\Leftrightarrow X = \langle ((g_{i,k})^{-1}g_{i',k'}) \rangle. \end{aligned}$$

It follows that  $\rho_{i,k} \sim \rho_{i',k'}$  if and only if  $g_{i,k} \cdot v_i \sim g_{i',k'} \cdot v_{i'}$ .  $\square$

### Quantum bijections which produce pseudo-telepathic graphs.

In contrast, we now present a sufficient condition on  $(L, \psi) < S_n$  for us to construct a graph structure  $\Gamma$  such that  $\Gamma_{L,\psi} \cong \Gamma$ .

**Definition 65.** Let  $(L, \psi) < S_n$ . We define the *homogeneous graph for  $L$*  to be the  $L$ -symmetric graph on the vertex set  $[n]$  where, for  $X \in \mathcal{H}_{ij}$ ,

$$\epsilon_{ij}(X) = 1 \text{ if and only if } 1 \notin X.$$

**Proposition 49.** Let  $(L, \psi) < S_n$  be a subgroup of central type with coisotropic stabilisers, and let  $\Gamma$  be the homogeneous graph for  $L$ . Then  $\Gamma_{L,\psi} \cong \Gamma$  if and only if, for each orbit  $O_i$ ,  $i \in I$  it is possible to choose a pairing of the representations  $\{\rho_{i,k}\}_{k \in K_i}$  of  $H_i$  with coset representatives  $\{g_{i,k}\}_{k \in K_i} \in G/H_i$  for each  $i$ , such that

$$(\rho_{i,k}) \not\sim (\rho_{i',k'}) \text{ if and only if } (g_{i,k})^{-1}g_{i',k'} \in H_i e H_j. \quad (7.21)$$

*Proof.* If it is possible to find such a pairing, then again, choose the bijection  $(\rho_{i,k}) \mapsto g_{i,k} \cdot v_i$ . We show that this is an isomorphism. By Proposition 47 and Definition 65:

$$\rho_{i,k} \not\sim \rho_{i',k'} \Leftrightarrow \rho_{i,k} \not\sim \rho_{i',k'} \quad (7.22)$$

By Definition 65:

$$g_{i,k} \cdot v_i \not\sim g_{i',k'} \cdot v_{i'} \Leftrightarrow v_i \not\sim ((g_{i,k})^{-1}g_{i',k'}) \cdot v_{i'} \quad (7.23)$$

$$\Leftrightarrow (g_{i,k})^{-1}g_{i',k'} \in H_i e H_j \quad (7.24)$$

Then (7.21) implies that  $\rho_{i,k} \not\sim \rho_{i',k'}$  if and only if  $g_{i,k} \cdot v_i \not\sim g_{i',k'} \cdot v_{i'}$ . The map is therefore an isomorphism.

In the other direction, suppose that there exists an isomorphism  $f : \Gamma_{L,\psi} \rightarrow \Gamma$ . Pair  $g_{i,k}$  with the preimages  $\rho_{i,k} = f^{-1}(g_{i,k} \cdot v_i)$ . Since the map is an isomorphism, we have that  $\rho_{i,k} \not\sim \rho_{i',k'}$  if and only if  $g_{i,k} \cdot v_i \not\sim g_{i',k'} \cdot v_{i'}$ , so we obtain by (7.22) and (7.23) that

$$(g_{i,k})^{-1}g_{i',k'} \in H_i e H_j \Leftrightarrow \rho_{i,k} \not\sim \rho_{i',k'}.$$

$\square$

## A recipe for finding pseudo-telepathic graph pairs

There are many graphs, but relatively few central type groups. In [77, Introduction], we showed that the smallest-known pair of quantum isomorphic graphs is generated by a quantum bijection arising from a central type subgroup  $(\mathbb{Z}_2)^4 < S_{24}$ . In this case, the target of the quantum isomorphism is the homogeneous graph (Definition 65).

It is a straightforward task to run through the central type groups of  $S_n$  for  $n \leq 24$  and see if the condition (7.21) is satisfied. In this way, it may be possible to find a smaller pseudo-telepathic graph pair. Regrettably, we have not had time to include this in the thesis.

## 7.5 Linear constraint systems

In the abelian case, our construction is closely related to the theory of linear constraint systems [27, 28].

### 7.5.1 Definition

**Definition 66.** A *linear constraint system* over a finite field  $\mathbb{Z}_p$ ,  $p$  prime, considered as a multiplicative group with elements  $\{e^{2k\pi i/p} \mid 0 \leq k \leq p-1\}$ , is defined by a set of *variables*  $X = \{x_i \mid 1 \leq i \leq n\}$  and a set of  $m$  *equations*, defined by subsets  $\{E_k \subset X \mid 1 \leq k \leq m\}$  of the variables and *constants*  $\{c_k \in \mathbb{Z}_p \mid 1 \leq k \leq m\}$ :

$$\prod_{x \in E_k} x = c_k$$

A *classical solution* of such a system is a function  $f : X \rightarrow \mathbb{Z}_p$  such that the equations hold.

Let  $U_p(d)$  be the group of unitary operators on a Hilbert space of dimension  $d$  with eigenvalues in  $\mathbb{Z}_p$ . A *operator solution* to a linear constraint system over  $\mathbb{Z}_p$  is a function  $q : X \rightarrow U_p$  such that:

- If  $x_1, x_2 \in X$  appear in the same equation, then  $q(x_1)q(x_2) = q(x_2)q(x_1)$ . (The operators for variables in the same equation are simultaneously measurable.)
- For each  $1 \leq k \leq m$ ,

$$\prod_{x \in E_k} q(x) = c_k \mathbb{1}.$$

(Measuring all operators in the same equation  $E_k$  and multiplying the outcome values will always give  $c_k$ .)



Classical and operator solutions to the LCS are classical and quantum strategies, respectively, for a certain nonlocal game.

**Definition 67.** A *local solution* for an equation  $E_k$  is a function  $l : E_k \rightarrow \mathbb{Z}_p$  such that  $\prod_{x \in E_k} l(x) = c_k$ .

**Definition 68** (Linear constraint system game [6]). The verifier gives Alice and Bob each an index  $1 \leq k_A, k_B \leq n$ , specifying an equation for each party. To win, Alice and Bob must return local solutions  $f_A : E_{k_A} \rightarrow \mathbb{Z}_p$  and  $f_B : E_{k_B} \rightarrow \mathbb{Z}_p$  respectively, such that  $f_A|_{E_{k_A} \cap E_{k_B}} = f_B|_{E_{k_A} \cap E_{k_B}}$ .

An operator solution defines a quantum strategy for the game. Alice and Bob share a maximally entangled state  $\sum_{i=1}^d |i\rangle \otimes |i\rangle$ . Alice measures the operators  $\{q(x) \mid x \in E_{k_A}\}$ , and returns the values measured. Bob measures the operators  $\{q(x)^T \mid x \in E_{k_B}\}$ , and returns the values measured. By (7.5.1), these will be local solutions, and the correlations from entanglement imply that they will agree on any overlapping variables.

## 7.5.2 Operator solutions from groups of central type

It has already been shown in [6] that an operator solution to a linear constraint system is a quantum graph isomorphism.

**Definition 69.** We define the *graph* of a linear constraint system as follows:

- A vertex for each local solution.
- An edge  $(E_k, l_k) \sim (E_{k'}, l_{k'})$  if and only if there is a contradiction between them; that is, a variable  $x \in E_k \cap E_{k'}$  such that  $l_k(x) \neq l_{k'}(x)$ .

**Definition 70.** The *homogenisation* of a linear constraint system has the same set of variables and equations, but all constants  $c_k$  are set to 1.

**Theorem 21** ([6]). *There is a classical (resp. operator) solution to a linear constraint system if and only if there is a classical (resp. quantum) isomorphism from the graph  $\Gamma$  of the linear constraint system to the graph  $\Gamma_0$  of its homogenisation.*

It should therefore be possible to construct operator solutions to linear constraint systems from central type symmetries of the graphs of their homogenisations. In fact, up to a minor subtlety, every abelian group  $(\mathbb{Z}_p)^{2n}$  of central type acting on a set gives a solution to a linear constraint system in this way. The correspondence depends on three lemmas.

**Lemma 20.** *The orthogonal complement  $H^\perp$  of any coisotropic subgroup  $H$  is isotropic.*

*Proof.* If  $H^\perp$  is orthogonal to all of  $H$ , it must certainly be orthogonal to  $H^\perp \subset H$ .  $\square$

**Lemma 21.** *Let  $(L, \psi)$  be an abelian group of central type, and  $H < L$  be a coisotropic subgroup. Let  $V$  be the unique irreducible module of  $\mathbb{C}L^\psi$ . Then the irreducible subspaces  $\rho \subset V_H$  are precisely the (possibly degenerate) joint eigenspaces for the operators  $\{\bar{h}|h \in H^\perp\}$ .*

*Proof.* We first show that the action of  $H$  on  $V_H$  preserves the eigenspaces of  $H^\perp$ . Indeed, let  $x \in H, y \in H^\perp$ , and  $v$  an eigenvector for  $H^\perp$  with eigenvalue  $\lambda_y$  for  $y$ . Then

$$\bar{y}hv = \bar{h}yv = \lambda_y \bar{h}v,$$

so the action of  $H$  preserves eigenspaces. Therefore the number of eigenspaces of  $H^\perp$  in  $V$  is less than or equal to the number of irreducible subspaces of  $V_H$ . We now show that there are as many eigenspaces in  $V$  as irreducible subspaces, and the result follows.

Firstly, we show that the distinct possible sets of joint eigenvalues of the operators in  $H^\perp$  is precisely the number of 1-cochains on  $H^\perp$  whose differential  $df$  is  $\psi|_{H^\perp}$ ; that is, the number of functions  $f : H^\perp \rightarrow U(1)$  such that  $f(h_1)f(h_2)/f(h_1h_2) = \psi(h_1, h_2)$  for all  $h_1, h_2 \in H^\perp$ . To see this, first note that any possible eigenvalue assignment  $f : H^\perp \rightarrow U(1)$  must satisfy  $df = \psi|_{H^\perp}$ , since, for  $v$  a joint eigenvector of  $\bar{h}_1, \bar{h}_2$ :

$$f(h_1)f(h_2)v = \bar{h}_1\bar{h}_2v = \psi(h_1, h_2)\bar{h}_1\bar{h}_2v = \psi(h_1, h_2)f(h_1h_2)v$$

To go in the other direction, observe that the difference  $f_1^{-1}f_2 : H^\perp \rightarrow U(1)$  between any two such 1-cochains is a character of  $H^\perp$ . The 1-cochains with differential  $\psi|_{H^\perp}$  therefore form a *torsor* for the character group  $(H^\perp)^*$  — that is, a set carrying a free and transitive action of  $(H^\perp)^*$  by multiplication — and are therefore in (non-canonical) bijection with the elements of  $(H^\perp)^*$ .

Now we show that  $(H^\perp)^*$  has  $|L|/|H|$  elements. This follows from the fact that the kernel of the surjective homomorphism

$$\begin{aligned} \rho : L &\rightarrow (H^\perp)^* \\ a &\mapsto \rho(a, -) \end{aligned}$$

is  $H$ . To see that this map is a homomorphism, simply observe:

$$\rho(a, bc)\bar{b}\bar{c}\bar{a} = \rho(a, bc)\psi(b, c)\bar{b}\bar{c}\bar{a} = \psi(b, c)\bar{a}\bar{b}\bar{c} = \bar{a}\bar{b}\bar{c} = \rho(a, b)\rho(a, c)\bar{c}\bar{a}\bar{b}$$

For surjectivity, recall from Proposition 35 that  $a \mapsto \rho(a, -)$  is an isomorphism  $L \rightarrow L^*$ , and so yields all multiplicative characters of  $L$ . Since any character of  $(H^\perp)$  induces a character of  $L$ , we obtain all the characters of  $H^\perp$  upon restriction. Finally, the kernel is by definition  $(H^\perp)^\perp$ ; since  $L$  is abelian,  $\rho$  is a symplectic form on a vector space, and so we can use dimension counting to obtain  $(H^\perp)^\perp = H$ .

We have now proved that  $H^\perp$  has the correct number of possible eigenvalues; to finish we must show that they all appear in  $V_H$ . For this, observe that the action of  $L$  on  $V$  varies the eigenspaces as

$$\bar{h}\bar{x}v = \rho(h, x)\lambda_h\bar{x}v.$$

As we have seen, this action is transitive; it is therefore clear that all joint eigenvalues of  $H^\perp$  have associated eigenspaces in  $V_H$ .  $\square$

**Lemma 22.** *For any abelian group  $A$ ,*

$$\sum_{g \in A} g = e, \tag{7.25}$$

*except when  $A$  contains precisely one self-inverse element.*

*Proof.* Let  $S < A$  be the subgroup of elements of order  $\leq 2$ . It is clear that  $\sum_{g \in A} g = \sum_{s \in S} s$ , since the elements which are not self-inverse will cancel. It is also clear that  $S \cong \mathbb{Z}_2^n$  for some  $n$ . For  $n = 0$ , (7.25) holds. For  $n \geq 1$ ,

$$\sum_{s \in \mathbb{Z}_2^n} s = \sum_{s \in \mathbb{Z}_2^{n-1}} (s, \bar{0}) + \sum_{s \in \mathbb{Z}_2^{n-1}} (s, \bar{1}) = \left( \sum_{s \in \mathbb{Z}_2^{n-1}} s, \bar{0} \right) + \left( \sum_{s \in \mathbb{Z}_2^{n-1}} s, 2^{\bar{n}-1} \right).$$

It is then easy to see that (7.25) holds except for  $n = 1$ .  $\square$

We are now ready to outline the correspondence. Given a central type group acting on a set, where the action has stabilisers  $H_i$ , we obtain a quantum solution to a linear constraint system where the variables in the  $i$ th equation are elements of  $H_i^\perp$ , and the constants are obtained from the 2-cocycle of the central type group.

**Proposition 50.** *Let  $(L, \psi) := (\mathbb{Z}_p^{2n}, \psi) < S_n$  be a central type group, let  $H_i$  be the stabilisers of the orbits, and let  $\Gamma$  be the homogeneous graph (Definition 65). If  $(H_i)^\perp \not\cong \mathbb{Z}_2$  for all  $i$ , then:*

- $\Gamma$  is the graph of the homogeneous linear constraint system with variables  $X = \{x \mid x \in \sqcup_i (H_i)^\perp\}$ , and equations defined by  $E_k = \{x \mid x \in H_k^\perp\}$ .

- $\Gamma_{L,\psi}$  is the graph of the same linear constraint system with constants  $c_k = \psi(E_k)$ .
- $q(x) = U_x$ , where  $U_x$  is the UEB associated to  $(L, \psi)$ , is an operator solution for the linear constraint system with constants  $c_k$ .

*Proof.* To demonstrate the first bullet point, we show that the vertex sets of each graph are isomorphic as  $L$ -sets, and that the connected double cosets are the same in each graph for each pair of orbits; the result then follows. By Proposition 35 we have an isomorphism of groups:

$$\begin{aligned} \rho : L/H_i &\rightarrow (H_i^\perp)^* \\ a &\mapsto \rho(a, -) \end{aligned}$$

Here  $(H_i^\perp)^*$  is the character group of  $H_i^\perp$ , which, by (7.25), is also the group of local solutions to the equation  $\prod_{x \in H_i^\perp} = 1$ . We therefore pick a vertex  $v_i$  in each orbit of  $\Gamma$  and a local solution  $\phi_i$  for  $\prod_{x \in H_i^\perp} = 1$ , and define a bijection from vertices in each orbit to local solutions:

$$a \cdot v_i \mapsto \rho(a, -)\phi_i.$$

This is clearly an isomorphism of  $L$ -sets; moreover, for each pair of orbits only the identity double coset is disconnected, so it must also be an isomorphism of graphs.

For the second bullet point, we use Lemma 21. In particular, each vertex corresponds to a representation of  $H_i$ , so is an eigenspace of  $H_i^\perp$ . The connectivity is clearly the same in each case, because  $\Gamma$  only had the identity double cosets disconnected, and by Proposition 47 this will be true of  $\Gamma_{L,\psi}$  also.

The third bullet point follows since the operators  $\{U_x \mid x \in H_i^\perp\}$  are all commuting (since  $H_i^\perp$  is isotropic) and  $\prod_{x \in H_i^\perp} U_x = \psi(H_i^\perp)\mathbb{1}$  (by Lemma 22).  $\square$

*Remark 14.* This justifies our use of the term ‘homogeneous graphs’ in Definition 65; they can be seen as nonabelian generalisations of graphs of homogeneous linear constraint systems.

*Remark 15.* This result can be extended to all abelian groups of central type by broadening the definition of linear constraint system to include variables taking values in different subfields of a larger finite field.

### 7.5.3 A characterisation of quantum solutions obtained from central type groups

It is a consequence of Proposition 50 that we can construct a linear constraint system and a quantum solution for any abelian group of central type acting on a set, as long

as none of the stabilisers of the orbits of the action are isomorphic to  $\mathbb{Z}_2$ . Here we determine which quantum solutions to linear constraint systems can be obtained in this way.

**Definition 71** ([27, Definition 3]). The solution group  $G$  for a linear constraint system  $X, \{E_k\}, \{C_k\}$  is presented by generators  $x \in X$  and  $J$ , and relations:

1.  $x^p = J^p = e$  for all  $x \in X$ .
2.  $[x, J] = e$  for all  $x \in X$  ( $J$  commutes with each generator).
3. If  $x, x' \in X$  appear in the same equation  $E_k$ , then  $[x, x'] = e$ .
4.  $\prod_{x \in E_k} x = J^{c_k}$ .

It was shown in [27] that unitary representations of this group where  $J$  is not represented by the identity matrix are, up to a phase, quantum solutions to the LCS. The first equation specifies that the operators have eigenvalues in  $\mathbb{Z}_p$ ; the second equation specifies that  $J$  will be taken to the complex root of unity defining the constants; the third equation specifies that operators corresponding to variables in the same equation are simultaneously measurable; and the fourth equation specifies that the values measured for observables in a given equation  $E_k$  will multiply to  $c_k$ .

*Remark 16.* In general this group is infinite, since there is no relation specified between generators not in the same equation.

*Remark 17.* Classical solutions correspond to the one-dimensional representations of the solution group.

One method of obtaining representations of the solution group is to consider its abelianisation.

**Definition 72.** The *abelianisation* of the solution group  $G' := G/[G, G]$  is the quotient of the solution group by its commutator subgroup. It has a generators-and-relations presentation as in Definition 71, but with the additional equations  $[x, x'] = e$  for all  $x, x' \in X$ .

Any representation of the abelianisation such that the image of  $J$  is not  $\mathbb{1}$  gives a quantum solution of the linear constraint system, after precomposition with the quotient map  $G \rightarrow G'$ . To relate this to our construction of quantum solutions to linear constraint systems from central type subgroups, we reformulate the definition of the solution group in the language of projective representation theory.

**Definition 73.** The *projectivisation*  $G_0$  of the solution group is the quotient of  $G$  by the central type subgroup  $\langle J \rangle$ . (It is generated by all the variables except  $J$ , with  $J$  taken to the identity in the relations.)

**Proposition 51.** *Quantum solutions to the LCS are in bijection with projective representations  $\rho$  of  $G_0$  with 2-cocycle  $\psi : G_0 \times G_0 \rightarrow \mathbb{Z}_p$  satisfying the following conditions:*

1. *The subgroups generated by the variables  $\langle E_k \rangle$  are isotropic.*
2.  *$\psi(E_k) = c_k$ .*

*In the quantum solution, the variable  $x$  is taken to the operator  $\rho(x)$ .*

*Proof.* We already know that the quantum solutions to the linear constraint system are representations  $\rho$  of  $G$  where  $J \mapsto \mathbb{1}$ . As in Proposition 34, this induces a projective representation  $\rho$  of  $G_0$ , where the generators  $x$  are mapped to  $\rho(x)$ . The 2-cocycle is defined by

$$\psi(x_1, x_2)\mathbb{1} = \rho(x_1)\rho(x_2)\rho(x_1x_2)^\dagger$$

The condition (1) follows from condition (3) of Definition (71), and the condition (2) follows from condition (4) of Definition (71).

In the other direction, given a projective representation of  $G_0$  with  $\mathbb{Z}_p$ -valued cocycle  $\psi$ , one obtains a representation of  $G_0 \times \mathbb{Z}_p$ , where that group has multiplication defined by

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, \psi(a_1, a_2)b_1b_2).$$

Let  $J$  be a generator of  $\mathbb{Z}_p$ . Then we have an ordinary representation of the free group on the generators of  $G$ . We now show that the conditions (1) and (2) imply all the relations in Definition 71. Relation (1) follows from the same relation in  $G'$  and the fact that the cocycle is  $\mathbb{Z}_p$ -valued. Relation (2) follows immediately from the direct product. Relation (3) follows from condition (1) above. Finally, relation (4) follows from condition (2) above. We therefore obtain an ordinary representation of  $G$ .

It is straightforward to see that these constructions are mutually inverse. In one direction, we start with an ordinary representation  $\rho$  of  $G$ ; we first eliminate the  $J$ , and then put it back when we identify it with a generator of  $\mathbb{Z}_p$ . As long as we pick that generator to be  $\rho(J)$  we therefore recover the original representation. The other direction is clear.  $\square$

**Definition 74.** The *projective abelianisation*  $G'_0$  is the quotient of  $G'$  by the central subgroup  $\langle J \rangle$  (or equivalently, the abelianisation of  $G_0$ ).

This group has a natural characterisation.

**Definition 75.** The *homogeneous solution group* of an LCS is the group of classical solutions to its homogenisation.

**Proposition 52.** *The group  $G'_0$  is isomorphic to the homogeneous solution group.*

*Proof.* Let  $(G'_0)^*$  be the dual of the abelian group  $G'_0$ ; that is, the (non-canonically) isomorphic group of its ordinary representations. As  $G'_0$  is the abelianisation of  $G_0$ , irreducible ordinary representations of  $G'_0$  are in one-to-one correspondence with irreducible one-dimensional ordinary representations of  $G_0$ . By Proposition 34, these are one-dimensional representations of  $G$  where  $J$  maps to 1, which are precisely the elements of the homogeneous solution group.  $\square$

Now we have introduced the group  $G'_0$ , we consider its relevance for the linear constraint system.

**Proposition 53.** *A quantum solution to the LCS with solution group  $G$  which factors through the abelianisation  $G'$  is precisely a projective representation of  $G'_0$  with 2-cocycle  $\psi$ , where:*

1. *The subgroups generated by the variables  $\langle E_k \rangle$  are isotropic.*
2.  *$\psi(E_k) = c_k$ .*

*Proof.* Follows from the fact that the quotient  $G \rightarrow G'_0$  is the same whether we quotient by the commutator subgroup first, or the group  $\langle J \rangle$ .  $\square$

*Remark 18.* The Mermin-Peres magic square solution is obtained in this way from the homogeneous solution group  $G'_0 \cong (\mathbb{Z}_2)^4$  of the associated linear constraint system (see [77, Introduction]).

In Proposition 50 we showed that, for any central type subgroup acting faithfully on a set, where all point stabilisers are coisotropic, we obtain a quantum solution of a certain linear constraint system. We now show that in fact this construction captures, in a precise sense, the nonclassical part of any solution to a linear constraint system which factors through the abelianisation of the solution group.

Let  $G'_0$  be the projective abelianisation of a solution group, with variable set  $X$ , and let  $\rho : G'_0 \rightarrow U(d)$  be a projective representation with  $\mathbb{Z}_p$ -cocycle. Up to a phase, the operator corresponding to a general element in  $G'_0$  can be expressed as

$$\bar{a} = \prod_{x \in X} \bar{x}^{n_x}$$

where  $0 \leq n_x \leq p - 1$  for all  $x$ . Some of these products of operators will commute with everything else in the solution group and can therefore be measured beforehand; suppose we have done this, and pick an eigenvalue for each of these operators. Since they commute with the measured operators, the other operators will restrict to unitaries on the corresponding joint eigenspace. We therefore obtain a new solution group, with additional equations (specifying the joint eigenvalues of the measured operators); and a new quantum solution, on a Hilbert space with decreased dimension (the dimension of the joint eigenspace of the measured operators), given by  $x \mapsto \pi \bar{x} \pi$ , where  $\pi$  is the Hermitian projection onto the joint eigenspace of the measured operators. If any of the operators for the generating variables are one-dimensional, remove those variables and change the constants accordingly. It may now be that some of the operators corresponding to elements of the new solution group commute with all the other operators in the new solution. In this case, repeat the above process. One will eventually arrive at an operator solution which has no operators commuting with all others.

**Definition 76.** We call the non-redundant quantum solution obtained in the above manner a *core* of the original operator solution.

A core is obviously non-unique in general, since it depends on a choice of eigenvalues. Since  $\rho(a, b)$  is 1 only if  $\bar{a}$  and  $\bar{b}$  commute, we obtain our final observation by Definition 50.

**Proposition 54.** *Any core of an operator solution to a linear constraint system factoring through the abelianisation is a representation of a group of central type.*



# Part III

## Conclusions

# Chapter 8

## Conclusions

Before concluding the thesis, let us take a few pages to suggest some avenues of further research based on the results we have derived.

**Applications of the results in Part I.** The first part of the thesis is at least a proof-of-principle that the categorical-algebraic approach is a viable method of generating novel operational quantum protocols which can be applied in the real world. But will these new teleportation schemes will be practically useful?

Our protocol for quantum teleportation with infinite reference frame misalignment should be applicable to most realistic cases in which two parties attempting to do quantum teleportation might experience reference frame misalignment as a result of their physical setup. Whether our scheme is more useful than others depends on the scenario being considered. Quantum technology is at an early stage, and it is perhaps unlikely experimentalists will look in the near future for a teleportation protocol which optimises resource use to the extent of our tight protocols, or encounter the kind of reference frame uncertainty for which they might be best suited.

Our perfect tight protocol for finite groups may be more suitable for near-term applications. It would be unusual for finite group reference frame uncertainty to arise ‘by accident’. However, it is certainly possible for communicating parties to deliberately induce reference frame uncertainty, using their reference frame configuration is a sort of secret key. In this setting, our protocol shows that it is possible to perform quantum teleportation without ever sharing a secret key, or leaking any information about the key one is using. This could have various applications to secure communication and computation: together with shared magic states, for instance, teleportation becomes a powerful computational primitive. The fact that there is no need to share a secret key is clearly important when many parties are involved.

On a theoretical level the main novelty is that, in order to extend quantum protocols to the setting of unspeakable information, it is natural also to encode classical information unspeakably. The possibilities opened up by this idea, such as doing important protocols other than teleportation without prior alignment and without leaking reference frame information, are largely unexplored.

**Applications of the results in Part II.** The first and most obvious application of the results in Part II is to generate new instances of quantum pseudo-telepathy in the graph isomorphism and linear constraint system games. Since already-known quantum strategies use Pauli or generalised Pauli matrices (abelian groups of central type), this more general construction from nonabelian groups of central type should provide novel examples of ‘nonabelian’ quantum strategies.

We have also identified intriguing hints of a compositional structure behind known quantum strategies. In particular, the quantum graph isomorphism from the Mermin-Peres magic square factors through a pair of isomorphisms to and from an intermediate *quantum set*. Could this have something to do with the appearance of pseudo-telepathy? Evidence will be obtained from observation of the behaviour of our group-theoretical construction under Cartesian product of central type groups. However, for a full understanding we will require a physical interpretation of quantum bijections between general quantum sets.

Indeed, perhaps the main future application of the results in Part II will be as a concrete example of quantum bijections in the case where classical sets are being related to classical sets. We finish by providing a conjecture as to the physical interpretation of quantum bijections between arbitrary finite quantum sets.

The quantum set should be considered as the *type* of an information source. A classical set, for instance, is the type of a classical information source; a matrix algebra is the type of a pure quantum source; while a general quantum set is the type of a mixed classical-quantum source. A quantum bijection between two quantum sets uses half of a maximally entangled state to reversibly transform one type of source into another, where the inverse transformation uses the other half of the maximally entangled state. One example is teleportation: a pure quantum source is reversibly transformed into a classical one using half of a maximally entangled state, then the other half of the entangled state is used to reverse the transformation and recover the classical information. These transformations relate not only sources, but also channels, described by their weighted noncommutative graphs; the notion of a quantum graph isomorphism can be used to classify channels which ‘pull through’ the transformation. This is why we have taken care to prove results here for general quantum sets, wherever possible: the case of classical sets will simply be a general

case of this theory of entanglement-assisted transformations, where both the input source and the transformed source are classical.

We will explore these ideas in future work.

# Bibliography

- [1] Samson Abramsky and Bob 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. arXiv:0808.1023, doi:<http://dx.doi.org/10.1016/B978-0-444-52869-8.50010-4>.
- [2] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007. arXiv:0702152, doi:[10.1103/PhysRevLett.98.230501](https://doi.org/10.1103/PhysRevLett.98.230501).
- [3] Yakir Aharonov and Leonard Susskind. Charge superselection rule. *Physical Review*, 155:1428–1431, 1967. doi:[10.1103/PhysRev.155.1428](https://doi.org/10.1103/PhysRev.155.1428).
- [4] A.V. Anufriev, Yu A. Zimin, A.L. Vol’pov, and I.N. Matveev. Change in the polarization of light in a turbulent atmosphere. *Soviet Journal of Quantum Electronics*, 13(12):1627, 1983.
- [5] Margaret A. Armstrong. *Groups and Symmetry*. Undergraduate Texts in Mathematics. Springer New York, 1997.
- [6] Albert Atserias, Laura Mančinska, David E Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. 2016. arXiv:1611.09837.
- [7] Laszlo Bacsardi. On the way to quantum-based satellite communication. *IEEE Communications Magazine*, 51(8):50–55, 2013. doi:[10.1109/MCOM.2013.6576338](https://doi.org/10.1109/MCOM.2013.6576338).
- [8] E. Bagan, M. Baig, A. Brey, R. Muñoz Tapia, and R. Tarrach. Optimal encoding and decoding of a spin direction. *Phys. Rev. A*, 63:052309, Apr 2001. arXiv:quant-ph/0012006, doi:[10.1103/PhysRevA.63.052309](https://doi.org/10.1103/PhysRevA.63.052309).

- [9] Emili Bagan and Ramon Munoz-Tapia. Aligning spatial frames through quantum channels. *International Journal of Quantum Information*, 4(01):5–16, 2006.
- [10] Yu. A. Bahturin and M. V. Zaicev. Group gradings on matrix algebras. *Canadian Mathematical Bulletin*, 45:499–508, December 2002. URL: <https://cms.math.ca/10.4153/CMB-2002-051-x>, doi:10.4153/CMB-2002-051-x.
- [11] Yu.A Bahturin, S.K Sehgal, and M.V Zaicev. Group gradings on associative algebras. *Journal of Algebra*, 241(2):677 – 698, 2001. URL: <http://www.sciencedirect.com/science/article/pii/S0021869300986435>, doi: <https://doi.org/10.1006/jabr.2000.8643>.
- [12] Teodor Banica and Benoît Collins. Integration over quantum permutation groups. *Journal of Functional Analysis*, 242(2):641–657, 2007. arXiv:math/0606132, doi:10.1016/j.jfa.2006.09.005.
- [13] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Decoherence-full subsystems and the cryptographic power of a private shared reference frame. *Physical Review A*, 70:032307, 2004. arXiv:quant-ph/0403161, doi:10.1103/PhysRevA.70.032307.
- [14] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Reviews in Modern Physics*, 79:555–609, 2007. arXiv:quant-ph/0610030, doi:10.1103/RevModPhys.79.555.
- [15] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. URL: [https://cds.cern.ch/record/111654/files/vol1p195-200\\_001.pdf](https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf), doi:10.1103/PhysicsPhysiqueFizika.1.195.
- [16] Nir Ben David, Yuval Ginosar, and Ehud Meir. Isotropy in group cohomology. *Bull. Lond. Math. Soc.*, 46(3):587–599, 2014. arXiv:1309.2438, doi:10.1112/blms/bdu018.
- [17] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. doi:10.1016/j.tcs.2014.05.025.

- [18] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.
- [19] Francis Borceux. *Handbook of Categorical Algebra*, volume 1 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1994. doi:10.1017/CB09780511525858.
- [20] Dirk Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997. doi:http://dx.doi.org/10.1038/37539.
- [21] Gilles Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003. arXiv:quant-ph/0101005, doi:10.1023/A:1026009100467.
- [22] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005. arXiv:quant-ph/0407221, doi:10.1007/s10701-005-7353-4.
- [23] V. Buzek, R. Derka, and S. Massar. Optimal quantum clocks. *Phys. Rev. Lett.*, 82:2207–2210, Mar 1999. arXiv:quant-ph/9808042, doi:10.1103/PhysRevLett.82.2207.
- [24] G. Chiribella, G. M. D’Ariano, P. Perinotti, and M. F. Sacchi. Efficient use of quantum resources for the transmission of a reference frame. *Phys. Rev. Lett.*, 93:180503, Oct 2004. arXiv:quant-ph/0405095, doi:10.1103/PhysRevLett.93.180503.
- [25] Giulio Chiribella, Vittorio Giovannetti, Lorenzo Maccone, and Paolo Perinotti. Teleportation transfers only speakable quantum information. *Physical Review A*, 86:010304, 2012. arXiv:1008.0967, doi:10.1103/PhysRevA.86.010304.
- [26] Giulio Chiribella, Lorenzo Maccone, and Paolo Perinotti. Secret quantum communication of a reference frame. *Phys. Rev. Lett.*, 98:120501, Mar 2007. arXiv:quant-ph/0608042, doi:10.1103/PhysRevLett.98.120501.
- [27] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017. arXiv:1606.02278, doi:10.1063/1.4973422.

- [28] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, pages 320–331, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg. arXiv:1209.2729, doi:10.1007/978-3-662-43948-7\_27.
- [29] Bob Coecke. Quantum picturalism. *Contemporary Physics*, 51(1):59–83, 2010. arXiv:0908.1787, doi:10.1080/00107510903257624.
- [30] Bob Coecke, Duško Pavlović, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 2009. arXiv:0810.0812, doi:10.1017/s0960129512000047.
- [31] Tania-Luminița Costache. On irreducible projective representations of finite groups. *Surveys in Mathematics & its Applications*, 4, 2009.
- [32] Toby S. Cubitt, Debbie Leung, William Matthews, and Andreas Winter. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.*, 104:230503, Jun 2010. arXiv:0911.5300, doi:10.1103/PhysRevLett.104.230503.
- [33] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing Series. Interscience, 1966.
- [34] Valerio D’Ambrosio, Eleonora Nagali, Stephen P. Walborn, Leandro Aolita, Sergei Slussarenko, Lorenzo Marrucci, and Fabio Sciarrino. Complete experimental toolbox for alignment-free quantum communication. *Nature Communications*, 3:961, 2012. arXiv:1203.6417, doi:10.1038/ncomms1951.
- [35] Sergio Doplicher and John E. Roberts. Why there is a field algebra with a compact gauge group describing the superselection structure in particle physics. *Communications in Mathematical Physics*, 131(1):51–107, Jul 1990. URL: <https://projecteuclid.org/euclid.cmp/1104200703>, doi:10.1007/BF02097680.
- [36] Runyao Duan, Simone Severini, and Andreas Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number. *IEEE Transactions on Information Theory*, 59(2):1164–1174, 2013. arXiv:1002.2514, doi:10.1109/TIT.2012.2221677.



- [37] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity. Low cost and compact quantum key distribution. *New Journal of Physics*, 8(10):249, 2006. [arXiv:quant-ph/0608213](https://arxiv.org/abs/quant-ph/0608213), doi:10.1088/1367-2630/8/10/249.
- [38] J. L. Duligall, M. S. Godfrey, A. M. Lynch, W. J. Munro, K. J. Harrison, and J. G. Rarity. Low cost quantum secret key growing for consumer transactions. In *CLEO Europe and IQEC 2007 Conference Digest*. Optical Society of America, 2007. doi:10.1364/IQEC.2007.JSI2\_4.
- [39] Peter Dybjer. *Category theory and programming language semantics: An overview*, pages 163–181. Springer Berlin Heidelberg, Berlin, Heidelberg, 1986. URL: [https://doi.org/10.1007/3-540-17162-2\\_121](https://doi.org/10.1007/3-540-17162-2_121), doi:10.1007/3-540-17162-2\_121.
- [40] Artur Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67(6):661, 1991. doi:10.1103/PhysRevLett.67.661.
- [41] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik. *Tensor Categories*. American Mathematical Society, 2015. Available online at <http://www.math.mit.edu/~etingof/egnobookfinal.pdf>. doi:10.1090/surv/205.
- [42] Leonhard Euler. Formulae generales pro translatione quacunque corporum rigidorum. *Novi Commentarii academiae scientiarum Petropolitanae*, 20:189–207, 1776.
- [43] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.6*, 2016. URL: <http://www.gap-system.org>.
- [44] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002. [arXiv:quant-ph/0101098](https://arxiv.org/abs/quant-ph/0101098), doi:10.1103/RevModPhys.74.145.
- [45] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999. doi:10.1038/46503.
- [46] Tatsuya Hagino. A typed lambda calculus with categorical type constructors. In David H. Pitt, Axel Poigné, and David E. Rydeheard, editors, *Category Theory and Computer Science*, pages 140–157, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.

- [47] William Helton, Kyle P Meyer, Vern I Paulsen, and Matthew Satriano. Algebras, synchronous games and chromatic numbers of graphs. *arXiv preprint arXiv:1703.00960*, 2017.
- [48] Chris Heunen and Sean Tull. Categories of relations as models of quantum theory. *Electronic Proceedings in Theoretical Computer Science*, 195:247–261, 2015. [arXiv:1506.05028](#).
- [49] Lawrence M. Ioannou and Michele Mosca. Public-key cryptography based on bounded quantum reference frames. *Theoretical Computer Science*, 560(P1):33–45, 2014. [arXiv:0903.5156](#), [doi:10.1016/j.tcs.2014.09.016](#).
- [50] Tanvirul Islam, Loïck Magnin, Brandon Sorg, and Stephanie Wehner. Spatial reference frame agreement in quantum networks. *New Journal of Physics*, 16(6):063040, 2014. [arXiv:1306.5295](#), [doi:10.1088/1367-2630/16/6/063040](#).
- [51] Tanvirul Islam and Stephanie Wehner. Asynchronous reference frame agreement in a quantum network. *New Journal of Physics*, 18(3):033018, 2016. [arXiv:1505.02565](#), [doi:10.1088/1367-2630/18/3/033018](#).
- [52] André Joyal and Ross Street. The geometry of tensor calculus, I. *Advances in Mathematics*, 88(1):55–112, 1991. [doi:10.1016/0001-8708\(91\)90003-P](#).
- [53] André Joyal and Ross Street. The geometry of tensor calculus II. 585, 1991. Available online at <http://maths.mq.edu.au/street/GTCII.pdf>. [doi:10.1016/0001-8708\(91\)90003-P](#).
- [54] G. Karpilovsky. *Projective representations of finite groups*. Monographs and textbooks in pure and applied mathematics. M. Dekker, 1985. URL: <https://books.google.co.uk/books?id=K-nuAAAAMAAJ>.
- [55] Gregory Kelly and Miguel Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19(Supplement C):193 – 213, 1980. [doi:10.1016/0022-4049\(80\)90101-2](#).
- [56] Alexei Kitaev, Dominic Mayers, and John Preskill. Superselection rules and quantum protocols. *Physical Review A*, 69:052326, 2004. [arXiv:quant-ph/0310088](#), [doi:10.1103/PhysRevA.69.052326](#).

- [57] Andreas Klappenecker and Martin Rötteler. Unitary error bases: Constructions, equivalence, and applications. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 139–149, Berlin, Heidelberg, 2003. Springer. doi:10.1007/3-540-44828-4\_16.
- [58] Andreas A. Klappenecker and Martin Roetteler. Catalogue of nice error bases. URL: <http://faculty.cs.tamu.edu/klappi/ueb/ueb.html>.
- [59] Joshua Von Korff and Julia Kempe. Quantum advantage in transmitting a permutation. *Phys. Rev. Lett.*, 93:260502, Dec 2004. arXiv:quant-ph/0405086, doi:10.1103/PhysRevLett.93.260502.
- [60] Greg Kuperberg and Nik Weaver. *A von Neumann algebra approach to quantum metrics/quantum relations*, volume 215. American Mathematical Society, 2012. arXiv:1005.0353, doi:10.1090/S0065-9266-2011-00637-4.
- [61] Anthony Laing, Valerio Scarani, John G. Rarity, and Jeremy L. O’Brien. Reference-frame-independent quantum key distribution. *Physical Review A*, 82:012304, 2010. arXiv:1003.1050, doi:10.1103/PhysRevA.82.012304.
- [62] J. Lambek and P. J. Scott. *Introduction to Higher Order Categorical Logic*. Cambridge University Press, New York, NY, USA, 1986.
- [63] Wen-Ye Liang, Shuang Wang, Hong-Wei Li, Zhen-Qiang Yin, Wei Chen, Yao Yao, Jing-Zheng Huang, Guang-Can Guo, and Zheng-Fu Han. Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding. *Scientific Reports*, 4:3617, 2014. arXiv:1405.2136, doi:10.1038/srep03617.
- [64] Daniel A. Lidar and K. Birgitta Whaley. *Decoherence-Free Subspaces and Subsystems*, pages 83–120. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003. arXiv:quant-ph/0301032, doi:10.1007/3-540-44874-8\_5.
- [65] Martino Lupini, Laura Mančinska, and David E. Roberson. Nonlocal games and quantum permutation groups. 2017. arXiv:1712.01820.
- [66] Ann Maes and Alfons Van Daele. Notes on compact quantum groups. *Nieuw Archief voor Wiskunde*, 4(16):73–112, 1998. arXiv:math/9803122.
- [67] I Marvian and RW Spekkens. Extending noether’s theorem by quantifying the asymmetry of quantum states. *Nature communications*, 5:3821, 2014.

- [68] Iman Marvian and Robert 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. [arXiv:1104.0018](#), [doi:10.1088/1367-2630/15/3/033001](#).
- [69] Ugo Marzolino and Andreas Buchleitner. Quantum teleportation with identical particles. *Physical Review A*, 91:032316, 2015. [arXiv:1502.05814](#), [doi:10.1103/PhysRevA.91.032316](#).
- [70] Ugo Marzolino and Andreas Buchleitner. Performances and robustness of quantum teleportation with identical particles. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 472(2185), 2016. [arXiv:1512.02692](#), [doi:10.1098/rspa.2015.0621](#).
- [71] Kevin McGerty. Lecture notes on groups and representation theory. January 2009. URL: <http://people.maths.ox.ac.uk/mcgerty/ImperialGRT.pdf>.
- [72] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373, 1990.
- [73] Jarosław A. Miszczak. Singular value decomposition and matrix reorderings in quantum information theory. *International Journal of Modern Physics C*, 22(09):897–918, 2011. [arXiv:1011.1585](#), [doi:10.1142/S0129183111016683](#).
- [74] Michael Müger. Abstract duality theory for symmetric tensor  $*$ -categories. In *Philosophy of Physics*, pages 865–922. Elsevier, 2007. [doi:10.1016/b978-044451560-5/50018-x](#).
- [75] Sreram Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 6:20463, 2016. [doi:10.1038/srep20463](#).
- [76] Benjamin Musto, David Reutter, and Dominic Verdon. A compositional approach to quantum functions. *J. Math. Phys.*, 2018. To appear. [arXiv:1711.07945](#).
- [77] Benjamin Musto, David Reutter, and Dominic Verdon. The Morita theory of quantum graph isomorphisms. *Comm. Math. Phys.*, 2018. To appear. [arXiv:1801.09705](#).

- [78] Benjamin Musto and Jamie Vicary. Quantum Latin squares and unitary error bases. *Quantum Information & Computation*, 16(15&16):1318–1332, 2016. [arXiv:1504.02715](#).
- [79] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.
- [80] Dusko Pavlovic. Quantum and classical structures in nondeterministic computation. In Peter Bruza, Donald Sofge, William Lawless, Keith van Rijsbergen, and Matthias Klusch, editors, *Quantum Interaction*, pages 143–157, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. [arXiv:0812.2266](#).
- [81] Asher Peres and Petra F. Scudo. Unspeakable quantum information. In A Khrennikov, editor, *Quantum Theory: Reconsideration of Foundations*. Vaxjo Univesity Press, 2002. [arXiv:quant-ph/0201017](#).
- [82] Stefano Pirandola and Stefano Mancini. Quantum teleportation with continuous variables: A survey. *Laser Physics*, 16(10):1418–1438, 2006. [arXiv:quant-ph/0604027](#), [doi:10.1134/S1054660X06100057](#).
- [83] W. Reiher. Monte Carlo Methods. *Biometrische Zeitschrift*, 8(3):209–209, 1966. [doi:10.1002/bimj.19660080314](#).
- [84] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, 2017. [arXiv:1707.00934](#), [doi:10.1038/nature23675](#).
- [85] Wojciech Roga, Zbigniew Puchała, Lukasz Rudnicki, and Karol Życzkowski. Entropic trade-off relations for quantum operations. *Physical Review A*, 87(3):032308, 2013. [arXiv:1206.2536](#), [doi:10.1103/PhysRevA.87.032308](#).
- [86] Wojciech Roga, Karol Życzkowski, and Mark Fannes. Entropic characterisation of quantum operations. *International Journal of Quantum Information*, 09(04):1031–1045, 2011. [doi:10.1142/S0219749911007794](#).
- [87] John H Selby, Carlo Maria Scandolo, and Bob Coecke. Reconstructing quantum theory from diagrammatic postulates. 2018. [arXiv:1802.00367](#).

- [88] Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, Lecture Notes in Physics, pages 289–355. Springer, Berlin, Heidelberg, 2010. [arXiv:0908.3347](#), [doi:10.1007/978-3-642-12821-9\\_4](#).
- [89] Michael Skotiniotis, Wolfgang Dür, and Barbara Kraus. Efficient quantum communication under collective noise. *Quantum Information and Computation*, 13(3&4):0290–0323, 2013. [arXiv:1204.0891](#).
- [90] Michael Skotiniotis and Gilad Gour. Alignment of reference frames and an operational interpretation for the G-asymmetry. *New Journal of Physics*, 14(7):073022, 2012. [arXiv:1202.3163](#), [doi:10.1088/1367-2630/14/7/073022](#).
- [91] William Slofstra. Tsirelson’s problem and an embedding theorem for groups arising from non-local games. 2016. [arXiv:1606.03140](#).
- [92] Piotr M. Sołtan. Quantum families of maps and quantum semigroups on finite quantum spaces. *Journal of Geometry and Physics*, 59(3):354–368, 2009. [arXiv:0610922](#), [doi:10.1016/j.geomphys.2008.11.007](#).
- [93] Federico M. Spedalieri. Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum. *Optics Communications*, 260(1):340 – 346, 2006. [arXiv:quant-ph/0409057](#), [doi:10.1016/j.optcom.2005.10.001](#).
- [94] Steven van Enk. The physical meaning of phase and its importance for quantum teleportation. *Journal of Modern Optics*, 48(13):2049–2054, 2001. [arXiv:quant-ph/0102004](#), [doi:10.1080/09500340108240906](#).
- [95] Dominic Verdon and Jamie Vicary. Tight reference frame-independent quantum teleportation. *Electronic Proceedings in Theoretical Computer Science*, 236:202–214, 2017. [arXiv:1603.08866v1](#), [doi:10.4204/EPTCS.236.13](#).
- [96] Dominic Verdon and Jamie Vicary. Tight quantum teleportation without a shared reference frame. *Phys. Rev. A*, 98:012306, Jul 2018. URL: <https://link.aps.org/doi/10.1103/PhysRevA.98.012306>, [doi:10.1103/PhysRevA.98.012306](#).
- [97] Jamie Vicary. Categorical formulation of finite-dimensional quantum algebras. *Communications in Mathematical Physics*, 304(3):765–796, 2010. [arXiv:0805.0432](#), [doi:10.1007/s00220-010-1138-0](#).

- [98] Jamie Vicary and Chris Heunen. Lecture notes in categorical quantum mechanics. URL: <http://www.cs.ox.ac.uk/people/jamie.vicary/IntroductionToCategoricalQuantumMechanics.pdf>.
- [99] J Wabnig, D Bitauld, H W Li, A Laing, J L O'Brien, and A O Niskanen. Demonstration of free-space reference frame independent quantum key distribution. *New Journal of Physics*, 15(7):073001, 2013. arXiv:1305.0158, doi:10.1088/1367-2630/15/7/073001.
- [100] Shuzhou Wang. Quantum symmetry groups of finite spaces. *Communications in Mathematical Physics*, 195(1):195–211, 1998. arXiv:math/9807091, doi:10.1007/s002200050385.
- [101] Nik Weaver. Quantum relations. 2010. arXiv:1005.0354.
- [102] Nik Weaver. Quantum graphs as quantum relations. 2015. arXiv:1506.03892.
- [103] Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001. arXiv:quant-ph/0003070, doi:10.1088/0305-4470/34/35/332.
- [104] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017. arXiv:1707.01339, doi:10.1126/science.aan3211.
- [105] Mário Ziman. Incomplete quantum process tomography and principle of maximal entropy. *Physical Review A*, 78(3):032118, 2008. arXiv:0802.3892, doi:10.1103/PhysRevA.78.032118.
- [106] Karol Życzkowski and Ingemar Bengtsson. On duality between quantum maps and quantum states. *Open Systems & Information Dynamics*, 11(01):3–42, 2004. arXiv:quant-ph/0401119, doi:10.1023/B:OPSY.0000024753.05661.c2.