2012-07-19

Rate of alignment and communication using quantum systems in the absence of a shared frame of reference

Skotiniotis, Michael

UNIVERSITY OF CALGARY

Rate of alignment and communication using quantum systems in the absence of a shared frame of reference

by

Michael Skotiniotis

A DISSERTATION
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PHYSICS AND ASTRONOMY

INSTITUTE FOR QUANTUM INFORMATION SCIENCE

CALGARY, ALBERTA

June, 2012

Abstract

Quantum information theory is concerned with the storage, transmission, and manipulation of information that is represented in the degrees of freedom of quantum systems. These degrees of freedom are described relative to an external frame of reference. The lack of a requisite frame of reference imposes restrictions on the types of states quantum systems can be prepared in and the type of operations that can be performed on quantum systems. This thesis is concerned with the communication between two parties that lack a shared frame of reference. Specifically, I introduce a protocol whereby the parties can align their respective frames of reference, and a protocol for communicating quantum information in a reference frame independent manner.

Using the accessible information to quantify the success of a reference frame alignment protocol I propose a new measure—the alignment rate—for quantifying the ability of a quantum state to stand in place of a classical frame of reference. I show that for the case where Alice and Bob lack a shared frame of reference associated with the groups $G = U(1)$ and $G = \mathbb{Z}_M$ (the finite cyclic group of M elements), the alignment rate is equal to the regularized, linearized G-asymmetry. The latter is a unique measure of the frameness of a quantum state and my result provides an operational interpretation of the G-asymmetry that was thus far lacking. In addition, I show that the alignment rate for finite cyclic groups of more than three elements is super-additive under the tensor product of two distinct pure quantum states. The latter is, to my knowledge, the first instance of a regularized quantity that exhibits super-additivity.

In addition, I propose a reference-frame-independent protocol for communicating quantum information in the absence of a shared frame of reference associated with a general finite group G. The protocol transmits m logical qudits using $r + m$ physical qudits prepared in a specific state that is reference-frame invariant. Measuring the first r

qudits allows one to infer the unitary correction that is required to retrieve the remaining m qudits with perfect fidelity. Moreover, the number of ancillary qudits, r, is finite and depends only the group G associated with the requisite frame of reference. I show that the number of single and two-qubit gates required to encode and decode m logical qudits into $m + r$ physical qudits scales linearly with m and the number of group elements $|G|$. Furthermore, the number of single and two-qubit gates required per logical qudit m is constant allowing for a more efficient implementation than the best currently known reference frame independent protocols.

Acknowledgements

It has been a long and interesting journey. I would like to thank my supervisor Dr. Gilad Gour and my co-supervisor Dr. Barry Sanders for giving my the opportunity to work with them, for their guidance, patience, encouragement in times of distress, and their support. I would also like to thank Dr. Aidan Roy, and Dr. Peter Turner for introducing me to representation theory and for their exposition of the subject.

Special thanks go toward the many grad students in the Institute for Quantum Information Science and the Department of Physics and Astronomy. In particular Borzumehr Toloui Semnani, Elliot Martin, Jérémie Choquette, Julia Pulwicki, Jop Briet, Michael Garrett, Michael Underwood, Michael Durocher, and Nathan Babcock for many stimulating conversations. Special mention goes to the many visitors and in particular Iman Marvian, Robert Spekkens, Giulio Chiribella, Aram Harrow, and Terry Rudolph with whom I shared my ideas and who have helped, either directly or indirectly, with my research.

I would also like to acknowledge CIFAR, EU-Canada exchange, GSA, iCORE, IQIS, NSERC, PIMS, USARO, and the University of Calgary for financial support throughout the duration of my PhD. I am also grateful to the Institute for Theoretical Physics at the University of Innsbruck, and in particular to Dr. Barbara Kraus and Dr. Wolfgang Dür for their gracious hospitality during the winter term of 2011. It was a pleasure and a privilege to have collaborated with them and I cannot thank them enough for the opportunity.

Last but not least, I am grateful to my parents for their many sacrifices in order for me to get to where I am today, my brother for being able to skype with me at absurd hours, and my sister for succeeding despite adversity. I love them dearly and wish to dedicate this past four and a half years to them.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this chapter I motivate the study of communication of information using quantum mechanical systems between parties lacking a requisite frame of reference (Sec. 1.1) and provide an extensive literature review of relevant results. These fall under three categories. In Sec. 1.2 I review how the lack of a shared frame of reference gives rise to a super-selection rule (SSR) and the consequences of the latter on quantum information processing tasks. In Sec. 1.3 I review how two parties can alleviate, at least partially, the restriction of lacking a shared frame of reference. In Sec. 1.4 I review how classical and quantum information can be efficiently communicated in the absence of a shared frame of reference. Finally, Sec. 1.5 outlines my contributions to the resource theory of quantum reference frames, reference frame alignment, and to the communication of information in the absence of a shared frame of reference.

1.1 Motivation

Information is physical. It is stored, processed, and communicated using physical systems whose states are used to represent information. Classical information theory deals with bits and boolean gates whereas quantum information theory uses quantum bits (or qubits) and unitary gates. One important difference between classical and quantum information is that the states of classical systems can be cloned whereas quantum states can not [1]. In addition, certain tasks such as super-dense coding [2] and informationally secure key distribution [3] are only possible in quantum information theory. Quantum information theory can also achieve computational speed-ups to some important algorithmic processes

such as factoring [4] and unstructured search [5].

This thesis is concerned with the communication of information represented in the degrees of freedom of quantum mechanical systems. As an example, consider two parties who wish to communicate classical information using the spin degree of freedom of an electron. The sender, Alice, may represent the classical message 0 (1) by preparing the spin of an electron as aligned (anti-aligned) along a particular direction, $\mathbf{n}$, shared between her and the receiver, Bob. Alice can then transmit the electron through a communication channel to Bob who measures the spin of the electron and retrieves the classical message.

In an ideal communication scenario we assume that Alice and Bob can prepare and measure the degrees of freedom of quantum systems with infinite precision. Furthermore, we assume that the communication channel acts upon every quantum system with the identity operation, and that Alice and Bob share a common frame of reference for the relevant degrees of freedom of quantum systems.

A frame of reference is a physical system whose degrees of freedom possess an inherent asymmetry with respect to a particular set of transformations. For example, a sphere can not serve as a directional frame of reference as it possesses rotational symmetry. A physical system whose degrees of freedom obey a symmetry can not serve as a reference frame for systems whose degrees of freedom do not obey that symmetry. In this thesis I will focus on symmetries that are described by a *group of transformations* G.

If Alice and Bob lack a shared frame of reference for the degrees of freedom of quantum systems used to represent their messages then communication of information is problematic. Indeed, as I show in chapter 2 the lack of a shared frame of reference between Alice and Bob imposes restrictions on the types of states that Alice can prepare and the types of operations that Alice can perform relative to Bob's frame of reference. These restrictions are equivalent to the restrictions imposed by super-selection rules, or SSRs

for short.

The restrictions imposed by the lack of a shared frame of reference can be alleviated, at least partially, if Alice transmits to Bob quantum systems that possess an inherent asymmetry associated with the requisite frame of reference. Such quantum systems are *bounded-sized tokens* of Alice's frame of reference. In chapter 3 I study the task of reference frame alignment using quantum systems and propose a new measure for quantifying a quantum system's ability to act as a bounded-sized token of a reference frame.

However, there are instances where Alice may wish not to alleviate the restrictions imposed by the lack of a shared frame of reference but still be able to communicate information to Bob. For example, it has been shown that if Alice shares a reference frame with a third party, Charlie, then she can communicate privately with Charlie over a public channel [6]. Therefore, it might be advantageous for Alice and Bob to utilize a communication protocol that does not allow either party to learn about the other party's reference frame. In chapter 4 I will introduce a novel protocol for communicating quantum information in the absence of a shared frame of reference whose implementation is more efficient than the best currently known protocols achieving the same goal.

Before outlining the significance of my contributions (Sec. 1.5) I provide a literature review of the main results associated with the problem of quantum communication without a shared frame of reference. Specifically, in Sec. 1.2 I review the main results regarding the equivalence between the restrictions imposed by the lack of a shared frame of reference and those imposed by SSRs. Sec. 1.3 reviews reference frame alignment protocols, and Sec. 1.4 reviews the main results on communication of classical and quantum information in the absence of a shared frame of reference.

1.2 Super-selection rules and quantum information

In this section I review the main results on SSRs and their consequences on quantum information processing tasks. Specifically, Sec. 1.2.1 reviews the main results concerning SSRs and their relation to the lack of a requisite frame of reference. Sec. 1.2.2 reviews the consequences of SSRs on quantum information processing tasks, and Sec. 1.2.3 reviews the main results in the resource theory of reference frames.

1.2.1 Super-selection rules and the lack of a requisite frame of reference.

SSRs, where first introduced by Wick et al. (WWW52) as axiomatic restrictions to quantum theory [7]. At the time SSRs were introduced particles had been observed in coherent superpositions of position eigenstates, linear and angular momentum eigenstates, but no particles had been observed in a coherent superposition of charge eigenstates or in superpositions of parity eigenstates. A SSR associated with a conserved quantity Q states that coherent superpositions of different eigenstates of Q can not be observed.

In quantum theory observables such as charge or angular momentum are represented by Hermitian operators and vice versa [8]. Under a SSR the set of observables is a strict sub-set of all Hermitian operators. Specifically, Hermitian operators whose eigenvectors are coherent superpositions of eigenstates of a conserved quantity, associated with the SSR, do not correspond to observables. As I show in chapter 2 a consequence of SSRs is that any coherent superposition of eigenstates of the conserved quantity associated with the SSR is operationally indistinguishable form an incoherent mixture of eigenstates of the conserved quantity.

The connection between SSRs and the lack of a requisite frame of reference was made by Aharonov and Susskind (AS67) [9]. AS67 showed that a party lacking the requisite frame of reference for the degrees of freedom associated with a conserved quantity faces the same restrictions as those that arise from SSRs. This equivalence is best exhibited

by considering the following example. An isolated laboratory is known to be in an eigenstate of $J_{\mathbf{z}}$, the total angular momentum along the **z**-direction. The laboratory contains a large number of electrons whose spins are aligned along the **z**-direction. At a later time the electrons pass through a magnetic field orientated along the $x-y$ plane of the laboratory. Two experimenters, O_1 standing outside the laboratory and O_2 standing inside the laboratory, are asked to determine the state of the electrons after they pass through the magnetic field. I will now show that from their measurement results O_1 concludes that a SSR is in place whereas O_2 concludes that no SSR is in place.

The probability that the electron's spin is aligned (anti-aligned) along a direction **m** is given by $\cos^2\theta$ ($\sin^2\theta$), where θ is the angle between the electron's spin and the direction **m**. As O_2 knows the direction of the magnetic field by virtue of being inside the laboratory there exists a measurement direction, corresponding to $\theta = 0$, where O_2 observes every electron's spin as aligned. It follows that O_2 is not subject to a SSR as the spin of an electron in any direction can be expressed as a coherent superposition of eigenstates of $J_{\mathbf{z}}$. However, by virtue of being outside the laboratory, observer O_1 has no knowledge of the orientation of the magnetic field and consequently of the direction of each electron's spin. Hence, averaging over all possible values of θ, O_1 finds that the electron's spin is equally likely to be aligned or anti-aligned in any direction he chooses to measure. Thus, O_1 concludes that all the electrons are prepared in an incoherent superposition of the two eigenstates of $J_{\mathbf{z}}$, and that a SSR is in place.

The example above shows that O_1 experiences a SSR as a result of lacking the requisite reference frame, i.e. the direction of the magnetic field in the $x-y$ plane. AS67, and also Mirman [10, 11], argued that SSRs for parity and charge proposed by WWW52 also arise due to the lack of a requisite frame of reference. A proposal for constructing coherent superpositions of charge eigenstates, i.e. a reference frame for charge, involving superconductors was outlined in [12]. Recently, experimental procedures have been proposed

for constructing coherent superpositions of eigenstates of atom number in Bose-Einstein condensates [13, 14, 15, 16, 17, 18].

A similar paradox to the one discussed above appeared in the field of quantum information, and more specifically in quantum optics, due to the work of Mølmer and Sanders et al. (SBRK03) [19, 20]. Prior to the results of Mølmer and SBRK03 it was assumed that the state of the output field of a laser is described by an ensemble of coherent superpositions of photon number eigenstates, known as coherent states[1]. Mølmer and SBRK03 showed that the density matrix describing the output field of a laser can also be described by an incoherent mixture of photon number eigenstates. The latter are states that obey a photon number SSR associated with the lack of a phase reference. Mølmer showed via numerical simulations that this description of the laser is not at odds with experimental results and argued that two lasers satisfying a photon number SSR can interfere [19]. Mølmer's result was verified analytically by SBRK03 [20].

The controversy of whether the optical field of a laser is subject to a photon number SSR or not was resolved by Bartlett et al. (BRS06) [22]. BRS06 showed that quantum coherence is reference-frame dependent: the quantum state of a system contains information not only about the degrees of freedom of a quantum system but also about the reference frame relative to which the degrees of freedom of a quantum system are described. The coherent state description of the output field of a laser describes the state of the optical field relative to an external phase reference whereas the photon-number eigenstate description assumes that no external phase reference is available.

The results outlined in this section show that SSRs impose restrictions on the types of operations a party can perform and that these restrictions, first thought to be axiomatic, arise due to the lack of a requisite frame of reference for the relevant degrees of freedom of quantum systems. As Bartlett et al. state there is no fundamental reason

[1] A coherent state is the right eigenstate of the annihilation operator [21].

why any SSR can not be alleviated other than the difficulty of preparing and maintaing an appropriate frame of reference [23]. In the next section I review the consequences to quantum information processing tasks due to the restrictions imposed by SSRs.

1.2.2 Quantum information subject to SSRs

As mentioned in Sec. 1.2.1 a party subject to a SSR faces restrictions on the observables he/she can measure. In this section I will review the main results regarding the consequences of the restrictions imposed by SSRs on quantum information processing tasks. In addition, I will review the main results on the effects of SSRs on the quantification of entanglement, a key resource in almost all quantum information processing tasks.

The consequences of SSRs were first investigated for quantum communication tasks, and in particular quantum data hiding protocols. In a data hiding protocol classical or quantum information is distributed amongst several parties in such a way that the message can be read if and only if the parties are provided with the means to perform joint measurements. It was shown that perfect data hiding using quantum systems is impossible [24, 25]. Verstraete and Cirac (VC03) showed that if all the parties in a quantum data hiding protocol are subject to a particle-number SSR then perfect quantum data hiding is possible [26]. However, as Kitaev et al. (KMP04) showed, VC03's protocol is not unconditionally secure [27]. An unconditionally secure protocol is one whose security can not be compromised even if the malicious party possess infinite resources. KMP04 noted that nothing prevents a malicious party from possessing a reference system that helps alleviate the SSR.

A key resource in most quantum communication and information tasks is entanglement. The state of a physical system is said to be *entangled* if it can not be written as a convex sum of product states. A measure of entanglement is a monotonic function that quantifies the amount of entanglement of a quantum state. Furthermore, an entangle-

ment measure is said to be *operational* if it quantifies the amount of entanglement of a quantum state by a well-defined task. For example, one can quantify a state $\rho \in \mathcal{B}(\mathcal{H})$ as containing more entanglement than a state $\sigma \in \mathcal{B}(\mathcal{H})$ if the success of performing a super-dense coding protocol [2] using state ρ, is higher than using σ. It follows that SSRs affect the quantification of entanglement by operational measures as I now explain.

Suppose Alice and Bob, located in spatially separate locations, possess a single photon described by the state

$$|\psi\rangle = \frac{1}{2}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right), \tag{1.1}$$

where $|ab\rangle = |a\rangle \otimes |b\rangle$ and $|0\rangle_A|1\rangle_B$ denotes the state where the photon is in Bob's laboratory. If no photon-number SSR is in place then the state of Eq. (1.1) contains the maximum amount of entanglement that can be shared between Alice and Bob regardless of what operational measure is used [28]. However, if Alice and Bob are subject to a photon-number SSR then Wiseman and Vaccaro (WV03) noted that some measures of entanglement would quantify the state in Eq. (1.1) as entangled whereas others would not [29]. Indeed, WV03 observed that under a photon-number SSR most operational measures of entanglement, such as violating a Bell-inequality [30] or performing teleportation [31], require Alice and Bob to perform operations that violate the photon-number SSR. WV03 proposed a new operational measure of entanglement under a SSR as the amount of entanglement that Alice and Bob can generate between their local registers, for which Alice and Bob share a reference frame, using the state of Eq. (1.1) and operations that respect the photon-number SSR.

The results outlined in this section show that the security of certain quantum information processing tasks can be enhanced under the restrictions imposed by a SSR [26]. However, this enhanced security is not unconditional [27]. Moreover, the restrictions imposed by SSRs require us to modify the way entanglement is quantified by operational measures [29]. In the next section I review how SSRs give rise to the resource theory of

quantum reference frames.

1.2.3 The resource theory of reference frames

The results reviewed in Secs.(1.2.1, 1.2.2) state that the restrictions imposed by SSRs can be alleviated if a party has access to a requisite frame of reference. If the reference frame is itself quantum mechanical, e.g. instead of a classical gyroscope one possesses only a handful of electrons, then the quantum mechanical system acts as a *bounded-sized token* of the reference frame. Such a token is a reference frame resource; it can be used to circumvent the restrictions imposed by SSRs. Furthermore, the resourcefulness of such a token gets depleted with every use [32, 33, 34]. In this section I review the major results in the resource theory of reference frames.

Similar to the resource theory of entanglement (see [35] for a review), a method is required to quantify the frameness resource of a bounded-sized token of a reference frame. An operational measure of frameness for the case of a photon-number SSR was proposed by Schuch et al. (SVC) [36, 37]. Specifically, SVC introduced the super-selected induced variance, to quantify the frameness of the state in Eq. (1.1). It was shown by Gour et al. (GMS09) that the super-selected induced variance quantifies the asymptotic rate of reversible interconversion between two bounded-sized tokens of a phase reference [38].

An operational measure of frameness for general SSRs was proposed by van Enk [39]. Just as an *e-bit* quantifies the resource required to lift the restriction of local operations and classical communication (LOCC), van Enk introduced the *ref-bit* to quantify the resource required to lift the restrictions imposed by SSRs. However, van Enk provides no method of calculating the amount of ref-bits of a given bounded-sized token of a reference frame.

A second operational measure of frameness was introduced by Bartlett et al. (BRST06) [32]. They quantified the frameness of a bounded-sized token of a reference frame by the

average probability of successfully estimating the state of a quantum system using the bounded-sized token of the reference frame. A drawback of BRST06's measure is that one requires a large ensemble of quantum systems in order to quantify the frameness of a bounded-sized token. Furthermore, BRST06's measure is ambiguous: if instead of the average probability of success one chooses the average fidelity of estimation, then a resourceful quantum system according to the average probability of success may be quantified as less resourceful under the average fidelity of estimation.

A special measure for quantifying the frameness of a bounded-sized token that will feature prominently in my thesis is the *G-asymmetry* of states introduced by Vaccaro et al. (VAWJ08) [40]. The G-asymmetry quantifies the amount of thermodynamical work that can be extracted from a bounded-sized token of a reference frame. Furthermore, the G-asymmetry is given by an easily computable mathematical expression defined for all groups, G, and for quantum systems of arbitrary dimension. Moreover, it was shown in [38] that the G-asymmetry is equal to the Holevo quantity [41] and the *relative entropy of frameness*, a quantity analogous to the relative entropy of entanglement in the resource theory of LOCC [42] (see chapter 2 for details).

However, whereas the relative entropy of entanglement has an operational interpretation [43] the relative entropy of frameness does not. In chapter 3 I provide an information theoretic, operational interpretation for the G-asymmetry and establish it's connection to reference frame alignment protocols, which I review in the next section.

1.3 Alignment of Reference Frames

In the previous section I reviewed how SSRs arise due to the lack of a requisite frame of reference. If Alice and Bob lack a shared frame of reference for the degrees of freedom of quantum systems used in a communication protocol then the restrictions on operations

that Alice and Bob face are equivalent to those of a SSR. These restrictions can be alleviated, at least partially, if Alice transmits to Bob a bounded-sized token of her reference frame. In this section I review the main results regarding the alignment of reference frames using quantum mechanical systems.

In the reference frame alignment protocols I consider in my thesis Alice prepares several quantum systems aligned in the orientation of her reference frame, and sends them to Bob who performs a measurement and guesses the orientation of Alice's frame of reference. I will focus mainly on reference frames associated with a symmetry group G. The success of the reference frame alignment protocol is quantified by a function $f(g, g')$, where $g \in G$ corresponds to the orientation of Alice's reference frame and $g' \in G$ is Bob's guess of the orientation of Alice's reference frame. The goal is to determine the state that Alice should prepare for her bounded-sized tokens and the measurement Bob should perform such that the *average* function $f(g, g')$ is optimized.

The function $f(g, g')$ used to quantify the success of an alignment protocol satisfies the following two properties. For all $h, g, g' \in G$, $f(hg, hg') = f(g, g')$, i.e. the success of the reference frame alignment protocol depends only on the relative orientation between Alice's and Bob's reference frames. For such functions Holevo showed that the measurement that optimizes the average of $f(g, g')$ is a *covariant measurement* [44]. The latter is a measurement whose elements are $\{E_g = T_g E_0 T_g^\dagger,\ g \in G\}$, where $T : G \to \mathrm{GL}(\mathcal{H}_d)$ is a *unitary representation* of the group G and E_0 is a *fiducial* element of the measurement.

Peres and Wootters (PW90) considered the following scenario akin to reference frame alignment [45]. Suppose that Alice and Bob are given instructions on how to prepare a quantum system in one of three possible ways. Alice and Bob are allowed to communicate classically so that they prepare their respective systems in the same quantum state. Alice and Bob then submit a finite number of systems to a third party, Charlie, whose task is to determine which one of the three possible states the quantum systems have been prepared

in. PW90 showed that the measurement that maximizes Charlie's average information gain about which of the three possible states the quantum systems are prepared in is a *joint measurement* on the quantum systems.

Following PW90's result Massar and Popescu (MP95) considered the case where Alice identically prepares the spins of a finite number, N, of spin-1/2 systems along a direction, $\mathbf{n}$, chosen uniformly at random [46]. Using the fidelity $\cos\left(\frac{\theta}{2}\right)$, where θ is the angle between Bob's guess of the direction of the spins and the true direction of the spins, MP95 showed that the measurement that optimizes the average fidelity is a joint measurement on the N systems. However, MP95's measurement is a continuously parametrized POVM that can not be physically realized. A physically realizable measurement that achieves the optimal average fidelity of MP95 was shown in [47]. Furthermore, it was shown that the physically realizable measurement of [47] also optimizes the average information gain [48].

Surprisingly, it turns out that identically preparing the spins of N spin-1/2 systems is not the best strategy for Alice and Bob to align their directional reference frames. Gisin and Popescu (GP99) showed that if Alice only has two spin-1/2 systems anti-parallel spins achieve a much higher average fidelity that parallel spins [49]. Subsequently, Bagan et al. (BBBM00), showed that the average fidelity of estimation in aligning a directional reference frame using N spin-1/2 systems is maximized if the N spins are prepared in an eigenstate of $J_{\mathbf{n}}$, the component of the total angular momentum of N spins pointing along the direction $\mathbf{n}$ of Alice's directional frame. Such a state achieves an average fidelity that approaches unity as $(1/N)^2$ in the limit $N \to \infty$, whereas a product state of N spin-1/2 systems achieves an average fidelity of $1/N$ as $N \to \infty$. Moreover, Massar showed that the state of the bounded-sized token that optimizes the average function $f(g, g')$ explicitly depends on the choice of function [50]. In addition, Chiribella et al. (CDS05) showed that the covariant measurements that optimize any function $f(g, g')$, satisfying

$f(hg, hg') = f(g, g')$, $\forall\, h, g, g' \in G$, depend on the *representation*, T, of the symmetry group G associated with the lack of a shared frame of reference [51].

Alignment of a full Cartesian reference frame, i.e. an orthogonal triplet of axis, was studied by Peres and Scudo (PS01) [52] and Bagan et al. (BBM01) [53]. PS01 showed how the alignment of a Cartesian frame of reference can be performed using a single atom of hydrogen in a Coulomb potential, whereas BBM01 used N spin-1/2 systems and showed that the average error in the estimation of a full Cartesian frame of reference approaches unity as $1/N$ in the limit $N \to \infty$.

A different approach to the problem of aligning a Cartesian frame of reference was given by Acìn et al. (AJV01) [54]. As AJV01 showed, and as I explain in chapter 2, the problem of Alice and Bob lacking a shared Cartesian frame of reference is equivalent to Alice and Bob sharing a collective noise channel. The latter is a channel that performs the same unitary operator, $U \in \mathrm{SU}(d)$, on every d-dimensional quantum system transmitted through it. AJV01 showed that if Alice and Bob are allowed to share entanglement then the average fidelity of aligning a full Cartesian reference frame scales quadratically with the size of the quantum system. Bagan et al. (BBM04) extended the result of AJV01 for the case where Alice and Bob use $2N$ spin-1/2 systems, prepared initially in an entangled state, to transmit a Cartesian frame of reference [55]. BBM04 showed that the average fidelity per axis scales as $(1/N)^2$ in the limit $N \to \infty$.

AJV01's results imply that the average fidelity of estimation of a Cartesian reference frame can be enhanced if Alice and Bob are allowed to share prior entanglement. However, Bagan et al. [56] and also Chiribella et al. [57] showed that the average fidelity and average transmission error can be made to approach unity as $(1/N)^2$, in the limit $N \to \infty$, without requiring prior shared entanglement. As Bagan et al. and Chiribella et al. show, and as I explain in chapter 2, the state of N spin-1/2 systems that maximizes the average fidelity and average transmission error is a linear superposition of entangled

states between *virtual sub-systems* [58]. The latter correspond to sub-spaces of the total Hilbert space of N spin-1/2 systems arising from the decomposition of the latter into a direct sum of super-selected sectors.

It follows from the discussion of reference frame alignment protocols that the optimal state, as quantified by the function, $f(g, g')$, allows Alice and Bob to lift the SSR associated with the lack of a shared reference frame. Hence, the optimal state in a reference frame alignment protocol is a resource. Therefore, one can define an operational measure of frameness based on a reference frame alignment protocol: the most resourceful bounded-sized token of a reference frame is the one that optimizes the average measure of success in a reference frame alignment protocol. However, due to the dependence of the optimal state on the function used to quantify the success of the protocol such an operational measure of frameness is ambiguous; it will quantify a bounded-sized token as more resourceful under one function but less resourceful under another. I will show in chapter 3 that the frameness of a bounded-sized token in a reference frame alignment protocol can be quantified using the G-asymmetry of [40], thus providing an operational interpretation for the G-asymmetry and establishing a connection between reference frame alignment and the resource theory of reference frames.

To summarize, in this section I reviewed the main results regarding two parties wishing to align their respective frames of reference. The measurements that optimize the average measure of success of a reference frame alignment protocol are covariant and depend on the unitary representation T of the group G associated with the reference frame. In addition, the optimal states depend on the function, $f(g, g')$, used to quantify the success of the alignment protocol. In the next section I review how classical and quantum communication can be achieved in the absence of a shared frame of reference.

1.4 Reference frame independent communication

In Sec. 1.3 I reviewed how the restrictions imposed by the lack of a shared frame of reference can be alleviated by performing a reference frame alignment protocol. However, the sender and receiver might wish for their respective reference frames to remain hidden as a party's reference frame might serve as a way of identifying themselves to some third party. Therefore, it is sometimes beneficial for Alice to communicate information to Bob in such a way so that Bob does not obtain any information about Alice's reference frame. I will refer to such communication protocols as reference frame independent communication protocols and this section reviews the main results regarding such protocols.

As pointed out by AJV01, and as I explain in chapter 2, the problem of two parties lacking a shared frame of reference is equivalent to the problem of two parties sharing a collective noise channel. Hence, communication of information in the absence of a shared frame of reference is equivalent to communication of information in the presence of a collective noise channel. Zanardi and Rasetti (ZR97) showed that collective noise channels allow for the construction of *error-avoiding*, or equivalently reference frame independent, communication protocols [59]. In such a protocol Alice performs a *logical encoding* described by the map $\mathcal{C}$ that maps the quantum state, $|\psi\rangle \in \mathcal{H}^{\otimes m}$, she wishes to transmit to a larger space $\mathcal{H}^{\otimes N}$, where $N > m$, known as the *code space*. Alice transmits the physical systems that comprise the code space through the channel to Bob who recovers the message, $|\psi\rangle \in \mathcal{H}^{\otimes m}$, by performing a *logical decoding* described by a map $\mathcal{D}$ that maps the code space $\mathcal{H}^{\otimes N}$ back to $\mathcal{H}_d^{\otimes m}$ (see Fig. 1.1). ZR97 showed that there exist sub-spaces of the code space that are not affected by the noise of the channel and can be used to transmit quantum information. Such sub-spaces are referred to as decoherence-free sub-spaces or DFS for short.

Subsequent work by Knill et al. (KLV00) gave rise to another type of reference frame

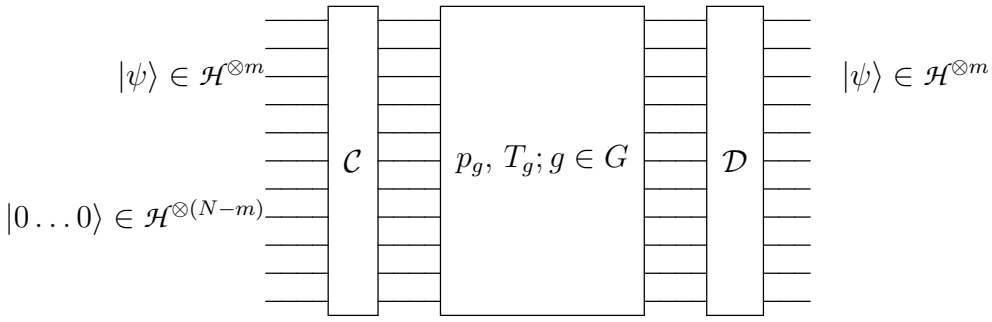

Figure 1.1: Encoding and decoding of quantum information in a reference frame independent protocol. Alice encodes her message $|\psi\rangle \in \mathcal{H}^{\otimes m}$ using $(N-m)$, auxiliary quantum systems by performing the logical encoding operation $\mathcal{C} : \mathcal{H}^{\otimes m} \rightarrow \mathcal{H}^{\otimes N}$. The channel acts collectively on all N systems with the same operation T_g, with some probability p_g. Bob performs the decoding operation, $\mathcal{D} : \mathcal{H}^{\otimes N} \rightarrow \mathcal{H}^{\otimes m}$, and recovers the Alice's message.

independent encoding using *decoherence-free sub-systems*, referred to as *noiseless subsystems*) or NS for short [60]. The difference between NS and DFS is rather subtle and is explained in more detail in chapter 2. KLV00 showed that NS are equivalent to an error-correcting code with infinite distance, i.e. an error correcting code that can correct for an arbitrary error. These NS were studied further by Zanardi, and were shown to arise from the representation of the noise operators of the collective noise channel [58, 61]. An experimental realization of NS using three spin-1/2 systems was proposed in [62] and [63] where explicit encoding and decoding circuits where provided.

To illustrate how information can be transmitted using a DFS/NS consider two parties that share a collective dephasing cannel associated with the lack of a shared phase reference. Suppose that Alice uses two photons prepared in the state

$$|\psi\rangle = \alpha|01\rangle + \beta|10\rangle, \tag{1.2}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. The state in Eq. (1.2) is an eigenstate of the total photon-number operator and belongs to the two-dimensional DFS spanned by $\{|01\rangle, |10\rangle\}$. Hence, Alice can use two photons to transmit one *logical qubit* by choosing the parameters α and β appropriately.

In the above example the *rate of transmission* of quantum information is 1/2. That is two physical qubits are required in order to transmit one logical qubit through the collective dephasing channel. Ideally we would like to construct codes with a high rate of transmission. It was shown by Lidar et al. (LCW98) [64] and Kempe et al. (KBLW01) [65] that in the limit where a large number of physical qubits are available to Alice the rate of transmission of quantum information using a DFS/NS code approaches unity. Furthermore, LCW98 and KBLW01 established necessary and sufficient conditions for the existence of DFS and NS respectively and showed that universal quantum computation can be performed within a DFS/NS[2]. The construction of DFS/NS as well as how to achieve universal control using *qudits* was shown by Byrd [66] and Bishop and Byrd [67] respectively.

In addition to constructing codes with high transmission rates it is also desirable to construct codes whose encoding and decoding maps, $\mathcal{C}$, $\mathcal{D}$, can be efficiently implemented. An efficient implementation of the maps $\mathcal{C}$, $\mathcal{D}$ was provided by Bacon et al. (BCH) [68, 69]. Specifically, BCH constructed a quantum circuit for encoding and decoding information in a DFS/NS and determined the number of single and two-qubit gates (henceforth referred to as elementary gates) that are required in order to encode and decode logical quantum information in a DFS/NS. BCH showed that, up to an arbitrary error ϵ, the number of elementary gates required to construct a DFS/NS using N d-dimensional quantum systems scales as $N\text{poly}(\log_2 N, d, \epsilon)$.

The results thus far indicate that reference frame independent communication is pos-

[2]A set of logical gates is called *universal* if any possible computation can be reduced to a sequence involving gates from the universal set.

sible using DFS/NS. How to perform such a reference frame independent communication in the case where parties lack a shared Cartesian frame of reference was first shown by Bartlett et al. (BRS03) [70]. Specifically, BRS03 showed that if Alice uses an asymptotically large number of spin-1/2 systems she can transmit one classical bit, or one logical qubit, per physical system sent to Bob. Indeed, it was shown that Alice and Bob can communicate even entangled quantum states and can perform a Bell inequality test [71], and quantum key distribution [72, 73, 74] in the absence of a shared frame of reference. As most implementations of quantum communication protocols use photons as information carriers, a complete description of how to implement DFS/NS schemes in the optical regime was provided by Ball and Banaszek [75, 76].

In this section I reviewed the main results relating to communication of information in the absence of a shared frame of reference. The work done in this field to date involves the use of DFS/NS codes that protect information from the noise associated with the lack of a shared frame of reference. DFS/NS codes were shown to achieve an optimal rate of transmission of information [64, 65] and the encoding and decoding circuits for such codes have been derived [68, 69]. The next section contains my contributions to the resource theory of quantum reference frames, alignment protocols, and reference frame independent communication.

1.5 My contributions

In Sec. 1.2 I reviewed the consequences of SSRs on quantum information processing tasks, how SSRs are equivalent to the lack of a requisite frame of reference for the degrees of freedom of quantum systems, and how the restrictions imposed by SSRs give rise to the resource theory of reference frames. In Sec. 1.3 I reviewed how a bounded-sized token of a party's frame of reference can be used in a reference-frame alignment protocol to

alleviate, at least partially, the restrictions imposed by the lack of a shared frame of reference.

In all reference frame alignment protocols reviewed in Sec. 1.3 the success of alignment was quantified by a function, $f(g, g')$, that depends solely on the relation between the orientation of Alice's frame of reference, $g \in G$, and Bob's guess of Alice's reference frame, $g' \in G$. The bounded-sized token that optimizes the success of the alignment protocol explicitly depends on the function $f(g, g')$. In chapter 3 I examine reference-frame alignment using the *accessible information*, the maximum amount of information that Bob can obtain given a bounded-size token of Alice's frame of reference. In addition, I determine the bounded-size token of Alice's reference frame that maximizes Bob's accessible information.

The quantification of alignment using the accessible information allows me to propose a new operational measure of frameness, the *alignment rate*, that quantifies the amount of information Bob learns per bounded-size token of Alice's frame of reference. I show that for the case of a phase reference, associated with the group $U(1)$, and for the case where the reference frame is associated with a finite cyclic group of M elements, $\mathbb{Z}_M$, the alignment rate is equal to the G-asymmetry [40]. My result provides an information theoretic, operational interpretation of the G-asymmetry that was thus far lacking in the literature, and establishes a clear connection between the resource theory of reference frames and reference-frame alignment protocols.

That the $\mathbb{Z}_M$-asymmetry is equal to the alignment rate for the case where Alice and Bob lack a shared reference frame associated with $\mathbb{Z}_M$ presented several challenges. Whereas at first sight it might seem that the rate of alignment for the case of reference frames associated with $\mathbb{Z}_M$ should follow from that of $U(1)$ (by observing that in the limit $M \to \infty$, $\mathbb{Z}_M \to U(1)$) I will show that the two cases are distinct. Remarkably, the rate of alignment for finite cyclic groups of more than three elements exhibits super-additivity,

a uniquely quantum mechanical phenomenon and the first example to my knowledge of a regularized quantity exhibits this property.

In addition, in chapter 4 I introduce a novel reference frame independent communication protocol. As I reviewed in Sec. 1.4 such protocols were shown to achieve an optimal rate of transmission of quantum information. However, the encoding and decoding circuits of all protocols reviewed in Sec. 1.4 require $N\text{poly}(\log_2 N, d, \epsilon)$ number of elementary gates in order to be implemented. I show that for the case where Alice and Bob lack a shared frame of reference associated with a finite group, G, the number of elementary gates required to implement my protocol is strictly less than those of [68, 69].

The circuit implementation for the encoding and decoding operations of my protocol presented several challenges. In particular, the encoding of logical quantum information using my protocol requires creating entanglement between the logical qubits and r auxiliary qubits such that the $m+r$ qubit state lies in a DFS. For certain groups the required number of elementary gates was significantly reduced by exploiting the structure of the group. As a result the number of gates that need to be implemented per logical qubit encoded is constant. It is just as easy to encode one logical qubit as it is to encode one thousand logical qubits using my protocol. To my knowledge no DFS protocol to date shares the above mentioned property.

Chapter 2

Preliminaries

In this chapter I introduce the mathematical background required in the study of communication of information using quantum mechanical systems between parties that lack a shared frame of reference. This chapter is organized as follows: Sec. 2.1 introduces the elements of quantum theory needed for this thesis, and Sec. 2.2 introduces representation theory in the context of quantum reference frames for finite and compact Lie groups. Readers familiar with either or both quantum theory and representation theory should skip ahead to Sec. 2.3 where I provide a formal treatment of the restrictions imposed by SSRs and the lack of a shared frame of reference. Finally, Sec. 2.4 outlines how two parties can communicate classical (Sec. 2.4.1) and quantum information (Sec. 2.4.2) in the absence of a shared frame of reference, as well as how parties can use bounded-sized tokens to align their respective reference frames (Sec. 2.4.3).

2.1 Quantum Information Theory

Quantum information theory deals with the representation, manipulation, and storage of information represented in the degrees of freedom of quantum mechanical systems. This section provides an overview of the quantum state formalism of quantum systems (Sec. 2.1.1), their manipulation (Sec. 2.1.2) and measurement (Sec. 2.1.3), as well as their composition (Sec. 2.1.4).

2.1.1 The quantum state

All the information known about a quantum system, i.e. the probability outcomes of any conceivable measurement on the quantum system, is contained in the *quantum state* of

the system. The quantum state of a system may be represented by a normalized vector in a Hilbert space, $\mathcal{H}$, a complex vector space equipped with an inner product that is complete in its norm. I will use Dirac notation [8] and denote the state of a quantum system as $|\psi\rangle \in \mathcal{H}$.

A quantum system whose state is represented by a normalized vector, $|\psi\rangle \in \mathcal{H}$, is said to be in a *pure state*. Equivalently, a quantum system known to be in a pure state can be described by a *density matrix* $\rho \in \mathcal{B}(\mathcal{H})$, a rank-one, bounded, positive semi-definite operator with unit trace. I will write the density matrix corresponding to a quantum system in a pure state $|\psi\rangle \in \mathcal{H}$ as $\rho = |\psi\rangle\langle\psi|$, where $\langle\psi|$ is the conjugate transpose of $|\psi\rangle$.

The density matrix is particularly convenient in describing a quantum system that is known to be in an *ensemble of states* ρ_i with probability p_i. The state representing such a quantum system is given by

$$\rho = \sum_i p_i \rho_i \tag{2.1}$$

and has rank strictly greater than one.

2.1.2 State evolution

The state of a quantum system describes more than just its internal degrees of freedom; it also describes the system's relation to an external frame of reference [9, 22]. For example, the direction of an electron's spin is defined relative to an external reference frame for direction such as a magnetic field or a gyroscope. The state of a quantum system can be transformed such that the quantum system holds a different relationship to the external frame of reference by performing an appropriate operation on the quantum system, i.e. by rotating the spin of the electron.

The transformation of the state of a quantum system is mathematically described by

a *quantum operation*, $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, satisfying the following three properties:

1. For any state $\rho \in \mathcal{B}(\mathcal{H})$, $0 \leq \mathrm{tr}\left(\mathcal{E}(\rho)\right) \leq 1$, where $\mathrm{tr}(\cdot)$ denotes the trace operation;

2. For arbitrary probabilities p_i, $\mathcal{E}\left(\sum_i p_i\rho_i\right) = \sum_i p_i\mathcal{E}(\rho_i)$;

3. $\mathcal{E}$ is a *completely positive map*. For any positive operator A, $(\mathcal{I} \otimes \mathcal{E})(A)$ is a positive operator where $\mathcal{I}$ is the identity operation acting on an ancillary system and $\otimes$ denotes the tensor product operation.

Any quantum operation satisfying the above three properties can be decomposed into a set of elements $\{K_i : \mathcal{H} \to \mathcal{H};\, i \in (1, \ldots, N)\}$, known as the *operator elements* of $\mathcal{E}$, such that [77]

$$\mathcal{E}(\rho) = \sum_{i=0}^{N} K_i \rho K_i^\dagger. \tag{2.2}$$

Furthermore, a quantum operation is called *trace-preserving* if

$$\sum_{i=0}^{n} K_i^\dagger K_i = \mathbb{1} \tag{2.3}$$

and *trace non-increasing* if

$$\sum_{i=0}^{n} K^\dagger K_i \leq \mathbb{1}. \tag{2.4}$$

If the inequality in Eq. (2.4) is strict then the operation is *trace-decreasing*.

Two common types of quantum operations are unitary and noisy quantum operations. A *unitary operation* is described by a quantum operation with a single operator element, i.e.

$$\mathcal{E}(\rho) = U\rho U^\dagger, \tag{2.5}$$

where $UU^\dagger = U^\dagger U = \mathbb{1}$. Unitary operations describe the evolution of isolated quantum systems. However, in real applications quantum systems are not isolated. The unwanted interactions between the system and its environment manifest themselves as noise. A *noisy quantum operation* is described by an ensemble of quantum operations $\{p_i, \mathcal{E}_i, i \in$

$(0, \ldots, N)\}$, where the quantum operation $\mathcal{E}_i$ is known to occur with probability p_i. If for all $i \in (1, \ldots, N)$ $\mathcal{E}_i(\cdot) = U_i(\cdot)U_i^\dagger$ then a quantum system is said to undergo *random unitary evolution* whose quantum operation is

$$\mathcal{E}(\cdot) = \sum_{i=1}^{N} p_i \, U_i(\cdot)U_i^\dagger. \tag{2.6}$$

Hence, a random unitary evolution is a noisy quantum operation whose operator elements are $\left\{\sqrt{p_i}\, U_i,\, i \in (1, \ldots, N)\right\}$. In Sec. 2.4 I will show that the lack of a shared frame of reference is mathematically described by a particular type of a noisy quantum operation.

2.1.3 Quantum Measurement

A special type of quantum operation is one that describes the process of measurement. A *measurement process* is described by a trace non-increasing quantum operation whose operator elements, referred to as *measurement operators*, are $\{M_i : \mathcal{H} \to \mathcal{H},\, i \in (1, \ldots, N);\, \sum_{i=1}^{N} M_i^\dagger M_i \leq \mathbb{1}\}$. If the state of the system prior to measurement is ρ the probability, p_i, that the measurement yields outcome i is given by

$$p_i = \mathrm{tr}\left(M_i^\dagger M_i \rho\right). \tag{2.7}$$

After the measurement the quantum system is in the state ρ_i given by

$$\rho_i = \frac{M_i \rho M_i^\dagger}{\mathrm{tr}\left(M_i^\dagger M_i \rho\right)}. \tag{2.8}$$

Two important types of quantum measurements are projective measurements and positive operator-valued measurements, or POVM for short. A *projective measurement* is described by a set of *Hermitian operators* $\left\{\Pi_i : \mathcal{H} \to \mathcal{H}, i \in (1, \ldots, N);\, \Pi_i = \Pi_i^\dagger\right\}$ that satisfy

$$\Pi_i \Pi_j = \delta_{ij} \, \Pi_i. \tag{2.9}$$

Any measurable quantity, such as the direction of an electron's spin or its total angular momentum, corresponds to Hermitian operator and vice versa [8]. Using the spectral

decomposition of Hermitian operators any measurable quantity, M, can be written as

$$M = \sum_i iP_i, \tag{2.10}$$

where $\{i\}$ denote the set of eigenvalues of M.

A second type of measurement that will feature heavily in this thesis is the POVM measurement. A POVM is described by a set of elements $\left\{E_i \equiv M_i^\dagger M_i,\, i \in (1,\ldots,N);\ \sum_{i=1}^N E_i = \mathbb{1}\right\}$ called the *POVM elements*. POVM measurements are useful in cases, such as the reference frame alignment protocol discussed in Sec. 1.3, where one is interested only in the measurement outcomes and not on the state of the system after measurement.

2.1.4 Composite quantum systems

For many quantum information tasks several quantum systems are manipulated. The state space, $\mathcal{H}$, of a composite quantum system made of n sub-systems with corresponding state spaces $\mathcal{H}^{(i)}$ is given by the *tensor product*

$$\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \ldots \otimes \mathcal{H}^{(n)}. \tag{2.11}$$

Furthermore, if the state of each sub-system is $\rho_i \in \mathcal{B}(\mathcal{H}^{(i)})$ then the state $\rho \in \mathcal{B}(\mathcal{H})$, describing the composite quantum system, is the *tensor product*

$$\rho = \bigotimes_{i=1}^{n} \rho_i \equiv \rho_1 \otimes \rho_2 \otimes \ldots \rho_n. \tag{2.12}$$

A composite system whose state is given by the tensor product of the states of its sub-systems is known to be in a *product state*. A composite system is said to be described by a *separable state*, ρ, if the latter can be written as a convex sum of product states, i.e.

$$\rho = \sum_{k=1}^{m} p_m \bigotimes_{i=1}^{n} \rho_i^{(k)}. \tag{2.13}$$

The state of a composite system is said to be *non-seperable* if it cannot be written as a convex sum of product states.

The above discussion shows how one describes the quantum state of a composite system given that the states of its sub-systems are known. Given the state $\rho \in \mathcal{B}(\mathcal{H})$ of a composite quantum system the state of the i^{th} sub-system, $\rho_i \in \mathcal{B}(\mathcal{H}^{(i)})$, is given by the *reduced density matrix*

$$\rho_i = \text{tr}_{\neq i}(\rho), \tag{2.14}$$

where $\text{tr}_{\neq i}$ denotes the *partial trace* operation over all sub-systems except sub-system i. For example, if the composite quantum system is made of two, two-dimensional sub-systems A and B, the partial trace operation over sub-system B is defined as

$$\text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2|\text{tr}(|b_1\rangle\langle b_2|), \tag{2.15}$$

where $|a_i\rangle$ ($|b_i\rangle$) are any two vectors in the Hilbert space, $\mathcal{H}^{(A)}$ ($\mathcal{H}^{(B)}$), of A (B).

Just as in the case of a single quantum system the transformation and measurement of the state of a composite system is described by a quantum operation, $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, with operator elements $\{K_m : \mathcal{H} \to \mathcal{H}, m \in (0, \ldots, N)\}$. A quantum operation is *separable* if its operator elements can be written as a tensor product of operator elements on each of the n sub-systems,

$$K_m = \bigotimes_{i=1}^{n} K_{m_i}, \tag{2.16}$$

where K_{m_i} denotes the operator element acting on subsystem i. A quantum operation whose operator elements cannot be written as a tensor product of operator elements on the individual sub-systems is called a *non-separable* operation.

2.2 Group representation theory

In this section I introduce the elements of group representation theory that are relevant to my thesis. Particularly, in Sec. 2.2.1 I show that the set of transformations of a reference frame for a particular degree of freedom of a quantum system form a unitary representation of a group. In Sec. 2.2.2 I define unitary and irreducible representations of finite and

compact Lie groups and in Sec. 2.2.3 I show how a representation can be reduced into its irreducible components by making use of the orthogonality relations between inequivalent irreducible representations. Finally, Sec. 2.2.4 introduces the regular representation of a group that will be used in chapter 4 and outlines some of its properties.

2.2.1 Group of transformations of a reference frame

In Sec. 2.1 I argued that the state of a quantum system describes both its internal degrees of freedom as well as its relationship to an external frame of reference relative to which the degrees of freedom of the quantum system are described. For example, when one describes the spin degree of freedom of an electron as pointing in some direction $\mathbf{n}$ then this direction is defined relative to an external directional reference frame.

Consequently, any transformation of the state of a quantum system is also defined relative to an external frame of reference. An *active transformation* changes the degrees of freedom of a quantum system leaving the external frame of reference unchanged, whereas a *passive transformation* changes the orientation of the external frame of reference leaving the degrees of freedom of a quantum system fixed.

The set of all possible transformations of a reference frame form a group as I now explain. Let G denote the set of all possible transformations of the reference frame, and for any two elements $g_1, g_2 \in G$ let $g_1 \cdot g_2$ denote their composition. Clearly the identity operation, e, associated with leaving the reference frame unchanged belongs to G. Furthermore, any two transformations applied consecutively give rise to another valid transformation; i.e. for g_1, $g_2 \in G$, $g_1 \cdot g_2 \in G$ and $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for all g_1, g_2, $g_3 \in G$. Moreover, for any transformation, $g_1 \in G$, there exists another transformation, $g_1^{-1} \in G$, that undoes the action of $g_1 \in G$; i.e. $g_1 \cdot g_1^{-1} = e \in G$. A set that satisfies all of the properties mentioned above is called a group.

A *sub-group*, H, of a group G is a subset of G that is itself a group under the

composition law for G. If H is a strict sub-set of G then the size of H is strictly less than the size of G. The size of any sub-group of G is quantified by a *measure* of G. Specifically, a measure of a group G is a function $\mu : G \to \mathbb{R},\ g \mapsto \mu(g)$ such that for a sub-group $H \subseteq G$

$$\mu(H) \equiv \int_H \mathrm{d}h\, \mu(h) \leq \int_G \mathrm{d}g\, \mu(g) \equiv \mu G, \tag{2.17}$$

where I have assumed that G is a continuous group. If G is a finite group then one simply replaces the integrals in Eq. (2.17) with sums over the group elements. The measure of a group is said to be *left-invariant* if for any $g \in G$ the measure of the set $gH = \{gh;\, h \in H \in G\}$, satisfies $\mu(gH) = \mu(H)$. Similarly, the measure of a group is said to be *right-invariant* if $\mu(Hg) = \mu(H)$ for any $g \in G$. The measure of a group is said to be *invariant* if it is both right-invariant and left-invariant. If the group G is either finite or a compact Lie group then it possess a unique, up to a multiplicative constant, invariant measure known as the *Haar measure* [78]. I will denote the Haar measure of a compact Lie group as $\mathrm{d}g$, whereas the Haar measure of a finite group is given by $\frac{1}{|G|}$ where $|G|$ is the order of the group.

2.2.2 Representations of groups

In the previous section I showed that the set of passive transformations of a reference frame form a group. As transformations are described by unitary operators in quantum theory the action of the group G, associated with a reference frame, on the state space of a quantum system is represented by a set of unitary transformations $\{T_g,\, g \in G\}$. A *representation* $T : G \to \mathrm{GL}(\mathcal{H})$ of a group G acting on the Hilbert space $\mathcal{H}$ is a homomorphism between G and $\mathrm{GL}(\mathcal{H})$, the general linear group of $\dim(\mathcal{H}) \times \dim(\mathcal{H})$ matrices over the complex numbers[1]. A *unitary presentation* $T : G \to \mathrm{GL}(\mathcal{H})$ is a

[1]In general a representation T is a homomorphism between G and $\mathrm{GL}(n, \mathbb{F})$, where $\mathbb{F}$ is a field, but as we are dealing with complex Hilbert spaces, I will only focus on the the field of complex numbers.

homomorphism between G and $\mathrm{GL}(\mathcal{H})$ that satisfies $T_{g^{-1}} = T_g^\dagger$, $\forall g \in G$.

The most fundamental representations for any group are the irreducible representations, or irreps for short. A representation $T : G \to \mathrm{GL}(\mathcal{H})$ is *reducible* if there exists a proper sub-space $\mathcal{V} \subset \mathcal{H}$ such that for any $|v\rangle \in \mathcal{V}$, $\forall g \in G$, $T_g|v\rangle \in \mathcal{V}$. The sub-space $\mathcal{V} \in \mathcal{H}$ is called a *proper invariant sub-space*. Alternatively, $T : G \to \mathrm{GL}(\mathcal{H})$ is *irreducible* if its action on $\mathcal{H}$ leaves no proper invariant sub-spaces. Two very important results regarding irreps of groups are Schur's lemmas [78].

Lemma 1 (Schur's 1st lemma)**.** *Let $T : G \to \mathrm{GL}(\mathcal{H})$ be a complex irrep and $M : \mathcal{H} \to \mathcal{H}$ a linear map such that*

$$MT_g = T_g M, \quad \forall g \in G. \tag{2.18}$$

Then

$$M = \lambda \mathbb{1}, \quad \lambda \in \mathbb{C}. \tag{2.19}$$

Lemma 2 (Schur's 2nd lemma)**.** *Let $T : G \to \mathrm{GL}(\mathcal{H}_1)$ and $U : G \to \mathrm{GL}(\mathcal{H}_2)$ be two irreps and let $M : \mathcal{H}_1 \to \mathcal{H}_2$ be a linear map such that*

$$MT_g = U_g M, \quad \forall g \in G. \tag{2.20}$$

Then either $M = 0$, i.e. $M|v\rangle = 0 \quad \forall |v\rangle \in \mathcal{H}_1$, or T and U are equivalent, i.e. $T_g = M^{-1} U_g M \quad \forall g \in G$.

A representation $T : G \to \mathrm{GL}(\mathcal{H})$ is *fully reducible* if, by a suitable choice of basis, every matrix $\{T_g,\, g \in G\}$ can be written as the *direct sum* of irreps, $T_g^{(\lambda)}$,

$$T_g \cong \bigoplus_{\lambda \in \Lambda} \alpha^{(\lambda)}\, T_g^{(\lambda)}, \tag{2.21}$$

where λ labels the inequivalent irreps of G, $\alpha^{(\lambda)} \in \mathbb{R}$ denotes the *multiplicity* of irrep $T^{(\lambda)}$, and Λ denotes the set of all inequivalent irreps of G. Consequently, the Hilbert

space upon which representation T acts can be conveniently written as

$$\mathcal{H} \cong \bigoplus_{\lambda \in \Lambda} \mathcal{H}^{(\lambda)} = \bigoplus_{\lambda \in \Lambda} \mathcal{M}^{(\lambda)} \otimes \mathcal{N}^{(\lambda)}, \tag{2.22}$$

where $\mathcal{M}^{(\lambda)}$ is the space upon which the irrep $T^{(\lambda)}$ of G acts, known as the *carrier space*, and $\mathcal{N}^{(\lambda)}$ is the space upon which the trivial (identity) representation of G acts[2], known as the *multiplicity space*. Two important results regarding unitary representations are that every finite unitary representation is fully reducible, and that every representation of a finite or compact Lie group is equivalent to a unitary representation [78]. For this reason I will only consider reference frames associated with finite or compact Lie groups.

In the next sub-section I show how a general representation $T : G \to \mathrm{GL}(\mathcal{H})$ can be reduced into inequivalent irreps using the orthogonality relations between inequivalent irreps.

2.2.3 Orthogonality relations of inequivalent irreducible representations

The inequivalent irreps of a finite or compact Lie group satisfy the following orthogonality relations [78].

Theorem 1. *Let $\{T^{(\lambda)}\}$ be a set of unitary, complex, inequivalent irreps of a compact Lie group G and let $d_\lambda = \dim(T^{(\lambda)})$. Then*

$$\int_G \mathrm{d}g\, T^{(\lambda)}_{kl}(g) T^{(\lambda')*}_{mn}(g) = \frac{1}{d_\lambda} \delta_{\lambda\lambda'} \delta_{km} \delta_{ln}, \tag{2.23}$$

where $\mathrm{d}g$ is the invariant Haar measure of G, and $T^{(\lambda')*}_{mn}(g)$ denotes the complex conjugate of $T^{(\lambda')}_{mn}(g)$.

Any result stated for compact Lie groups applies for finite groups as well by replacing $\int_G \mathrm{d}g$ by $\frac{1}{|G|}\sum_{g\in G}$. Theorem 1 provides an upper bound on the sum of the squares of

[2]The identity representation of a group G is the representation where every element $g \in G$ is represented by the identity matrix.

the dimensions of all inequivelent irreps of a finite group G as the set of $\sum_{\lambda\in\Lambda} d_\lambda^2$ vectors,

$$\mathbf{T}^{(\lambda)}_{\mathbf{kl}} \equiv \begin{pmatrix} T^{(\lambda)}_{kl}(g=g_1) \\ \vdots \\ T^{(\lambda)}_{kl}(g=|G|) \end{pmatrix}, \ \lambda\in\Lambda,\, k,l\in(1,\dots d_\lambda), \tag{2.24}$$

form an orthogonal set in the G-dimensional vector space of square integrable functions of G. As a $|G|$-dimensional vector space cannot have more than $|G|$ orthogonal vectors it follows that

$$\sum_{\lambda\in\Lambda} d_\lambda^2 \leq |G|. \tag{2.25}$$

Theorem 1 can be re-stated in terms of the characters of inequivalent irreps. The *character*, χ_g, of T_g is defined as $\chi_g \equiv \mathrm{tr}(T_g)$. It follows from the cyclic property of the trace that $\mathrm{tr}(T_h T_g T_{h^{-1}}) = \chi_g$, and hence elements in the same conjugacy class[3], $[s]$, have the same character. Defining $S \equiv \{[s]\}$ as the set of all conjugacy classes of a group the *compound character*, χ, of a representation $T : G \to \mathrm{GL}(\mathcal{H})$ is an $|S|$-dimensional vector whose entries are $\chi_{[s]}$, where $\chi_{[s]}$ is the character of conjugacy class $[s]$. Similarly, $\chi^{(\lambda)}$ denotes the $|S|$-dimensional compound character of irrep $T^{(\lambda)}$. The following theorem establishes the orthogonality relations between characters of inequivalent irreps.

Theorem 2. *The characters of the inequivalent irreps of a compact Lie group G satisfy*

$$\int_G \mathrm{d}g\, \chi^{(\lambda)}_g \chi^{(\lambda')*}_g = \delta_{\lambda\lambda'}, \tag{2.26}$$

where $\mathrm{d}g$ *is the Haar measure of G and $\chi^{(\lambda')*}_g$ denotes the complex conjugate of $\chi^{(\lambda')}_g$.*

Theorem 2 implies that the number of inequivalent irreps of a finite group is less than or equal to the number of conjugacy classes of the group as the set of $|\Lambda|$ vectors, $\{\chi^{(\lambda)},\, \lambda\in\Lambda\}$, form an orthogonal set in an $|S|$-dimensional vector space. As the latter cannot have more than $|S|$ orthogonal vectors it follows that $|\Lambda| \leq |S|$.

[3] A conjugacy class $[s]$ is defined as $[s] \equiv \{s \in G \text{ for which } \exists\, h \in G \text{ such that } s = hgh^{-1} \text{ for fixed } g \in G\}$.

In the next section I introduce the regular representation for finite and compact Lie groups and show that the regular representation contains every inequivalent irrep a number of times equal to its dimension. Using the regular representation I show that the number of inequivalent irreps of a finite or compact Lie group is equal to the number of conjugacy classes of the group.

2.2.4 The regular representation

An important representation for finite and compact Lie groups is the regular representation $\mathcal{R} : G \to \mathrm{GL}(\mathcal{H})$ of dimension $|G|$. For ease of exposition consider the case where G is a finite group, and to every element $g \in G$ associate a basis vector $|g\rangle \in \mathcal{H}$, where $\dim(\mathcal{H}) \geq |G|$. Relative to this basis the *regular representation*, $\mathcal{R} : G \to \mathrm{GL}(\mathcal{H})$, of a finite group G is a representation of G as a set of $|G| \times |G|$ matrices that map the set $\{|g\rangle \in \mathcal{H};\, g \in G\}$ into itself. It follows that the character of the regular representation satisfies

$$\mathrm{tr}(\mathcal{R}_g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise.} \end{cases} \tag{2.27}$$

Using Theorem 2 Eq. (2.27) implies

$$\frac{1}{|G|}\sum_{g\in G} \chi_g^{(\lambda)*}\,\chi = \frac{1}{|G|}\sum_{g\in G}\sum_{\lambda'\in S} \chi_g^{(\lambda)*}\alpha^{(\lambda')}\chi_g^{(\lambda')}$$
$$\chi_e^{(\lambda)*} = \sum_{\lambda'} \alpha^{(\lambda')}\delta_{\lambda\lambda'}. \tag{2.28}$$

As $\chi_e^{(\lambda')*} = \chi_e^{(\lambda')} = d_{\lambda'}$ the regular representation contains every irrep $T^{(\lambda)}$ a number of times equal to the dimension d_λ of $T^{(\lambda)}$,

$$\mathcal{R} = \bigoplus_{\lambda\in\Lambda} d_\lambda\, T_g^{(\lambda)}. \tag{2.29}$$

Eq. (2.29) implies that the equality in Eq. (2.25) holds if the set of inequivalent irreps

$\{T^{(\lambda)}\}$ is complete as

$$\chi(\mathcal{R}_e) = |G| = \sum_\lambda d_\lambda \chi_e^{(\lambda)}$$
$$= \sum_\lambda d_\lambda^2. \tag{2.30}$$

Indeed, from the discussion in Sec. 2.2.3, Eq. (2.30) implies that $|S| = |\Lambda|$; i.e. the number of inequivalent irreps of a finite group G is equal to the number of conjugacy classes of the group. The result is also true for the case of compact Lie groups.

In the next section I will apply the tools of representation theory to establish the mathematical equivalence between SSRs and the lack of a shared frame of reference.

2.3 SSRs and the lack of a shared frame of reference

In this section I provide a mathematical treatment of the operational restrictions imposed by SSRs (Sec. 2.3.1) and the restrictions imposed upon two parties lacking of a shared frame of reference (Sec. 2.3.2).

2.3.1 Formal treatment of SSRs

In non-relativistic quantum theory every observable quantity corresponds to a Hermitian operator and vice versa [8]. A SSR, as introduced by WWW52 [7], states that there exist Hermitian operators that do not correspond to measurable quantities; i.e. the set of observables, $\mathcal{O}$, is a strict sub-set of all Hermitian operators acting on the Hilbert space of a quantum system. Specifically, let $|i\rangle$, $|j\rangle \in \mathcal{H}$ be two eigenstates of the conserved quantity C corresponding to two distinct eigenvalues. A SSR for C states that for *all* observables $\mathcal{O}$,

$$\langle i|\mathcal{O}|j\rangle = 0. \tag{2.31}$$

Eq. (2.31) implies that the relative phase in a coherent superposition of eigenstates of C cannot be measured. Indeed, let $|\psi\rangle = a|i\rangle + be^{\mathrm{i}\theta}|j\rangle$ where $a, b \in \mathbb{R}$ and $\theta \in (0, 2\pi)$.

Then

$$\langle\psi|\mathcal{O}|\psi\rangle = a^2\langle i|\mathcal{O}|i\rangle + b^2\langle j|\mathcal{O}|j\rangle \tag{2.32}$$

does not depend on θ. Consequently, the state $|\psi\rangle$ is *operationally indistinguishable* from the mixed state

$$\rho = a^2|i\rangle\langle i| + b^2|j\rangle\langle j|. \tag{2.33}$$

No measurement exists that distinguishes $|\psi\rangle\langle\psi|$ from the state in Eq. (2.33). Consequently, the total Hilbert space, $\mathcal{H}$, can be conveniently written as

$$\mathcal{H} \cong \bigoplus_c \mathcal{H}^{(c)}, \tag{2.34}$$

where $\mathcal{H}^{(c)} \equiv \{|i\rangle;\, \hat{C}|i\rangle = c|i\rangle\}$ are the eigenspaces, or *charge sectors*, corresponding to the eigenvalues of the operator $\hat{C}$ associated with the conserved quantity C[4]. It follows that superpositions of eigenstates of a conserved quantity C cannot be prepared under a SSR, as one way to prepare such states is to measure an observable whose eigenstates are coherent superpositions of eigenstates of the conserved quantity C.

In addition, a SSR also imposes restrictions on the types of operations that can be performed. Specifically, the only allowed unitary transformations, U, that can be performed under a SSR are those that satisfy $[U, \hat{C}] = 0$. In the next section I show that the restrictions on the types of states and operations faced by two parties that lack a shared frame of reference are equivalent to the restrictions that arise from SSRs.

2.3.2 Formal treatment of the lack of a shared frame of reference

In this sub-section I will provide a mathematical description on the types of states Alice can prepare, as well as the types of operations that Alice can perform relative to Bob's frame of reference which she is lacking. I will show that the restrictions Alice faces due

[4]Note that the dimensions of the charge sectors, $\mathcal{H}^{(c)}$ can in general be greater than one.

to the lack of a shared frame of reference with Bob are equivalent to the restrictions Alice faces under a SSR for a conserved quantity, Λ, associated with the reference frame.

Consider two parties, Alice and Bob, who wish to communicate information represented in the degrees of freedom of quantum systems but lack a shared frame of reference relative to which the degrees of freedom of quantum systems are described. The set of all possible transformations relating Alice's and Bob's frames of reference forms a unitary representation of some symmetry group G. The knowledge Alice and Bob have about which transformation $\{T_g,\, g \in G\}$ relates their reference frames is given by the probability distribution $\{p_g\}$, a measure on the group G. If Alice and Bob are completely ignorant about the transformation relating their reference frames then $\{p_g\}$ is given by the Haar measure.

Suppose Alice prepares the degrees of freedom of a quantum system in her possession to be in a state $\rho \in \mathcal{B}(\mathcal{H})$ according to her frame of reference. As Bob has complete ignorance of Alice's reference frame the description of the quantum system relative to his frame of reference is given by the state

$$\mathcal{G}[\rho] \equiv \int_G \mathrm{d}g\, T_g \rho T_g^\dagger, \tag{2.35}$$

where $\mathcal{G}$ is the *G-twirling operation*. Note that the quantum operation of Eq. (2.35) has the form of a random unitary operation (see Eq. (2.6) of Sec. 2.1.2).

As unitary representations of finite or compact Lie groups are fully reducible there exists a basis relative to which the representation $T : G \to \mathrm{GL}(\mathcal{H})$ can be written as

$$T \cong \bigoplus_{\lambda \in \Lambda'} \alpha^{(\lambda)} T^{(\lambda)}, \tag{2.36}$$

where λ labels the d_λ-dimensional inequivalent irreps $T^{(\lambda)}$ of the group G, $\alpha^{(\lambda)}$ denotes the multiplicity of $T^{(\lambda)}$, and $\Lambda' \equiv \{\lambda \in \Lambda;\, \alpha^{(\lambda)} \neq 0\}$. Consequently, the Hilbert space $\mathcal{H}$

upon which representation T acts can be conveniently written as

$$\mathcal{H} \cong \bigoplus_{\lambda \in \Lambda'} \mathcal{H}^{(\lambda)} = \bigoplus_{\lambda \in \Lambda'} \mathcal{M}^{(\lambda)} \otimes \mathcal{N}^{(\lambda)}, \tag{2.37}$$

where $\mathcal{H}^{(\lambda)}$ are the various sectors of the Hilbert space indexed by the irrep label λ. Each sector can be written as a tensor product of two *virtual* sub-systems with corresponding state spaces $\mathcal{M}^{(\lambda)}$, $\mathcal{N}^{(\lambda)}$ [58]. The space $\mathcal{M}^{(\lambda)}$ is the d_λ-dimensional space upon which the irrep $T^{(\lambda)}$ of G acts irreducibly, and $\mathcal{N}^{(\lambda)}$ is the $\alpha^{(\lambda)}$-dimensional space upon which the trivial (identity) representation of G acts.

From the discussion above it follows that there exists a basis, $\{|\lambda, m, \beta\rangle\}$, relative to which the total Hilbert space can be written as in Eq.(2.37) where λ denotes the irrep of G, $|\lambda, m\rangle$ is an orthonormal basis of $\mathcal{M}^{(\lambda)}$, and $|\lambda, \beta\rangle$ is an orthonormal basis of $\mathcal{N}^{(\lambda)}$. In this basis the G-twirling operation of Eq. (2.35)) can be written as

$$\mathcal{G} = \sum_{\lambda \in \Lambda'} (\mathcal{D}_{\mathcal{M}^{(\lambda)}} \otimes \mathcal{I}_{\mathcal{N}^{(\lambda)}}) \circ P^{(\lambda)}, \tag{2.38}$$

where $\mathcal{D}$ is the completely depolarizing map[5],

$$\mathcal{D}(A) = \frac{\mathrm{tr}(A)}{\dim(\mathcal{H})} \mathbb{1}, \quad \forall A \in \mathcal{B}(\mathcal{H}), \tag{2.39}$$

$\mathcal{I}$ is the identity map, and

$$\mathcal{P}^{(\lambda)}(A) = \Pi_\lambda A \Pi_\lambda, \tag{2.40}$$

where Π_λ is the projector onto the space $\mathcal{H}^{(\lambda)}$ [23]. Hence, in the basis $\{|\lambda, m, \beta\rangle\}$ the effect of the G-twirling operation is to eliminate any coherence between the various sectors, $\mathcal{H}^{(\lambda)}$, of the Hilbert space.

Indeed, the state in Eq. (2.35) is a *G-invariant state*, $[\mathcal{G}[\rho], T_g] = 0$ for all $g \in G$. Thus, under the lack of a shared frame of reference with Bob, the only states Alice can prepare

[5] If the probability distribution $\{p_g\}$ is not given by the Haar measure, then $\mathcal{D}$ is given by the partially depolarizing channel.

relative to Bob's frame of reference are G-invariant states. This restriction is identical to the one faced if Alice was subject to a SSR associated with a conserved quantity Λ.

Similarly, Alice faces a restriction on the types of operations she can perform relative to Bob's frame of reference. Suppose for a moment that the transformation T_g relating Alice's and Bob's frames of reference is known. Let Bob prepare the degrees of freedom of a quantum system in the state $\rho \in \mathcal{B}(\mathcal{H})$ according to his frame of reference, send the quantum system to Alice who performs the unitary operation $\mathcal{U}[\rho] \equiv U\rho U^\dagger$ (according to her frame of reference) and returns the system back to Bob. Relative to Bob's frame of reference the resulting state of the quantum system is

$$\tilde{\mathcal{U}}[\rho] \equiv \mathcal{T}_g \circ \mathcal{U} \circ \mathcal{T}_{g^{-1}}[\rho], \tag{2.41}$$

where $\mathcal{T}_{g^{-1}}(\cdot) = T_g^\dagger(\cdot)T_g$, and $\mathcal{X} \circ \mathcal{Y}[\rho] = \mathcal{X}[\mathcal{Y}[\rho]]$. If Alice and Bob have complete ignorance about the transformation relating their frames of reference then Eq. (2.41) becomes

$$\tilde{\mathcal{U}}[\rho] = \int_G \mathrm{d}g \mathcal{T}_g \circ \mathcal{U} \circ \mathcal{T}_{g^{-1}}[\rho]. \tag{2.42}$$

Indeed, the most general quantum operation, $\mathcal{E}$, performed relative to Alice's frame of reference is described relative to Bob's frame of reference as

$$\tilde{\mathcal{E}} = \int_G \mathrm{d}g\, \mathcal{T}_g \circ \mathcal{E} \circ \mathcal{T}_{g^{-1}}. \tag{2.43}$$

The quantum operation of Eq. (2.43) is *G-invariant*; i.e. $[\tilde{\mathcal{E}}, \mathcal{T}_g] = 0$ for all $g \in G$ where $[\mathcal{X}, \mathcal{Y}] = \mathcal{X} \circ \mathcal{Y} - \mathcal{Y} \circ \mathcal{X}$. If Alice lacks a shared frame of reference with Bob the only quantum operations that Alice can implement relative to Bob's frame of reference are G-invariant operations. This is precisely the same restriction Alice faces if she is subjected to a SSR associated with the conserved quantity Λ.

In the next section I show how classical and quantum information can be communicated between two parties that lack a shared frame of reference as well as how two parties can align their respective frames of reference using quantum mechanical systems.

2.4 Communication in the absence of a shared frame of reference

In this section I describe how parties can communicate classical (Sec. 2.4.1) and quantum (Sec. 2.4.2) information in the absence of a shared frame of reference as well as how to align their respective reference frames (Sec. 2.4.3).

2.4.1 Communication of classical information in the absence of a shared frame of reference

Suppose that Alice has in her possession quantum mechanical systems and wishes to communicate a classical message to Bob with whom she lacks a shared frame of reference for the degrees of freedom of the quantum systems. As explained in Sec. 2.3.2 the lack of a shared frame of reference causes Bob to describe any quantum state, ρ, prepared by Alice as $\mathcal{G}[\rho]$ where $\mathcal{G}$ is a random unitary operation. Hence, the problem of communicating information between two parties lacking a shared frame of reference is operationally equivalent to the problem where the parties share a common frame of reference but communicate through a *collective noise channel*.

The action of a collective noise channel on the quantum state $\rho \in \mathcal{B}(\mathcal{H}^{\otimes N})$ of N quantum systems is given by

$$\mathcal{G}_N[\rho] \equiv \int_G \mathrm{d}g\, T_g^{\otimes N}[\rho] T_g^{\otimes N\,\dagger}, \tag{2.44}$$

where $T_g^{\otimes N} \equiv T_g^{(1)} \otimes \ldots \otimes T_g^{(N)}$ with $T_g^{(i)}$ denoting the action of the channel on the i^{th} quantum system. As $T : G \to \mathrm{GL}(\mathcal{H})$ is a unitary representation the collective representation $T^{\otimes N} : G \to \mathrm{GL}(\mathcal{H}^{\otimes N})$, where $\mathcal{H}^{\otimes N} \equiv \mathcal{H}^{(1)} \otimes \ldots \otimes \mathcal{H}^{(N)}$ with $\mathcal{H}^{(i)}$ the state space of the i^{th} quantum system, can be reduced into irreps as (see Eq, (2.36))

$$T^{\otimes N} \cong \bigoplus_{\lambda \in \Lambda'} \alpha^{(\lambda)}\, T^{(\lambda)}. \tag{2.45}$$

Consequently, the total Hilbert space, $\mathcal{H}^{\otimes N}$, can be conveniently written in the block diagonal basis $\{|\lambda, m, \beta\rangle\}$ as

$$\mathcal{H}^{\otimes N} \cong \bigoplus_{\lambda \in \Lambda'} \mathcal{H}^{(\lambda)} = \bigoplus_{\lambda \in \Lambda'} \mathcal{M}^{(\lambda)} \otimes \mathcal{N}^{(\lambda)}. \tag{2.46}$$

As the inequivalent sectors $\mathcal{H}^{(\lambda)}$ can be perfectly distinguished by a measurement whose operators are the projectors $\{\Pi_\lambda\}$ Alice can communicate at most $\log_2(|\Lambda'|)$ classical messages to Bob. As the number of inequivalent irreps for finite and compact Lie groups is equal to the number of conjugacy classes of the group the maximum number of classical bits that Alice can communicate is equal to $\log_2(|S|)$, where $|S|$ denotes the number of conjugacy classes of G. It follows that for the case of finite groups the rate of transmission of classical information, defined as the ratio of classical bits to physical quantum systems sent through the channel in the limit where the latter is asymptotically large, is zero.

In the case where the lack of a shared frame of reference is associated with the compact Lie groups $U(1)$ and SO(3), associated with the lack of an optical phase reference and a Cartesian frame of reference respectively, the rate of transmission of classical information was shown to approach unity in the asymptotic limit [23, 70]. In the next section, I show how Alice and Bob can communicate quantum information in the absence of a shared frame of reference.

2.4.2 Communication of quantum information in the absence of a shared frame of reference

Consider the problem where Alice and Bob lack a shared frame of reference for the degrees of freedom of a quantum system and wish to communicate quantum information. Recall that the action of the G-twirling operation in the block diagonal basis $\{|\lambda, m, \beta\rangle\}$ can be described by Eq. (2.38). As $\mathcal{G}$ acts irreducibly on $\mathcal{M}^{(\lambda)}$ the virtual sub-system

associated with this state space is a *decoherence-full sub-system*. On the other hand, the G-twirling operation acts trivially on the multiplicity space $\mathcal{N}^{(\lambda)}$ and the virtual sub-system associated with this space is a *decoherence-free* or *noiseless* sub-system (NS). The sector $\mathcal{H}^{(\lambda)}$ is a decoherence-free *sub-space* (DFS) [59] if for any state $\left|\psi^{(\lambda)}\right\rangle \in \mathcal{H}^{(\lambda)}$ and any $g \in G$

$$T_g^{(\lambda)}\left|\psi^{(\lambda)}\right\rangle = \omega^{(\lambda)}(g)\left|\psi^{(\lambda)}\right\rangle, \tag{2.47}$$

where $\omega^{(\lambda)}(g) \in \mathbb{C}$ and $|\omega^{(\lambda)}(g)||^2 = 1$, $\forall g \in G$. It follows that $\mathcal{H}^{(\lambda)}$ is a DFS if and only if the dimension of the decoherence-full sub-system is trivial.

Alice can communicate quantum information to Bob by utilizing a DFS/NS of the total Hilbert space. However, as the action of the G-twirling operation destroys coherences between the various sectors of the total Hilbert space only a single DFS/NS can be used to transmit quantum data. The maximum amount of quantum information that can be transmitted is $\log_2\left(\max_{\lambda\in\Lambda'}\dim\left(\mathcal{N}^{(\lambda)}\right)\right)$. The rate of transmission of quantum information, defined as the ratio between the number of logical qubits to physical quantum systems sent through the channel in the limit where the latter is asymptotically large, was shown to be $1 - \mathcal{O}\left(\log_2(N)/N\right)$ [65].

However, in order to transmit either classical or quantum information in the absence of a shared frame of reference Alice and Bob need to be able to perform the basis transformation, V, that maps the *tensor product basis*, $|i_1\rangle \otimes \ldots \otimes |i_N\rangle$, to the *block diagonal basis*, $|\lambda, m, \beta\rangle$. The basis transformation, V, is known as the *Schur-transform*. It was shown that the Schur transform can be implemented, up to an arbitrary error ϵ, using a number of elementary gates that grows as $N \cdot \mathrm{poly}(\log(N), d, \log(\epsilon^{-1}))$, where N is the total number of quantum systems and d is their dimension [68, 69]. In chapter 4 I will introduce an alternative protocol for transmitting information through a collective noise channel that requires fewer elementary gates in order to be implemented and achieves the same asymptotic rate of transmission of quantum information as the protocols described

in this section.

Whereas it is possible to efficiently communicate both classical and quantum information in the absence of a shared frame of reference the protocols described in this section and in Sec. 2.4.1 require that Alice and Bob have the resources to implement the Schur transform every time they wish to communicate. Furthermore, Alice and Bob still face the restrictions outlined in Sec. 2.3.2. In the next section I show how Alice and Bob can lift the restrictions imposed by the lack of a shared frame of reference by performing a reference frame alignment protocol.

2.4.3 Reference frame alignment

In this section I show how Alice and Bob can align their corresponding frames of reference. In a reference-frame alignment protocol Alice prepares N quantum systems in a state representing the orientation of her reference frame, $g \in G$, and sends them to Bob who performs a measurement on the N systems and guesses the orientation of Alice's reference frame. The success of Bob's guess, $g' \in G$, regarding Alice's reference frame is quantified by a *cost function*, $f(g, g')$.

The task is to derive the state, $|\psi\rangle \in \mathcal{H}^{\otimes N}$, that Alice should prepare and the POVM, $\{E'_g,\, g' \in G\}$, that Bob should perform in order to maximize/minimize the *average cost* [57]

$$\bar{f} = \int_G \mathrm{d}g\, p_{g'|g}\, f(g, g'), \tag{2.48}$$

where $p_{g'|g}$ is the conditional probability that Bob guesses Alice's frame of reference to be $g' \in G$ given that it is $g \in G$[6].

The cost function, $f(g, g')$, is chosen so that it satisfies some physically reasonable conditions; it should be independent of any background frame of reference and should

[6] If Bob has some knowledge about Alice's reference frame, given by the probability distribution $\{p_g\}$, then $\bar{f} = \int_G \mathrm{d}g\, p_g\, p_{g'|g}\, f(g', g)$.

only depend on the relative orientation between Alice's and Bob's frame of reference. The former condition implies that the cost function is *right-invariant*, $f(gh^{-1}, g'h^{-1}) = f(g, g')$, $\forall h \in G$, whereas the latter implies that the cost function is *left-invariant*, $f(hg, hg') = f(g, g')$, $\forall h \in G$. It was shown by Holevo [41] that for left-invariant cost functions the optimal measurement is a *covariant POVM* whose elements are of the form

$$E_g = T_g E_0 T_g^\dagger, \tag{2.49}$$

where $E_0 \equiv |e\rangle\langle e|$ is a rank-one fiducial POVM element and $T : G \to \mathrm{GL}(\mathcal{H})$. Eq. (2.49) as well as the completeness relation $\int_g \mathrm{d}g\, E_g = \mathbb{1}$ completely specify the form of $|e\rangle$ to be [57]

$$|e\rangle = \sum_{\lambda \in \Lambda'} \sqrt{d_\lambda} \sum_{n=1}^{\dim(\mathcal{N}^{(\lambda)})} \left|\xi_n^{(\lambda)}\right\rangle \otimes \left|\zeta_n^{(\lambda)}\right\rangle, \tag{2.50}$$

where $\left\{\left|\xi_n^{(\lambda)}\right\rangle\right\}$ $\left(\left\{\left|\zeta_n^{(\lambda)}\right\rangle\right\}\right)$ denotes an orthonormal basis of $\mathcal{M}^{(\lambda)}$ $\left(\mathcal{N}^{(\lambda)}\right)$. Hence, the measurement that optimizes the average cost of Eq. (2.48) is completely specified.

To determine the optimal state Alice should prepare let $|\psi(g)\rangle \equiv T_g|\psi\rangle$ be the state that represents Alice's frame of reference. Substituting

$$p(g|g') = \mathrm{tr}\left(E_{g'}|\psi(g)\rangle\langle\psi(g)|\right) \tag{2.51}$$

into Eq. (2.48) yields

$$\begin{aligned} \bar{f} &= \int_G \mathrm{d}g \int_G \mathrm{d}g'\, \mathrm{tr}\left(E_{g'}|\psi(g)\rangle\langle\psi(g)|\right) f(g, g') \\ &= \int_G \mathrm{d}g \int_G \mathrm{d}g'\, \mathrm{tr}\left(T_{g'}|e\rangle\langle e|T_{g'}^\dagger T_g|\psi\rangle\langle\psi|T_g^\dagger\right) f(g, g'). \end{aligned} \tag{2.52}$$

Using the cyclic property of the trace, the invariance of the Haar measure, and the left-invariance of $f(g, g')$ Eq. (2.52) reduces to

$$\begin{aligned} \bar{f} &= \int_G \mathrm{d}g \int_G \mathrm{d}g'\, \mathrm{tr}\left(T_{g'^{-1}g}^\dagger|e\rangle\langle e|T_{g'^{-1}g}|\psi\rangle\langle\psi|\right) f(g, g') \\ &\equiv \langle\psi|A|\psi\rangle, \end{aligned} \tag{2.53}$$

where

$$A \equiv \int_G \mathrm{d}g \int_G \mathrm{d}g' \, T^{\dagger}_{g'^{-1}g} |e\rangle\langle e| T_{g'^{-1}g} \, f(g, g'). \tag{2.54}$$

Thus, the state $|\psi\rangle \in \mathcal{H}^{\otimes N}$ that optimizes the average cost of Eq. (2.48) is the eigenstate of operator A with the maximum/minimum (depending on the cost function used) eigenvalue. The general form of $|\psi\rangle^{\otimes N}$ is

$$|\psi\rangle^{\otimes N} = \sum_{\lambda \in \Lambda'} \sum_{n=1}^{\dim\left(\mathcal{N}^{(\lambda)}\right)} a_n^{(\lambda)} \left|\xi_n^{(\lambda)}\right\rangle \otimes \left|\zeta_n^{(\lambda)}\right\rangle, \tag{2.55}$$

where the coefficients $a_n^{(\lambda)}$ depend on the choice of cost function. Notice that in general the optimal state is entangled across the sub-spaces $\mathcal{M}^{(\lambda)}$ and $\mathcal{N}^{(\lambda)}$.

The state $|\psi\rangle \in \mathcal{H}^{\otimes N}$ that optimizes the average cost of the alignment protocol is a *reference-frame resource*. However, as the optimal state depends on the cost function used to quantify the reference-frame alignment protocol a situation may arise where a particular state is deemed very resourceful under one cost function but less resourceful under another. In the next chapter I introduce a new operational measure for quantifying the success of an alignment protocol and establish a connection between reference-frame alignment and the resource theory of quantum reference frames.

Chapter 3

Information theoretic interpretation of the G-asymmetry for Abelian Groups

In this chapter I derive an operational, information-theoretic interpretation of the G-asymmetry [40] that was thus far lacking. This chapter is organized as follows. In Sec. 3.1 I show that the G-asymmetry is equivalent to the relative entropy of frameness [38] and is an upper bound to the accessible information. In Sec. 3.2 I introduce the *alignment rate* as the amount of information Bob acquires per bounded-sized token of Alice's reference frame. For the case of a phase reference, associated with the group $U(1)$ (Sec. 3.3), and reference frames associated with $\mathbb{Z}_M$ (Sec. 3.4) I show that the alignment rate is equal to the *linearized, regularized* G-asymmetry.

3.1 Relative entropy of frameness, the Holevo Bound, and the G-asymmetry

I now introduce the G-asymmetry of a state [40] and establish its connection to the Holevo bound [41] and the relative entropy of G-frameness [38]. As mentioned in Sec. 2.3.2, relative to Bob's frame of reference, Alice is restricted to preparing G-invariant states and G-invariant operations. It follows that any state that is not G-invariant is a resource. Similar to the resource theory of entanglement the resourcefulness of a state is measured by *frameness monotones* [79], or simply asymmetry measures [38, 80], that do not increase under the set of G-invariant quantum operations. One measure of the resourcefulness of

a state, $\rho \in \mathcal{B}(\mathcal{H})$, is the G-asymmetry defined as [40]

$$A_G(\rho^{\otimes N}) := S\left(\mathcal{G}_N\left[\rho^{\otimes N}\right]\right) - S(\rho^{\otimes N}), \tag{3.1}$$

where $S(\rho) \equiv -\mathrm{tr}(\rho \log \rho)$ is the von Neumann entropy [8]. The G-asymmetry is defined for all groups and for quantum systems of arbitrary dimension.

The G-asymmetry is equal to the Holevo quantity as I now show. For an ensemble of states $\left\{\mathrm{d}g,\ \left(T_g \rho T_g^\dagger\right)^{\otimes N}\right\}$ the Holevo quantity, $\chi^{(N)}$, is defined as

$$\chi^{(N)} \equiv S\left(\int_G \mathrm{d}g\ \left(T_g \rho T_g^\dagger\right)^{\otimes N}\right) - \int_G \mathrm{d}g\, S\left(\left(T_g \rho T_g^\dagger\right)^{\otimes N}\right). \tag{3.2}$$

Noting that for any unitary transformation U, $S(U\rho U^\dagger) = S(\rho)$, Eq. (3.2) yields

$$\begin{aligned}\chi^{(N)} &= S\left(\int_G \mathrm{d}g\ \left(T_g \rho T_g^\dagger\right)^{\otimes N}\right) - S(\rho^{\otimes N}) \\ &= S\left(\mathcal{G}_N[\rho]\right) - S(\rho^{\otimes N}) = A_G(\rho^{\otimes N}).\end{aligned} \tag{3.3}$$

The G-asymmetry is also equal to the relative entropy of frameness as I now show. The relative entropy of frameness, $\mathfrak{R}$, is defined as

$$\mathfrak{R} \equiv \min_{\sigma \in \mathfrak{I}} S\left(\rho||\sigma\right), \tag{3.4}$$

where $S\left(\rho||\sigma\right) = -S(\rho) - \mathrm{tr}\left(\rho \log \sigma\right)$, and $\mathfrak{I} \equiv \{\sigma |\, \mathcal{G}[\sigma] = \sigma \in \mathcal{B}(\mathcal{H}_d)\}$ is the set of invariant states. The equality between the relative entropy of frameness and the G-asymmetry follows from the observation that the G-twirling operation is both idempotent, $\mathcal{G} \circ \mathcal{G} = \mathcal{G}$[1], and unital, $\mathcal{G}[I] = I$. For such a quantum operation the following theorem holds [38].

Theorem 3. *Let $\mathcal{G}$ be a trace-preserving, completely positive map that is unital and idempotent. Then the minimum relative entropy distance between an arbitrary state $\rho \in \mathcal{B}(\mathcal{H})$ and a state $\sigma \in \mathrm{Image}(\mathcal{G})$ satisfies*

$$\min_{\sigma \in \mathfrak{I}} S\left(\rho||\sigma\right) = S\left(\mathcal{G}[\rho]\right) - S(\rho). \tag{3.5}$$

[1]More precisely a map $\mathcal{E}$ is idempotent if and only if the image of $\mathcal{E}$ is equal to the set of fix points of $\mathcal{E}$.

The relative entropy of frameness is analogous to the relative entropy of entanglement in the resource theory of LOCC. Indeed the *regularized* relative entropy of entanglement, the relative entropy of entanglement per system of an N-partite state, has an operational interpretation; it quantifies the rate of interconversion between states in a reversible theory of entanglement [43]. However, no equivalent operational interpretation for the relative entropy of frameness exists as it was shown by GMS09 that the *regularized* G-asymmetry

$$\lim_{N\to\infty} \frac{A_G(\rho^{\otimes N})}{N} = 0, \tag{3.6}$$

on all states $\rho \in \mathcal{B}(\mathcal{H})$, and for all finite and compact Lie groups [38].

In Secs. (3.3, 3.4) I will show that the relative entropy of frameness is equal to the alignment rate in a reference-frame alignment protocol which I define in the next section.

3.2 The alignment rate

Consider the reference-frame alignment protocol described in Sec. 2.4.3 and let Alice prepare a quantum system in the pure state $|\psi\rangle \in \mathcal{H}$. Bob's description of the state of Alice's system is given by $\mathcal{G}[|\psi\rangle\langle\psi|]$ (Eq. (2.35)); i.e. the pure state ensemble $\{\mathrm{d}g,\, T_g|\psi\rangle\}$ ($\{1/|G|,\, T_g|\psi\rangle\}$ in the case of a finite group). Hence, Bob's task is to determine $g \in G$.

Let X be the random variable consisting of the elements of G with uniform probability distribution given by the Haar measure. Alice sends classical information to Bob by preparing N quantum systems in the state $\rho(X)^{\otimes N} = \big(T(X)\rho T(X)^\dagger\big)^{\otimes N}$, where $\rho = |\psi\rangle\langle\psi| \in \mathcal{B}(\mathcal{H})$ is a pure state. Bob performs a positive operator valued measure (POVM) $\{E_y\}$ and obtains outcome y with probability p_y. Let Y denote the random variable associated with Bob's measurement outcome. It is natural to quantify Bob's success in determining $g \in G$ by the *accessible information*, $I^{(N)}(X : Y)$, defined as

the maximum amount of *mutual information* between random variables X and Y (see Fig. 3.1), where the maximization is performed over all of Bob's possible POVMs. The

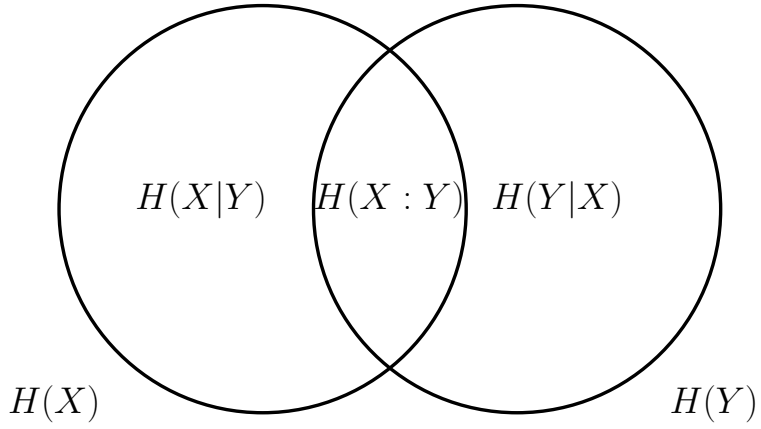

Figure 3.1: A Venn diagram representation of the relationships between various entropies. The mutual information denotes the common information between random variables X and Y and is defined as $H(X:Y) \equiv H(X) + H(Y) - H(X,Y)$.

accessible information between X and Y is known to be upper bounded by the Holevo quantity [41]. As the latter is equal to the G-asymmetry (Sec. 3.1) it follows that

$$I^{(N)}(X:Y) \leq \chi^{(N)} = A_G(\rho^{\otimes N}), \tag{3.7}$$

and the amount of accessible information per quantum system sent by Alice is

$$\frac{I^{(N)}(X:Y)}{N} \leq \frac{A_G(\rho^{\otimes N})}{N}. \tag{3.8}$$

However, the *regularized G-asymmetry*, Eq. (3.6), is zero on all states and for all finite and compact Lie groups [38] (see Eq. (3.6)). This is because the G-asymmetry is not an extensive quantity. For this reason define the *linearization function* $\mathcal{L} : \mathbb{R} \to \mathbb{R}$, a monotonically increasing function that linearizes $A_G(\rho^{\otimes N})$; that is, $\mathcal{L}$ is chosen such that $\mathcal{L}(A_G(\rho^{\otimes N})) \propto N$ in the limit $N \to \infty$ and define the *regularized, linearized G-asymmetry* as

$$A_G^{(\mathrm{reg})}(\psi) \equiv \lim_{N\to\infty} \frac{\mathcal{L}\left(A_G\left(|\psi\rangle\langle\psi|^{\otimes N}\right)\right)}{N}. \tag{3.9}$$

Similarly, the *alignment rate* of a state $|\psi\rangle \in \mathcal{H}$ is defined as

$$R_G(\psi) \equiv \lim_{N\to\infty} \frac{\mathcal{L}(I^{(N)}(X:Y))}{N}. \tag{3.10}$$

As $\mathcal{L}$ is a monotonic function the Holevo bound implies that $R_G(\psi)$ is bounded above by $A_G^{(\mathrm{reg})}(\psi)$. In the next section I will show that for the case where $G = U(1)$, associated with the important case of photon-number SSR the alignment rate is equal to the linearized, regularized $U(1)$-asymmetry.

3.3 Optimal rate for alignment of a phase reference

Let Alice and Bob share an ideal quantum channel but lack a shared phase reference. The relevant group of transformations associated with a phase reference is $U(1)$, the group of real numbers modulo 2π. Physically, Alice and Bob lack a shared phase reference if their local oscillators have an unknown relative phase, i.e. they are not phase locked. The unitary representation, T, describing a phase shift $\theta \in U(1)$ is given by $T_\theta = e^{\imath\theta\hat{N}}$, where $\hat{N}$ is the number operator. If Alice and Bob have complete ignorance as to the relative phase between their respective local oscillators then any state $\rho \in \mathcal{B}(\mathcal{H})$ prepared by Alice is described as $\mathcal{G}[\rho]$ by Bob.

As the number operator is unbounded (from above) T acts on an infinite dimensional Hilbert space $\mathcal{H}$. Using Schur's lemmas [78], the representation $T : U(1) \to \mathrm{GL}(\mathcal{H})$ can be decomposed into the one-dimensional irreps, $T_\theta^{(n)} = e^{\imath\theta n}$ of $U(1)$

$$T_\theta \cong \bigoplus_{n=0}^{\infty} \alpha^{(n)}\, T_\theta^{(n)}, \tag{3.11}$$

where the irrep label n represents the total photon number, and $\alpha^{(n)}$ is the multiplicity of irrep $T^{(n)}$. As I discussed in Sec. 2.3.2 the lack of a shared phase reference with Bob imposes a photon-number SSR on Alice [23]. Consequently, it is convenient to write the

total Hilbert space, $\mathcal{H}$, as

$$\mathcal{H} \cong \bigoplus_{n=0}^{\infty} \mathcal{H}^{(n)} = \bigoplus_{n=0}^{\infty} \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}, \tag{3.12}$$

where $\mathcal{M}^{(n)}$ carries the irrep $T^{(n)}$ and $\mathcal{N}^{(n)}$ carries the trivial representation of $U(1)$.

In addition, under a photon-number SSR Alice is restricted to $U(1)$-invariant operations that were shown in [79] to be of two types: shifts in the total photon number (by adding or removing photons), and changes in the relative amplitudes of different photon-number states. In particular, the set of $U(1)$-invariant *reversible* transformations consists of all unitary matrices that commute with the number operator and shifts in photon number.

Thus, any qudit $|\psi\rangle \in \mathcal{H}$ can be brought by $U(1)$-invariant unitary transformations and shifts to a standard form

$$|\psi\rangle = \sum_{n=0}^{d-1} \sqrt{p_n}|n\rangle, \tag{3.13}$$

where the coefficients p_n are real, $\sum_n p_n = 1$, and $|n\rangle \equiv |n, \alpha = 1\rangle$ is a state in $\mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$ chosen to be the standard one. This is because under a photon-number SSR all states $|n, \alpha\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$, for a given total photon-number n, are equivalent up to $U(1)$-invariant unitary transformations. Hence, we can pick any pure state, say $|n, \alpha = 1\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$, as our standard one.

Consider now a phase alignment protocol where Alice sends N copies of a qudit prepared in the state $|\psi\rangle$ of Eq. (3.13) to Bob. The state $|\psi\rangle^{\otimes N}$ is a superposition of the *tensor product basis* $\{|x_1 \dots x_N\rangle,\ x_1, \dots, x_N \in (0, \dots, d-1)\}$. Each such state can be written in terms of the total photon number n and its multiplicity α. That is $|n, \alpha\rangle \equiv |x_1 \dots x_N\rangle$ and $\alpha = 1, ..., l_n$, where l_n denotes the number of orthonormal states with the same photon number n. In the basis $|n, \alpha\rangle$ the state $|\psi\rangle^{\otimes N}$ can be written as

$$|\psi\rangle^{\otimes N} = \sum_{n=0}^{N(d-1)} \sum_{\alpha=1}^{l_n} \sqrt{c_{n,\alpha}}\ |n, \alpha\rangle, \tag{3.14}$$

where $c_{n,\alpha}$ are of the form $c_{n,\alpha} = \Pi_{j=0}^{d-1} p_j^{r_j}$ and r_j are positive integers (corresponding to the number of times $x_j \in (0, \ldots, d-1)$ appears in $|n, \alpha\rangle$) satisfying $\sum_j r_j = N$ and $\sum_j j r_j = n$. Moreover, by $U(1)$-invariant unitary operations the state

$$\frac{\sum_\alpha \sqrt{c_{n,\alpha}} |n, \alpha\rangle}{\sqrt{\sum_\alpha c_{n,\alpha}}} \tag{3.15}$$

can be transformed to the standard state $|n\rangle \in \mathcal{M}^{(n)} \otimes \mathcal{N}^{(n)}$. This transformation brings $|\psi\rangle^{\otimes N}$ to the form

$$|\psi\rangle^{\otimes N} = \sum_{n=0}^{N(d-1)} \sqrt{c_n}\, |n\rangle, \tag{3.16}$$

where (see [37, 79])

$$c_n = \sum \binom{N}{r_0 \ldots r_{d-1}} p_0^{r_0} \ldots p_{d-1}^{r_{d-1}} \tag{3.17}$$

are the multinomial coefficients that arise from the expansion $\left(\sum_n \sqrt{p_n} |n\rangle\right)^{\otimes N}$, where terms giving rise to the same total photon number n are grouped together. Note that the sum in Eq. (3.17) is taken over all non-negative integers r_j for which $\sum_{j=0}^{d-1} r_j = N$ and $\sum_{j=0}^{d-1} j r_j = n$.

Bob's description of the N qudits sent to him by Alice is given by

$$|\psi(\theta)\rangle^{\otimes N} = (T_\theta |\psi\rangle)^{\otimes N} = \sum_{n=0}^{N(d-1)} \sqrt{c_n}\, e^{\imath n\theta} |n\rangle. \tag{3.18}$$

Due to the lack of a shared phase reference Bob has complete ignorance about the value of θ. As the photon-number SSR does not forbid us from performing any unitary on the multiplicity spaces the state $|\psi(\theta)\rangle^{\otimes N}$ can be embedded in a $(N(d-1)+1)$-dimensional Hilbert space. This is the key reason why the $U(1)$-asymmetry is not an extensive quantity. Bob's task is, therefore, to extract information about θ from a state in an $N(d-1)+1$-dimensional Hilbert space instead of a d^N-dimensional Hilbert space.

Suppose Bob's POVM is given by $\{E_{\theta'}\, \mathrm{d}\theta'\}$, where $E_{\theta'} \geq 0$ with $\int_0^{2\pi} E_{\theta'} \mathrm{d}\theta' = \mathbb{1} = \sum_{n=0}^{N(d-1)} |n\rangle\langle n|$. How much does Bob learn about θ from such a measurement? Denote by Θ the random variable associated with the relative phase, θ, between Alice's and Bob's

phase references. That is $\Theta = \theta$ with uniform probability distribution $p_\theta = 1/2\pi$. Denote also by Θ' the random variable associated with Bob's measurement outcome θ'. Then as discussed Sec. 3.2 the accessible information, $I^{(N)}(\Theta : \Theta')$, satisfies

$$I^{(N)}(\Theta : \Theta') \leq A_{U(1)}\left((|\psi\rangle\langle\psi|)^{\otimes N}\right). \tag{3.19}$$

Using Eqs. (3.1, 3.18), the right-hand side of Eq. (3.19) is

$$\begin{aligned} A_{U(1)}\left((|\psi\rangle\langle\psi|)^{\otimes N}\right) &= S\left(\mathcal{G}\left[|\psi\rangle\langle\psi|^{\otimes N}\right]\right) - S\left(|\psi\rangle\langle\psi|^{\otimes N}\right) \\ &= S\left(\sum_{n=0}^{N(d-1)} c_n |n\rangle\langle n|\right) = H\left(\{c_n\}\right), \end{aligned} \tag{3.20}$$

where $H(\{c_n\})$ is the Shannon entropy of the probability distribution $\{c_n\}$. Consequently, the accessible information per copy of the state $|\psi\rangle \in \mathcal{H}_d$ obeys

$$\frac{I^{(N)}(\Theta : \Theta')}{N} \leq \frac{H\left(\{c_n\}\right)}{N}. \tag{3.21}$$

As I explained in Sec. 3.1 the right-hand side of Eq. (3.21) tends to zero in the limit $N \to \infty$ [38]. Indeed, so long as the photon-number spectrum is gapless, i.e. $p_n \neq 0$ for $0 < n < d-1$ [37], the probability distribution $\{c_n\}$ can be approximated, in the limit $N \to \infty$, with the normal distribution [81]

$$c_n = \frac{1}{\sqrt{2\pi\sigma_N^2}} \exp\left(-\frac{(n-\mu_N)^2}{2\sigma_N^2}\right) + O\left(\frac{1}{N}\right), \tag{3.22}$$

where

$$\begin{aligned} \sigma_N^2 &= NV(\psi) \equiv N\left(\sum_{n=0}^{d-1} n^2 p_n - \left(\sum_{n=0}^{d-1} n p_n\right)^2\right) \\ \mu_N &= N\sum_{n=0}^{d-1} n p_n, \end{aligned} \tag{3.23}$$

with $V(\psi)$ the photon-number variance of the state $|\psi\rangle$. Using Eq. (3.22) the right-hand side of Eq. (3.20) reads (see [38] for details)

$$\frac{H\left(\{c_n\}\right)}{N} = \frac{\frac{1}{2}\log(4\pi N V(\psi)) + O\left(\frac{1}{\sqrt{N}}\right)}{N}. \tag{3.24}$$

Due to the logarithmic dependence of $H(\{c_n\})$ on N the $U(1)$-asymmetry is not an extensive quantity, and as a result the limit $N \to \infty$ of Eq. (3.24) tends to zero.

Following the discussion of Sec. 3.2 introduce the linearization function, $\mathcal{L}(x) = 2^{2x}$, so that the *regularized, linearized $U(1)$-asymmetry* is given by

$$A^{(reg)}_{U(1)}(\psi) = \lim_{N\to\infty} \frac{\mathcal{L}\left(A_{U(1)}\left(|\psi\rangle\langle\psi|^{\otimes N}\right)\right)}{N} = 4\pi V(\psi). \tag{3.25}$$

Furthermore, as $\mathcal{L}(x) = 2^{2x}$ is a monotonically increasing function it follows from Eq. (3.21) that Eq. (3.25) is an upper bound for the rate of accessible information

$$\frac{\mathcal{L}(I^{(N)}(\Theta:\Theta'))}{N} \leq \frac{\mathcal{L}(A_{U(1)}\left(|\psi\rangle\langle\psi|^{\otimes N}\right)}{N}. \tag{3.26}$$

In the following theorem I show that in the limit $N \to \infty$ the inequality in Eq. (3.26) is saturated. That is, for $G = U(1)$ the alignment rate, Eq (3.10), is equal to the regularized, linearized G-asymmetry.

Theorem 4. *For $G = U(1)$*

$$R_G(\psi) = A^{(reg)}_G(\psi) = 4\pi V(\psi),$$

where $V(\psi)$ is the photon-number variance of the state $|\psi\rangle$.

Proof. Recall that the accessible information is the maximum mutual information, $H(\Theta:\Theta')$, over all possible POVMs. Let Bob's POVM elements be given by $E_{\theta'} = |e_{\theta'}\rangle\langle e_{\theta'}|$, where

$$|e_{\theta'}\rangle = \frac{1}{\sqrt{2\pi}} \sum_{n=0}^{N(d-1)} e^{in\theta'}|n\rangle. \tag{3.27}$$

Note that $\int \mathrm{d}\theta'\, E_{\theta'} = \mathbb{1}^{(N)}$, where $\mathbb{1}^{(N)} = \sum_{n=0}^{N(d-1)} |n\rangle\langle n|$. I remark that the measurement of Eq. (3.27) has been shown to be optimal if the success of the alignment protocol is quantified by a covariant cost function [56, 57]. I will show that in the limit $N \to \infty$ this measurement also maximizes $H^{(N)}(\Theta:\Theta')$ given by

$$H^{(N)}(\Theta:\Theta') = \int_0^{2\pi} \mathrm{d}\theta \int_0^{2\pi} \mathrm{d}\theta' p(\theta,\theta')\, \log\left(\frac{p(\theta,\theta')}{p(\theta')\,p(\theta)}\right), \tag{3.28}$$

where the joint probability distribution $p(\theta, \theta')$ can be calculated using Bayes' rule, $p(\theta, \theta') = p(\theta'|\theta)\, p(\theta)$. In this case

$$\begin{aligned} p(\theta) &= \frac{1}{2\pi} \\ p(\theta'|\theta) &= \left| \langle e(\theta') | \psi(\theta) \rangle^{\otimes N} \right|^2 . \end{aligned} \tag{3.29}$$

Substituting Eqs. (3.17, 3.18) into Eq. (3.29) gives

$$\begin{aligned} p(\theta'|\theta) &= \frac{1}{2\pi} \sum_{n,m=0}^{N} \sqrt{c_n c_m}\, e^{(\imath(m-n)(\theta-\theta'))} \\ &= \frac{1}{2\pi} \left| \sum_{m=0}^{N} \sqrt{c_m} e^{\imath m(\theta-\theta')} \right|^2 . \end{aligned} \tag{3.30}$$

From the equation above we see that $p(\theta'|\theta) = p(\theta|\theta')$. Therefore, the probability that $\Theta' = \theta'$ is given by

$$p(\theta') = \int_0^{2\pi} p(\theta'|\theta) p(\theta) \mathrm{d}\theta = \frac{1}{2\pi} \int_0^{2\pi} p(\theta|\theta') \mathrm{d}\theta = \frac{1}{2\pi}. \tag{3.31}$$

Hence, Eq. (3.28) reduces to

$$H^{(N)}(\Theta : \Theta') = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\theta \int_0^{2\pi} \mathrm{d}\theta' p(\theta'|\theta) \log(2\pi p(\theta'|\theta)). \tag{3.32}$$

The expression for the conditional probabilities $p(\theta'|\theta)$ can be greatly simplified. Note that the sum in Eq. (3.30) runs over positive integers. In the limit of large N the sum can be approximated by an integral over a continuous variable m. Furthermore, as μ_N is large and positive the probability distribution corresponding to small photon numbers lies at the tail end of the Gaussian distribution. Using the properties of the error function the lower limit of integration can be extended to negative photon numbers accumulating a negligible ($O(N^{-1})$) total probability. Making a change of variable, $\phi = \theta - \theta'$, and using Eq. (3.19), Eq. (3.30) becomes

$$\begin{aligned} p_\phi \equiv p(\theta|\theta') &= \frac{1}{\sqrt{2\pi\sigma_N^2}} \left| \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}}\, e^{\left(-\frac{(m-\mu_N)^2}{4\sigma_N^2}\right)} e^{\imath m\phi} \mathrm{d}m \right|^2 + O\left(\frac{1}{\sqrt{N}}\right) \\ &= \sqrt{\frac{2\sigma_N^2}{\pi}} e^{-2\phi^2\sigma_N^2} + O\left(\frac{1}{\sqrt{N}}\right). \end{aligned} \tag{3.33}$$

Using Eq. (3.33) and noting that

$$\int_0^{2\pi} \mathrm{d}\theta \int_o^{2\pi} \mathrm{d}\theta' = \int_{-2\pi}^{2\pi} \mathrm{d}\phi \int_\phi^{2\pi} \mathrm{d}\theta, \tag{3.34}$$

Eq. (3.32) reduces to

$$H^{(N)}(\Theta : \Theta') = \sqrt{\frac{2\sigma_N^2}{\pi}} \int_{-2\pi}^{2\pi} \mathrm{d}\phi e^{-2\phi^2\sigma_N^2} \times \log\left(\sqrt{8\pi\sigma_N^2}\, e^{-2\phi^2\sigma_N^2}\right) + O\left(\frac{1}{\sqrt{N}}\right). \tag{3.35}$$

I note that the mutual information does not depend on the mean photon number as expected, as the latter can be shifted using $U(1)$-invariant operations and therefore cannot carry any phase information.

Using the approximations

$$\int_{-2\pi}^{2\pi} \mathrm{d}\phi\, e^{-2\phi^2\sigma_N^2} = \int_{-\infty}^{\infty} \mathrm{d}x\, e^{-2\sigma_N^2 x^2} + O\left(\frac{1}{N}\right)$$
$$\int_{-2\pi}^{2\pi} \mathrm{d}\phi\, \phi^2\, e^{-2\phi^2\sigma_N^2} = \int_{-\infty}^{\infty} \mathrm{d}x\, x^2\, e^{-2\sigma_N^2 x^2} + O\left(\frac{1}{N}\right),$$

where the integrals on the right-hand side of Eq. (**??**) are equal to $\sqrt{\pi/2\sigma_N^2}$ and $1/2\sqrt{\pi/8\sigma_N^6}$ respectively one obtains, after simple algebra,

$$H^{(N)}(\Theta : \Theta') = \frac{1}{2}\log(4\pi\sigma_N^2) + O\left(\frac{1}{\sqrt{N}}\right). \tag{3.36}$$

Finally, linearizing the accessible information and taking the limit gives

$$\lim_{N\to\infty} \frac{\mathcal{L}(I^{(N)}(\Theta : \Theta')}{N} = \lim_{N\to\infty} \frac{2^{\log(4\pi N V(\psi))}}{N} = 4\pi V(\psi). \tag{3.37}$$

This completes the proof. □

In the next section I show that the equality between the alignment rate and linearized, regularized G-asymmetry also holds for the case where $G = \mathbb{Z}_M$.

3.4 Reference frame associated with $\mathbb{Z}_M$

Consider now the case where Alice and Bob share an ideal quantum channel but lack a shared reference frame associated with the finite cyclic group of M elements $\mathbb{Z}_M$. For

example, the case $G = \mathbb{Z}_2$ corresponds to the situation where Alice and Bob lack a reference frame for chirality [79]. In this case the optimal rate for the alignment of reference frames is not proportional to the variance even in the limit $M \to \infty$, unlike the $U(1)$-case in the previous section. This is not inconsistent with Theorem 4, as the main assumption here is that $N \gg M$. Therefore, the results obtained in this section are completely independent of the results in Sec. 3.3.

The unitary representation $T : \mathbb{Z}_M \to \mathrm{GL}(\mathcal{H})$ can be decomposed into one-dimensional irreps, $T^{(k)}$, as

$$T_g \cong \bigoplus_{k=0}^{M-1} \alpha^{(k)} T_g^{(k)}, \tag{3.38}$$

where k labels the irreps of $\mathbb{Z}_M$ and $\alpha^{(k)}$ is the multiplicity of irrep $T^{(k)}$. The lack of a shared reference frame associated with $\mathbb{Z}_M$ imposes restrictions on the type of states Alice can prepare with respect to Bob's reference frame. In order to describe these restrictions it is convenient to write the total Hilbert space, $\mathcal{H}$, as

$$\mathcal{H} \cong \bigoplus_{k=0}^{M-1} \mathcal{H}^{(k)} = \bigoplus_{k=0}^{M-1} \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}, \tag{3.39}$$

where $\mathcal{M}^{(k)}$ is the carrier space of $T^{(k)}$ and $\mathcal{N}^{(k)}$ carries the trivial representation of $\mathbb{Z}_M$. Note that unlike the case in Sec. 3.3 there are a finite number of sectors, $\mathcal{H}^{(k)}$, equal to the order of the group.

In addition to preparation of states Alice also faces restrictions on the types of operations she can perform relative to Bob's reference frame. More precisely, Alice is restricted to $\mathbb{Z}_M$-invariant operations. In the case were Alice and Bob lack a chiral frame of reference (associated with $\mathbb{Z}_2$) it was shown in [79] that $\mathbb{Z}_2$-invariant operations are of two types: shifts in the irrep label k (which in the case of chiral frames corresponds to the bit flip operation, X), and changes in the relative amplitudes of different eigenstates of irrep label k. Similarly, in the case of a $\mathbb{Z}_M$-SSR the $\mathbb{Z}_M$-invariant operations consist of shifts (mod M) in the irrep label k, and changes in the relative amplitudes of different

eigenstates of irrep label k.

Thus, any qudit $|\psi\rangle \in \mathcal{H}$ can be brought by $\mathbb{Z}_M$-invariant unitary transformations (and shifts) to a standard form

$$|\psi\rangle = \sum_{k=0}^{M-1} \sqrt{p_k}|k\rangle, \tag{3.40}$$

where the coefficients p_k are real, $\sum_k p_k = 1$, and $|k\rangle \equiv |k, \alpha = 1\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$ is a state in $\mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$ chosen to be the standard one. This is because under the $\mathbb{Z}_M$-SSR all states $|k, \alpha\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$, for a given irrep label k, are equivalent up to $\mathbb{Z}_M$-invariant unitary transformations. Hence, we can pick any pure state, say $|k, \alpha = 1\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$, as our standard one.

In the reference-frame alignment protocol considered here, where the reference frame is associated with $\mathbb{Z}_M$, Alice sends N copies of a qudit prepared in the state $|\psi\rangle$ of Eq. (3.40) to Bob. The state $|\psi\rangle^{\otimes N}$ is a superposition of the tensor product basis $\{|x_1 \dots x_N\rangle,\ x_1, \dots, x_N \in (0, \dots, d-1)\}$. Each such state can be written in terms of the irrep label k and its multiplicity α. That is $|k, \alpha\rangle \equiv |x_1 \dots x_N\rangle$ and $\alpha = 1, \dots, l_k$, where l_k denotes the number of orthonormal states with the same irrep label k. In the basis $|k, \alpha\rangle$, the state $|\psi\rangle^{\otimes N}$ can be written as

$$|\psi\rangle^{\otimes N} = \sum_{k=0}^{M-1} \sum_{\alpha=1}^{l_k} \sqrt{c_{k,\alpha}}\ |k, \alpha\rangle, \tag{3.41}$$

where $c_{k,\alpha}$ are of the form $c_{k,\alpha} = \Pi_{j=0}^{M-1} p_j^{r_j}$ and r_j are positive integers (corresponding to the number of times $x_j \in (0, \dots, d-1)$ appears in $|k, \alpha\rangle$) satisfying $\sum_j r_j = N$ and $\left(\sum_j j r_j\right)_{\mathrm{mod}\, M} = k$. Moreover, by $\mathbb{Z}_M$-invariant unitary operations the state

$$\frac{\sum_\alpha \sqrt{c_{k,\alpha}}|k, \alpha\rangle}{\sqrt{\sum_\alpha c_{k,\alpha}}} \tag{3.42}$$

can be transformed to the standard state $|k\rangle \in \mathcal{M}^{(k)} \otimes \mathcal{N}^{(k)}$. This transformation brings $|\psi\rangle^{\otimes N}$ to the form

$$|\psi\rangle^{\otimes N} = \sum_{k=0}^{M-1} \sqrt{c_k}|k\rangle, \tag{3.43}$$

where

$$c_k = \sum \binom{N}{r_0 \dots r_{M-1}} p_0^{r_0} \dots p_{M-1}^{r_{M-1}} \tag{3.44}$$

are the multinomial coefficients that arise from the expansion $\left(\sum_k \sqrt{p_k}|k\rangle\right)^{\otimes N}$, where terms giving rise to the same irrep label k are grouped together. I note that the sum in Eq. (3.44) is taken over integers r_j for which $\sum_j r_j = N$ and $\left(\sum_j j r_j\right)_{\mathrm{mod}\, M} = k$.

Note that Eq. (3.44) is similar to Eq. (3.17) in Sec. 3.3 with the important difference that $\sum_j j r_j$ is modulo M. As we are considering finite cyclic groups for which $N \gg M$, in the limit $N \to \infty$ the probability distribution $\{c_k\}$ can no longer be approximated with the normal distribution.

The coefficients c_k can also be written as

$$c_k = \sum_{m_1=0}^{M-1} \dots \sum_{m_N=0}^{M-1} \delta_{\bar{m},k} p_{m_1} \dots p_{m_N}, \tag{3.45}$$

where $\bar{m} = \sum_i m_i$. In order to simplify calculations involving the discreet probability coefficients $\{c_k\}$ the latter can be written, using the discreet Fourier transform, as

$$c_k = \frac{1}{M} \sum_{n=0}^{M-1} e^{-\frac{\imath 2\pi k n}{M}} z_n, \tag{3.46}$$

where

$$z_n \equiv \left(\sum_{m=0}^{M-1} e^{\frac{\imath 2\pi n m}{M}} p_m \right)^N \equiv (r_n e^{\imath\theta_n})^N \tag{3.47}$$

with $0 < r_n \leq 1$ and the phase $\theta_n \in [0, 2\pi)$. As $z_0 = 1$ Eq. (3.46) can be written as

$$c_k = \frac{1}{M} \left(1 + \sum_{n=1}^{M-1} e^{-\frac{\imath 2\pi k n}{M}} z_n \right) \equiv \frac{1}{M}(1 + \Delta_k), \tag{3.48}$$

where Δ_k must be real since c_k are real. Moreover, using the triangle inequality $|\Delta_k| \leq \sum_{n=1}^{M-1} |z_n|$. As $1 \leq n \leq M-1$ and $\sum_{m=0}^{M-1} p_m = 1$, where $p_m < 1$, $\forall m \in (0, \dots, M-1)$, there exists $0 < s_n < 1$ such that $|r_n e^{\imath\theta_n}| < s_n$. Therefore, $|z_n| < s_n^N$. Denoting $s_{\max} \equiv \max\{s_n\}$ it follows that $|\Delta_k| \leq (M-1) s_{\max}^N$ and in the limit $N \to \infty$ $|\Delta_k|$ goes exponentially to zero for all k which also implies that as $N \to \infty$, $c_k \to 1/M$.

Indeed the set of states

$$\left\{ T(g)|+\rangle = \frac{1}{M}\sum_{k=0}^{M-1} e^{\frac{\imath 2\pi kg}{M}}|k\rangle \;\Big|\; g = 0,\ldots,M-1 \right\}, \tag{3.49}$$

where $|+\rangle \equiv T(g=0)|+\rangle$, are optimal resources if Alice and Bob lack a shared frame of reference for $\mathbb{Z}_M$. Bob can perfectly distinguish the states in Eq. (3.49) and learn Alice's reference frame. For example, if Alice and Bob lack a chiral frame, associated with $\mathbb{Z}_2$, then the states $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ encode all the information about Alice's reference frame. If Bob detects $|+\rangle$ then he knows that his and Alice's chiral frames are aligned, else they are anti-aligned.

Bob's description of the N qudits sent to him by Alice is given by

$$|\psi(g)\rangle = (T_g|\psi\rangle)^{\otimes N} = \sum_{k=0}^{M-1} \sqrt{c_k}\, e^{\frac{\imath 2\pi kg}{M}}|k\rangle. \tag{3.50}$$

Due to the lack of a shared reference frame Bob has complete ignorance about the element $g \in \mathbb{Z}_M$. As the SSR does not forbid us from performing any unitary on the multiplicity spaces the state $|\psi(g)\rangle^{\otimes N}$ can be embedded in a M-dimensional Hilbert space. Bob's task is, therefore, to extract information about $g \in \mathbb{Z}_M$ from a state in an M-dimensional Hilbert space instead of a d^N-dimensional Hilbert space.

Suppose Bob's POVM is given by $\{E_y,\, y \in \mathbb{Z}_M\}$, where $E_y \geq 0$ with $\sum_{y\in\mathbb{Z}_M} E_y = \mathbb{1} = \sum_{k=0}^{M-1} |k\rangle\langle k|$. How much does Bob learn about $g \in \mathbb{Z}_M$ from such a measurement? Denote by X the random variable associated with the relative group element, $x \in \mathbb{Z}_M$, between Alice's and Bob's reference frames. That is $X = x$ with uniform probability distribution $p_x = 1/M$. Denote also by Y the random variable associated with Bob's measurement outcome, $y \in \mathbb{Z}_M$. Using the same reasoning as in Sec. 3.3 the accessible information per copy obeys

$$\frac{I^{(N)}_{\mathbb{Z}_M}(X:Y)}{N} \leq \frac{H\left(\{c_k\}\right)}{N}. \tag{3.51}$$

where $H(\{c_k\})$ is the Shannon entropy of the probability distribution $\{c_k\}$. Using Eq. (3.48) the latter reads

$$H\left(\{c_k\}\right) = -\frac{1}{M}\sum_{k=0}^{M-1}(1+\Delta_k)\log\left(\frac{1}{M}(1+\Delta_k)\right). \tag{3.52}$$

As Δ_k are small the Taylor expansion for the logarithm can be used. Noting that $\sum_{k=0}^{M-1}\Delta_k = 0$ Eq. (3.52) can be written as

$$H\left(\{c_k\}\right) = \log M - \frac{1}{M\ln 2}\sum_{k=0}^{M-1}\sum_{n=2}^{\infty}(-1)^n\frac{\Delta_k^n}{n(n-1)}. \tag{3.53}$$

Note that $H\left(\{c_k\}\right)$ is equal to $\log M$ with a correction that, for large N, goes exponentially to zero (recall that the Δ_k's go exponentially to zero). I now determine the dominant part of this correction.

First note that

$$\begin{aligned}
\sum_k \Delta_k^2 &= \sum_{k=0}^{M-1}\sum_{n,m=1}^{M-1} e^{\frac{\imath 2\pi k(n+m)}{M}} z_n z_m = M\sum_{n=1}^{M-1}|z_n|^2 \\
\sum_k \Delta_k^3 &= \sum_{k=0}^{M-1}\sum_{n,m,l=1}^{M-1} e^{\frac{\imath 2\pi k(n+m+l)}{M}} z_n z_m z_l \\
&= M\sum_{n,m=1}^{M-1} z_n z_m z_{M-(m+n)},
\end{aligned} \tag{3.54}$$

and similar expressions can be found for $\sum_k \Delta_k^n$ for $n > 3$. Writing the complex numbers z_n as in Eq. (3.47), Eq. (3.54) becomes

$$\begin{aligned}
\sum_k \Delta_k^2 &= M\sum_{n=1}^{M-1} r_n^{2N} \\
\sum_k \Delta_k^3 &= M\sum_{n,m=1}^{M-1}\left(r_n r_m r_{M-(m+n)}\right)^N \cos\left(N(\theta_n+\theta_m+\theta_{M-(m+n)})\right).
\end{aligned} \tag{3.55}$$

As the sums in Eq. (3.55) are over terms that are very small only the dominant terms, with the maximum value of r_n, will contribute. Define

$$Q = \{l \mid r_l = r_{\max}\} \;\; ; \;\; r_{\max} \equiv \max_{n=1,\ldots,M-1}\left|\sum_{m=0}^{M-1} e^{\frac{\imath 2\pi nm}{M}} p_m\right| \tag{3.56}$$

to be the set of all integers, l, for which the magnitude of z_l (see Eq. (3.47)) is maximum.

While the dominant terms in the first sum of Eq. (3.55) are proportional to $r_{\max}^{2N}$ the second sum is exponentially smaller than $r_{\max}^{2N}$. Similarly, for any $n > 2$ the sum $\sum_k \Delta_k^n$ is exponentially smaller than $r_{\max}^{2N}$. Therefore, Eq. (3.53) can be written as

$$H\left(\{c_k\}\right) = \log M - r_{\max}^{2N}\left(\frac{|Q|}{2\ln 2} + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right), \tag{3.57}$$

where r is some positive number smaller than $r_{\max}$ and $|Q|$ denotes the size of Q. Note that the maximum $H\left(\{c_k\}\right)$ can be is $\log M$ and this maximum is achieved if and only if $|\psi\rangle$ in Eq. (3.40) is one of the optimal resource states in Eq. (3.52). It follows that the regularized $\mathbb{Z}_M$-asymmetry goes to zero in the limit $N \to \infty$.

Just as in Sec. 3.3 the $\mathbb{Z}_M$-asymmetry is modified so that it scales linearly in N. This is achieved by defining the linearization function $\mathcal{L} : \mathcal{R} \to \mathcal{R}$ to be[2] $\mathcal{L}(x) = -\log(\log M - x)$. As this is a monotonically increasing function it follows that

$$\frac{\mathcal{L}(I^{(N)}_{\mathbb{Z}_M}(X:Y))}{N} \leq \frac{\mathcal{L}\left(A_{\mathbb{Z}_M}\left((|\psi\rangle\langle\psi|)^{\otimes N}\right)\right)}{N}. \tag{3.58}$$

In the following theorem I show that in the limit $N \to \infty$ the inequality in Eq. (3.58) is saturated.

Theorem 5. *Let* $|\psi\rangle = \sum_{k=0}^{M-1}\sqrt{p_k}|k\rangle$ *as in Eq.* (3.40). *Then for* $G = \mathbb{Z}_M$

$$R_G(\psi) = A_G^{(reg)}(\psi) = -2\log r_{\max},$$

where

$$r_{\max} = \max_{n\in\{1,2,\ldots,M-1\}}\left|\sum_{m=0}^{M-1} e^{\frac{\imath 2\pi nm}{M}} p_m\right|.$$

Proof. Let Bob's POVM elements be given by $E_y = |e_y\rangle\langle e_y|$, where

$$|e_y\rangle = \frac{1}{\sqrt{M}}\sum_{k=0}^{M-1} e^{\frac{\imath 2\pi ky}{M}}|k\rangle. \tag{3.59}$$

[2]Following the linearization introduced in [79] for the special case of $G = \mathbb{Z}_2$.

Note that $\sum_{y\in\mathbb{Z}_M} E_y = \mathbb{1} = \sum_{k=0}^{M-1} |k\rangle\langle k|$. I will show that the measurement in Eq. (3.59) maximizes $H^{(N)}(X:Y)$ given by

$$H^{(N)}(X:Y) = \sum_{x,y} p(x,y) \log\left(\frac{p(x,y)}{p(x)p(y)}\right), \tag{3.60}$$

where the joint probability distribution $p(x,y)$ can be calculated using Bayes' rule, $p(x,y) = p(y|x)p(x)$, and

$$\begin{aligned} p(x) &= \frac{1}{M} \\ p(y|x) &= |\langle e_y|\psi(x)\rangle|^2 . \end{aligned} \tag{3.61}$$

Substituting Eqs. (3.50, 3.59) into Eq. (3.61) gives

$$\begin{aligned} p(y|x) &= \frac{1}{M}\sum_{k,l=0}^{M-1} \sqrt{c_k\, c_l} e^{\frac{\imath 2\pi(k-l)(x-y)}{M}} \\ &= \frac{1}{M}\left|\sum_{k=0}^{M-1} \sqrt{c_k} e^{\frac{\imath 2\pi k(x-y)}{M}}\right|^2 . \end{aligned} \tag{3.62}$$

From the equation above we see that $p(y|x) = p(x|y)$. Therefore, the probability that $Y = y$ is given by

$$p(y) = \sum_{x=0}^{M-1} p(y|x)p(x) = \frac{1}{M}\sum_{x=0}^{M-1} p(y|x) = \frac{1}{M}. \tag{3.63}$$

Hence, Eq. (3.60) reduces to

$$H^{(N)}(X:Y) = \log M + \frac{1}{M}\sum_{x,y=0}^{M-1} p(y|x)\log(p(y|x)), \tag{3.64}$$

and using Eq. (3.48) the conditional probabilities, $p(y|x)$, maybe written as

$$p(y|x) = \frac{1}{M^2}\sum_{k,l=0}^{M-1} e^{\frac{\imath 2\pi(k-l)(x-y)}{M}} \sqrt{(1+\epsilon_{kl})}, \tag{3.65}$$

where $\epsilon_{kl} = \Delta_k + \Delta_l + 2\Delta_k\Delta_l$. As ϵ_{kl} is small and second order in Δ expanding the square root in Eq. (3.65) to second order in ϵ_{kl} gives

$$p(y|x) = \frac{1}{M^2}\sum_{k,l=0}^{M-1} e^{\frac{\imath 2\pi(k-l)(x-y)}{M}} \left(1 + \frac{1}{2}(\Delta_k + \Delta_l) - \frac{1}{8}(\Delta_k^2 + \Delta_l^2) + \frac{1}{4}\Delta_k\Delta_l\right) + O(\epsilon_{kl}^3). \tag{3.66}$$

As $p(y|x) = p(x|y)$ and $\sum_{k=0}^{M-1} \Delta_k = 0$

$$\frac{1}{4M^2} \sum_{k,l=0}^{M-1} e^{\frac{\imath 2\pi (x-y)(k-l)}{M}} \Delta_k \Delta_l = \begin{cases} 0 & \text{if } x = y \\ \frac{1}{4}|z_{x-y}|^2 & \text{if x>y} \end{cases}, \tag{3.67}$$

and Eq. (3.66) can be written, after some algebra, as

$$\begin{aligned} p(x|x) &= 1 - \frac{1}{4M} \sum_{k=0}^{M-1} \Delta_k^2 + O(\Delta_k^3) \\ p(y \neq x|x) &= \frac{1}{4}|z_{x-y}|^2. \end{aligned} \tag{3.68}$$

Using the same arguments as in Eqs. (3.53-3.56) above Eq. (3.68) can be written as

$$\begin{aligned} p(x|x) &= 1 - \frac{r_{\max}^{2N}}{4} \left(|Q| + O\left(\left(\frac{r}{r_{\max}} \right)^N \right) \right) \\ p(y \neq x|x) &= \frac{1}{4}|z_{x-y}|^2. \end{aligned} \tag{3.69}$$

I now break the mutual information, Eq. (3.64), into two terms

$$H^{(N)}(X:Y) = \log M + \frac{1}{M} \sum_{x=0}^{M-1} p(x|x) \log(p(x|x)) + \frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)). \tag{3.70}$$

Using Eq. (3.69), the approximation $(1-x)\log(1-x) = \frac{1}{\ln 2}(-x + O(x^2))$, and noting that the terms in the first sum of Eq. (3.70) are independent of x yields

$$\frac{1}{M} \sum_{x=0}^{M-1} p(x|x) \log p(x|x) = -\frac{r_{\max}^{2N}}{4 \ln 2} \left(|Q| + O\left(\left(\frac{r}{r_{\max}} \right)^N \right) \right). \tag{3.71}$$

The second sum in Eq. (3.70) reads

$$\frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)) = \frac{1}{2M} \sum_{x>y} |z_{x-y}|^2 \log\left(\frac{|z_{x-y}|^2}{4} \right). \tag{3.72}$$

Denoting $n = x - y$, and noting that $\sum_{x>y} = \sum_{n=1}^{M-1} \sum_{y=0}^{M-1-n}$, Eq. (3.72) becomes

$$\frac{2}{M} \sum_{x>y} p(y|x) \log(p(y|x)) = \frac{1}{2M} \sum_{n=1}^{M-1} (M-n)|z_n|^2 \left(\log|z_n|^2 - 2 \right). \tag{3.73}$$

Plugging Eqs. (3.71, 3.73) into Eq. (3.70) gives

$$H^{(N)}(X:Y) = \log M - \frac{r_{\max}^{2N}}{4\ln 2}\left(|Q| + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right) + \frac{1}{2M}\sum_{n=1}^{M-1}(M-n)|z_n|^2\left(\log|z_n|^2 - 2\right). \tag{3.74}$$

As only the largest $|z_n|$'s will contribute significantly to the mutual information Eq. (3.74) reduces to

$$H^{(N)}(X:Y) = \log M - r_{\max}^{2N}\left(\frac{|Q|}{4\ln 2} + \frac{1}{M}\sum_{q\in Q}(M-q) + \frac{N\log(r_{\max})}{M}\sum_{q\in Q}(M-q) + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right). \tag{3.75}$$

Denoting by $D \equiv \frac{\sum_{q\in Q}(M-q)}{M}$ Eq. (3.73) becomes

$$H^{(N)}(X:Y) = \log M - r_{\max}^{2N}\left(\frac{|Q|}{4\ln 2} + D(1 - N\log r_{\max}) + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right). \tag{3.76}$$

Finally, linearizing both the mutual information and the $\mathbb{Z}_M$-asymmetry yields

$$\begin{aligned}\mathcal{L}(A_{\mathbb{Z}_M}\left((|\psi\rangle\langle\psi|)^{\otimes N}\right) &= -\log\left(\frac{|S|}{2\ln 2} + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right) - 2N\log r_{\max},\\ \mathcal{L}(H^{(N)}(X:Y)) &= -\log\left(\frac{|S|}{4\ln 2} + D(1 - N\log r_{\max}) + O\left(\left(\frac{r}{r_{\max}}\right)^N\right)\right) - 2N\log r_{\max}.\end{aligned} \tag{3.77}$$

Dividing both quantities in Eq. (3.77) by N and taking the limit $N\to\infty$ one notes that the first term in both quantities tends to zero. Thus

$$\begin{aligned}\lim_{N\to\infty}\frac{\mathcal{L}(A_{\mathbb{Z}_M}\left((|\psi\rangle\langle\psi|)^{\otimes N}\right)}{N} &= \lim_{N\to\infty}\frac{\mathcal{L}(H^{(N)}(X:Y))}{N}\\ &= -2\log r_{\max}.\end{aligned} \tag{3.78}$$

This completes the proof. □

Thus, the alignment rate is equal to the regularized, linearized $\mathbb{Z}_M$-asymmetry.

In this chapter I introduced a new measure for quantifying the success of an alignment protocol, the alignment rate, and showed that for the case of a SSR associated with the groups $U(1)$ and $\mathbb{Z}_M$ the alignment rate is equal to the linearized regularized G-asymmetry. The results in this chapter provide an information-theoretic, operational interpretation of the G-asymmetry which was thus far lacking. In the next chapter I introduce a novel protocol for the communication of quantum information in the absence of a shared frame of reference associated with an arbitrary finite group G.

Chapter 4

Efficient quantum communication under collective noise

In this chapter I introduce a reference-frame independent protocol for communicating quantum information in the absence of a shared frame of reference. Specifically, in Sec. 4.1 I introduce a protocol for communicating quantum information in the absence of a shared frame of reference associated with an arbitrary finite group G. In Sec. 4.2 I construct the encoding and decoding circuit implementation of my protocol and discuss the required resources, i.e. the number of elementary gates, required to implement it. I show that for specific groups, such as abelian (Sec. 4.2.1) and cyclic groups (Sec. 4.2.2), the total number of elementary gates can be significantly decreased relative to the implementation of [**?**].

4.1 A novel protocol for transmitting quantum data in the absence of a shared frame of reference

Suppose Alice and Bob lack a shared frame of reference associated with a finite group G. If Alice prepares N, d-dimensional quantum systems in a state $\rho \in \mathcal{B}(\mathcal{H}_d^{\otimes N})$ then Bob's description of the state of the N systems is

$$\mathcal{E}_N[\rho] = \sum_{g \in G} p_g T_g^{\otimes N} \rho T_g^{\otimes N,\dagger}, \tag{4.1}$$

where $T^{\otimes N} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes N})$ and the probability distribution $\{p_g;\, g \in G\}$ denotes Alice's and Bob's knowledge of the element $g \in G$ relating their reference frames. As I mentioned in Sec. 2.4.1 the lack of a shared frame of reference between two parties (Eq. (4.1)) is

equivalent to the parties sharing a collective noise channel.

For an r-qudit state $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$ and a representation $T : G \to \mathrm{GL}(\mathcal{H}_d)$ define the set of states $S^{(T)}_{(r,|\psi\rangle)} \equiv \{|\psi(g)\rangle = T_g^{\otimes r}|\psi\rangle,\, g \in G\}$. I will be interested in those sets, $S^{(T)}_{(r,|\psi\rangle)}$, for which the following two conditions are fulfilled. For any pair $g,\, h \in G$, it holds that:

(1) the states $|\psi(g)\rangle,\, |\psi(h)\rangle \in S^{(U)}_{(r,|\psi\rangle)}$ are mutually orthogonal, i.e. $\langle\psi(g)|\psi(h)\rangle = \delta_{gh}$,

(2) $T_h^{\otimes r}|\psi(g)\rangle = |\psi(h \cdot g)\rangle \in S^{(T)}_{(r,|\psi\rangle)}$, where $h \cdot g$ denotes the group product between $g,\, h \in G$. In particular, the set $S^{(T)}_{(r,|\psi\rangle)}$ is closed under the action of $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes r})$.

I now show how the existence of a set of states satisfying the above two properties allows for the possibility of error-free transmission of quantum information through a collective noise channel; i.e. for a reference frame independent quantum communication.

Suppose Alice wishes to transmit a state $|\phi\rangle \in \mathcal{H}_d^{\otimes m}$ to Bob through a collective noise channel described by Eq. (4.1), and assume for now that there exists an integer r and a state $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$ such that $S^{(T)}_{(r,|\psi\rangle)}$ fulfills condition (1) and (2) above. Alice can *encode* the state $|\phi\rangle \in \mathcal{H}_d^{\otimes m}$ by preparing $m + r$ qudits in the state

$$|\chi_\phi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |\psi(g)\rangle \otimes (T_g^{\otimes m}|\phi\rangle), \tag{4.2}$$

with $|\psi(g)\rangle \in S^{(T)}_{(r,|\psi\rangle)}$. Sending the $r+m$ qudits prepared in the state of Eq. (4.2) through the channel yields

$$\begin{aligned} \left|\chi'_\phi\right\rangle &= T_h^{\otimes(r+m)}|\chi_\phi\rangle \\ &= \frac{1}{\sqrt{|G|}} \sum_{g \in G} T_h^{\otimes r}|\psi(g)\rangle \otimes (T_h T_g)^{\otimes m}|\phi\rangle), \end{aligned} \tag{4.3}$$

for some $h \in G$. As $T_h^{\otimes r}|\psi(g)\rangle = |\psi(h \cdot g)\rangle \in S^{(T)}_{(r,|\psi\rangle)}$ (condition (2)) Eq. (4.3) becomes,

using $h \cdot g = k \in G$,

$$\left|\chi'_\phi\right\rangle = \frac{1}{\sqrt{|G|}} \sum_{k \in G} |\psi(k)\rangle \otimes (T_k^{\otimes m} |\phi\rangle) = |\chi_\phi\rangle. \tag{4.4}$$

Therefore, the state of Eq. (4.2) lies in a DFS as it is invariant under the action $T_h^{\otimes(m+r)}$ for all $h \in G$ and for any probability distribution $\{p_g;\, g \in G\}$.

To decode the quantum data Bob performs the measurement described by $\{M_{g'} = |\psi(g')\rangle\langle\psi(g')| \text{ for } g' \in G,\, M_\perp = I - \sum_{g' \in G} A_{g'}\}$ on the first r qudits. Conditioned on the outcome $g' \in G$ Bob applies the unitary correction $T_{g'^{-1}}$ on all the remaining m qudits. Note that outcome $M_\perp$ has zero probability of occurring.

The protocol outlined above is an extension of the measure and re-align protocol of Bartlett et al. where Alice prepares the state $|\chi_\phi\rangle = |\psi(g)\rangle \otimes U_g^{\otimes m} |\phi\rangle$ for some $g \in G$ [82]. Unlike the measure and re-align protocol, where Bob measures the first r qudits to learn Alice's frame of reference, no information about Alice's frame of reference is obtained by measuring the first r qudits of Eq. (4.2), only about which unitary transformation is needed in order to retrieve the message.

I now show that for isomorphic representations of finite groups the set of states $S^{(T)}_{(r,|\psi\rangle)}$ can always be constructed (Theorem 7). First, I show that for an isomorphic representation $T : G \to \mathrm{GL}(\mathcal{H}_d)$ there exists a finite integer r such that $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes r})$ contains the regular representation, $\mathcal{R}$, of G as a sub-representation. Next I show that there exists an integer r and a state $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$ such that the set of states $S^{(T)}_{(r,|\psi\rangle)}$ satisfies conditions (1) and (2) above if and only if $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes r})$ contains the regular representation, $\mathcal{R}$, of G as a sub-representation.

Lemma 3. *Let $T : G \to \mathrm{GL}(\mathcal{H}_d)$ be an isomorphic representation of G. Then there exists a finite integer r such that $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes r})$ contains the regular representation, $\mathcal{R}$, as a sub-representation.*

To prove Lemma 3 I will make use of the following theorem whose proof can be found in [83].

Theorem 6. *Let $T : G \to \mathrm{GL}(\mathcal{H}_d)$ be an isomorphic representation of G. Then there exists an integer n such that $T^{\otimes n} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes n})$ contains every irrep of G at least once.*

Proof. (Lemma 3). As G is a finite group and $T : G \to \mathrm{GL}(\mathcal{H}_d)$ is isomorphic to G it follows from Theorem 6 that there exists an integer n such that $T^{\otimes n} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes n})$ contains every irrep of G at least once. Defining $\Gamma = \bigoplus_{k=1}^{|\Lambda|} T^{(k)}$, where Λ denotes the complete set of inequivalent irreps of G, it follows that

$$T^{\otimes n} \cong \Gamma \bigoplus V, \tag{4.5}$$

where V is a representation of G. Now consider the decomposition of $T^{\otimes nm} : G \to \mathrm{GL}(\mathcal{H}^{\otimes nm})$ where m is some integer. This may be written as

$$T^{\otimes nm} \cong \left(\Gamma \bigoplus V\right)^{\otimes m}. \tag{4.6}$$

If two matrices A and B are block diagonal then $A \otimes B$ is also block diagonal, and if A and B are representations of G then so is $A \otimes B$. Moreover, $A \otimes B$ is reducible so that each block of $A \otimes B$ can be reduced further into sub-blocks. Consider only the block $\Gamma^{\otimes m}$ from Eq. (4.6). This block can be written as

$$\begin{aligned}\Gamma^{\otimes m} &\cong \left(\bigoplus_{k=1}^{|\Lambda|} T^{(k)}\right) \otimes \Gamma^{\otimes m-1} \\ &= \bigoplus_{k=1}^{|\Lambda|} T^{(k)} \otimes \left(\bigoplus_{k'=1}^{|\Lambda|} T^{(k')}\right)^{\otimes m-1}.\end{aligned} \tag{4.7}$$

Each block, labeled by k, in Eq. (4.7) consists of sub-blocks given by $T^{(k)} \bigotimes_{i=1}^{m-1} T^{(\nu_i)}$, where ν_i can take any value from Λ. One such sub-block is the one where all $\nu_i = k$. If

$T^{(k)}$ is simply isomorphic to G then by Theorem 6 there exists an integer m such that $T^{(k)\otimes m} = \Gamma \bigoplus V'$, where V' is a representation of G. If $T^{(k)}$ is not isomorphic to G then $T^{(k)} \otimes \Gamma = \bigoplus_{k'} a^{(k')} T^{(k')}$, and $T^{(k)} \otimes \Gamma^{\otimes m-1} = \left(\bigoplus_{k'} a^{(k')} T^{(k')}\right) \otimes \Gamma^{\otimes m-2}$. Using the same reasoning as above it follows that for suitable integer m the block $T^{(k)} \otimes \Gamma^{\otimes m}$ will contain Γ as a sub-representation. Hence

$$\Gamma^{\otimes m} \cong \kappa\Gamma \bigoplus \Omega, \tag{4.8}$$

where $\kappa > 1$ is an integer and Ω is a representation of G. This process can be carried as far as we like increasing the multiplicity of every irrep as much as we like.

As the dimensions of all irreps are finite there exists an integer, r_k for each k, such that the irrep $T^{(k)}$ occurs at least $\dim(T^{(k)})$ times in $T^{\otimes r_k}$. Choosing $r = \max\{r_k\}$ ensures that $T^{\otimes r}$ contains the regular representation, $\mathcal{R}$, as a sub-representation. □

Using the results of Lemma 3 the existence of the set $S^{(T)}_{(r,|\psi\rangle)}$ follows directly from the next theorem.

Theorem 7. *Let $T : G \to \mathrm{GL}(\mathcal{H}_d)$. Then there exists an integer r and a state $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$ such that $S^{(T)}_{(r,|\psi\rangle)}$ satisfies both conditions (1) and (2) if and only if $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}_d^{\otimes r})$ contains the regular representation, $\mathcal{R}$, of G.*

Proof. To prove the backward implication assume that $T^{\otimes r} = \mathcal{R} \bigoplus_k \alpha^{(k)} T^{(k)}$. The total Hilbert space, $\mathcal{H}_d^{\otimes r}$, decomposes as $\mathcal{H}_d^{\otimes r} \cong \mathcal{H}_{\mathcal{R}} \bigoplus_k \mathcal{H}^{(k)}$, where $\mathcal{H}_{\mathcal{R}}$ is the Hilbert space on which the regular representation, $\mathcal{R}$, is acting. Denote by $\{|\psi(g)\rangle;\, g \in G\}$ the first $|G|$ standard basis vectors in $\mathcal{H}_d^{\otimes r}$; i.e. the computational basis of $\mathcal{H}_{\mathcal{R}}$ embedded in the d^r-dimensional Hilbert space $\mathcal{H}_d^{\otimes r}$. From the definition of the regular representation it follows that

$$T_h^{\otimes r} |\psi(g)\rangle = |\psi(h \cdot g)\rangle = |\psi(k)\rangle, \quad \forall\, h, g, k \in G. \tag{4.9}$$

Thus the set of states $\{|\psi(g)\rangle;\, g \in G\}$ satisfies properties (1) and (2).

To prove the forward implication assume that the set of states $S^{(T)}_{(r,|\psi\rangle)}$, where $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$, satisfies properties (1) and (2). Define

$$\begin{aligned} P_G &\equiv \frac{1}{|G|}\sum_{g\in G} T_g^{\otimes r}|\psi\rangle\langle\psi|T_g^{\otimes r\,\dagger} \\ &= \frac{1}{|G|}\sum_{g\in G}|\psi(g)\rangle\langle\psi(g)|. \end{aligned} \tag{4.10}$$

Then by property (2)

$$\begin{aligned} T_h^{\otimes r}\,P_G\,T_h^{\otimes r\,\dagger} &= \frac{1}{|G|}\sum_{g\in G} T_h^{\otimes r}|\psi(g)\rangle\langle\psi(g)|T_h^{\otimes r\,\dagger} \\ &= \frac{1}{|G|}\sum_{g\in G}|\psi(h\cdot g)\rangle\langle\psi(h\cdot g)| = P_G. \end{aligned} \tag{4.11}$$

It then follows form Schur's first lemma [78] that P_G is a multiple of the G-dimensional identity. Using Eq. (2.38), Eq. (4.11) may also be written as

$$P_G = \sum_k \left(\mathcal{D}_{\mathcal{M}^{(k)}} \otimes \mathcal{I}_{\mathcal{N}^{(k)}}\right)\circ\mathcal{P}^{(k)}[|\psi\rangle\langle\psi|]. \tag{4.12}$$

Write

$$|\psi\rangle = \sum_k c_k\left|\psi^{(k)}\right\rangle, \tag{4.13}$$

where $c_k \in \mathbb{C}$ satisfy $\sum_k |c_k|^2 = 1$ and $\left|\psi^{(k)}\right\rangle = \Pi_k|\psi\rangle$. Using the Schmidt decomposition and defining $\left\{\left|\xi_n^{(k)}\right\rangle\right\}$ and $\left\{\left|\zeta_n^{(k)}\right\rangle\right\}$ as orthonormal basis for $\mathcal{M}^{(k)}$ and $\mathcal{N}^{(k)}$ respectively $\left|\psi^{(k)}\right\rangle$ may be written as

$$\left|\psi^{(k)}\right\rangle = \sum_{n=1}^{\tilde{d}_k}\mu_n^{(k)}\left|\xi_n^{(k)}\right\rangle\left|\zeta_n^{(k)}\right\rangle, \tag{4.14}$$

where $\tilde{d}_k \leq \min\{d_k = \dim(\mathcal{M}^{(k)}), \dim(\mathcal{N}^{(k)})\}$ and $0 \neq \mu_n^{(k)} \in \mathbb{R}$ are the *Schmidt coefficients*. Substituting Eq. (4.14) into Eq. (4.12), and using Eq. (2.39), gives

$$P_G = \sum_\lambda |c_\lambda|^2 \sum_{n=1}^{\tilde{d}_\lambda}|\mu_n^{(\lambda)}|^2\frac{\mathbb{1}_{d_\lambda}}{d_\lambda}\otimes|\zeta_n^{(\lambda)}\rangle\langle\zeta_n^{(\lambda)}|. \tag{4.15}$$

Computing the rank on both sides of Eq. (4.15), and using the notation $\rho_{\mathcal{N}^{(k)}} = \mathrm{tr}_{\mathcal{M}^{(k)}}[|\psi^{(k)}\rangle\langle\psi^{(k)}|]$, one obtains

$$|G| = \sum_k d_k \,\mathrm{rk}\left(\rho_{\mathcal{N}^{(k)}}\right). \tag{4.16}$$

As $|G| = \sum_k d_k^2$ (see Sec. 2.2.4) and $\mathrm{rk}\left(\rho_{\mathcal{N}^{(k)}}\right) = \tilde{d}_k \leq d_k \;\forall k$ it follows that $\mathrm{rk}\left(\rho_{\mathcal{N}^{(k)}}\right) = \tilde{d}_k = d_k$. Hence, $\tilde{d}_k = \min\{d_k = \dim(\mathcal{M}^{(k)}), \dim(\mathcal{N}^{(k)})\}$ and therefore the multiplicity of each irrep, $\dim(\mathcal{N}^{(k)})$, occurs a number of times greater than or equal to its dimension d_k. Thus, $T^{\otimes r} : G \to \mathrm{GL}(\mathcal{H}^{\otimes r})$ contains the regular representation, $\mathcal{R}$, of G as a sub-representation. This completes the proof. □

Using Theorem 7 the state $|\psi\rangle \in \mathcal{H}_d^{\otimes r}$ can be chosen to be

$$|\psi\rangle = \sum_k \sqrt{\frac{d_k}{|G|}} \sum_{n=1}^{d_k} \left|\xi_n^{(k)}\right\rangle \otimes \left|\zeta_n^{(k)}\right\rangle \tag{4.17}$$

as I now show. Using the observation of Eq. (4.11) $P_G = \frac{1}{|G|}\mathbb{1}$, where $\mathbb{1}$ is the G-dimensional identity operator, and substituting Eqs. (4.13, 4.14) one obtains

$$P_G = \frac{1}{|G|}\sum_k I_{\mathcal{M}^{(k)}} \otimes I_{\mathcal{N}^{(k)}} = \sum_k |c_k|^2 \left(\mathcal{D}_{\mathcal{M}^{(k)}} \otimes \mathcal{I}_{\mathcal{N}^{(k)}}\right)\left[|\psi^{(k)}\rangle\langle\psi^{(k)}|\right]. \tag{4.18}$$

As both $\mathcal{D}$ and $\mathcal{I}$ are trace-preserving quantum operations looking at a single sector, k, and computing the trace on both $\mathcal{M}^{(k)}$ and $\mathcal{N}^{(k)}$ yields

$$\frac{1}{|G|}d_k^2 = |c_k|^2. \tag{4.19}$$

Furthermore, as $P_G^2 = \frac{1}{|G|}P_G$ and

$$P_G^2 = \sum_k |c_k|^4 \sum_n |\mu_n^{(k)}|^4 \frac{|\xi_n^{(k)}\rangle\langle\xi_n^{(k)}|}{d_k^2} \otimes |\zeta_n^{k)}\rangle\langle\zeta_n^{k)}|, \tag{4.20}$$

equating the terms of Eq. (4.20) and Eq. (4.15) yields

$$\frac{|c_\lambda|^2|\mu_n^{(\lambda)}|^2}{d_\lambda}\left(\frac{|c_\lambda|^2|\mu_n^{(\lambda)}|^2}{d_\lambda} - \frac{1}{|G|}\right) = 0. \tag{4.21}$$

Thus, using Eq. (4.19) $\mu_n^{(k)} = d_k^{-1/2}\;\forall k, n$.

In the next section I calculate the number of single and two-qubit gates required to encode quantum data using the protocol outlined in this section.

4.2 Circuit implementation of reference frame independent protocol

In this section I analyze the required resources for encoding and decoding quantum data using the protocol introduced in Sec. 4.1. In addition, I show that the number of elementary gates can be greatly reduced in the case where G is a finite abelian (Sec. 4.2.1) or cyclic group (Sec. 4.2.2). For ease of exposition I will assume throughout this section that all the physical systems are qubits and determine the number of elementary gates for the case of qudits at the end of this section.

Recall that the protocol encodes quantum information contained in an m-qubit state, $|\phi\rangle \in \mathcal{H}_2^{\otimes m}$, by preparing the state of Eq. (4.2) where $|\psi\rangle \in \mathcal{H}_2^{\otimes r}$ for finite r is given by Eq. (4.17). Note that there are $r' = \log_2|G|$ orthogonal token states that are, however, encoded into $r \geq r'$ qubits to ensure the proper behavior under the action of the collective noise channel (Eq. (4.1)). To each group element, $g \in G$, associate a computational basis vector

$$|g\rangle \equiv |i_{r'}, \ldots i_1\rangle \in \mathcal{H}_2^{\otimes r'}, \tag{4.22}$$

where $g = \sum_{k=1}^{r'} 2^{k-1} i_k$ is a binary representation of the element $g \in G$. Define the unitary operation, A, as

$$A|0\rangle^{\otimes r-r'}|g\rangle \equiv |\psi(g)\rangle, \tag{4.23}$$

i.e. a computational basis state $|g\rangle$ of r' qubits embedded into $\mathcal{H}_2^{\otimes r}$ is transformed to a state $|\psi(g)\rangle \in S^{(T)}_{(r,|\psi\rangle)}$. Thus, Eq. (4.2) can be re-written as

$$|\chi_\phi\rangle = \big(A \otimes \mathbb{1}\big)|0\rangle^{\otimes r-r'} \frac{1}{|G|} \sum_{g\in G} |g\rangle \otimes T_g^{\otimes m}|\phi\rangle. \tag{4.24}$$

The encoding of quantum information takes place in two steps. First one prepares

the $r' + m$ qubit state

$$\frac{1}{|G|}\sum_{g\in G}|g\rangle \otimes T_g^{\otimes m}|\phi\rangle, \tag{4.25}$$

followed by the r qubit operation $A \otimes \mathbb{1}$ which can be implemented using at most $\mathcal{O}(2^r)$ elementary gates. The latter is the number of gates required to implement the measure and re-align protocol of BRST09 [82][1]. In the following I concentrate on the first step, and in particular the efficient implementation of the unitary operation, W, acting on $r' + m$ qubits

$$W = \sum_{g\in G}|g\rangle\langle g| \otimes T_g^{\otimes m}. \tag{4.26}$$

To present a circuit implementation of the gate in Eq. (4.26) define the unitary operators

$$\begin{aligned} W_g &= (\mathbb{1} - |g\rangle\langle g|) \otimes \mathbb{1} + |g\rangle\langle g| \otimes T_g, \\ W_g^m &= (\mathbb{1} - |g\rangle\langle g|) \otimes \mathbb{1} + |g\rangle\langle g| \otimes T_g^{\otimes m}. \end{aligned} \tag{4.27}$$

In case $\{|g\rangle\}$ forms a complete orthonormal basis on $\mathcal{H}_2^{\otimes r'}$ (i.e. $|G| = 2^{r'}$) one obtains

$$W \equiv \prod_{g\in G} W_g^m \tag{4.28}$$

and

$$W\left(|+\rangle^{\otimes r'} \otimes |\phi\rangle\right) = \frac{1}{|G|}\sum_{g\in G}|g\rangle \otimes T_g^{\otimes m}|\phi\rangle, \tag{4.29}$$

where

$$|+\rangle^{\otimes r'} = \frac{1}{|G|}\sum_{g\in G}|g\rangle. \tag{4.30}$$

If $\{|g\rangle\}$ does not form a complete orthonormal basis, that is $|G| < 2^{r'}$, W must be applied to a state $|\Upsilon\rangle \in \mathcal{H}_2^{\otimes r'}$, that is the superposition of $|G|$ computational basis states and

[1]Note that Alice can always choose to send the state $|\psi(e)\rangle \otimes |\phi\rangle$.

does not coincide with $|+\rangle^{r'}$. Such an input state can be easily generated in the following way. Let $\tilde{r} < r'$ be such that $2^{\tilde{r}-1} < |G| < 2^{\tilde{r}}$. Then,

$$|\Upsilon\rangle = \bigotimes_{i=2}^{\tilde{r}} \left(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U_i\right) |+\rangle^{\otimes r'}. \tag{4.31}$$

Choosing U_i, acting on qubit i, either as $U_i = \mathbb{1}$ or $U_i|+\rangle = |0\rangle$ and preparing the first qubit in a state $\cos\alpha|0\rangle + \sin\alpha|1\rangle$, for some choice of α rather than $|+\rangle$, allows one to generate any desired superposition of the form $|0\rangle|+\ldots+\rangle + |1\rangle|+0\ldots0+\rangle$ with $\tilde{r}$ gates.

I will now outline a circuit implementing the gate W of Eq. (4.26), that corresponds to the sequence of controlled-unitary gates, W_g^m, for all possible values of $g \in G$. The latter can be implemented by applying local unitaries $\sigma_x^{(i_{r'})} \otimes \ldots \otimes \sigma_x^{(i_1)}$ to the first r' qubits such that

$$\sigma_x^{(i_{r'})} \otimes \ldots \otimes \sigma_x^{(i_1)} |i_{r'} \ldots i_1\rangle = |1\rangle^{\otimes r'} \tag{4.32}$$

and then applying the gate

$$V_g^m \equiv (\mathbb{1} - |1\rangle\langle 1|^{\otimes r'}) \otimes \mathbb{1} + |1\rangle\langle 1|^{\otimes r'} \otimes T_g^{\otimes m}. \tag{4.33}$$

The gate in Eq. (4.33) can be implemented by applying the gate

$$V_g = (\mathbb{1} - |1\rangle\langle 1|^{\otimes r'}) \otimes \mathbb{1} + |1\rangle\langle 1|^{\otimes r'} \otimes T_g \tag{4.34}$$

m times, where the control qubits remain the same but the target qubit is always a new one. The implementation of the gates $V_{11\ldots1}^m$ corresponding to the group element $|g\rangle = |11\ldots1\rangle$, W_g^m, and W is shown in Figs. (4.1, 4.2, 4.3) respectively.

It was shown in [84] that a control gate of the form

$$\Lambda_{r'}(U) = (\mathbb{1} - |1\rangle\langle 1|^{\otimes r'}) \otimes \mathbb{1} + |1\rangle\langle 1|^{\otimes r'} \otimes U, \tag{4.35}$$

where r' denotes the number of control qubits, can be implemented using $40(r'-2)+1$ elementary gates. In order to apply a controlled-$T_g^{\otimes m}$ gate one simply applies the m

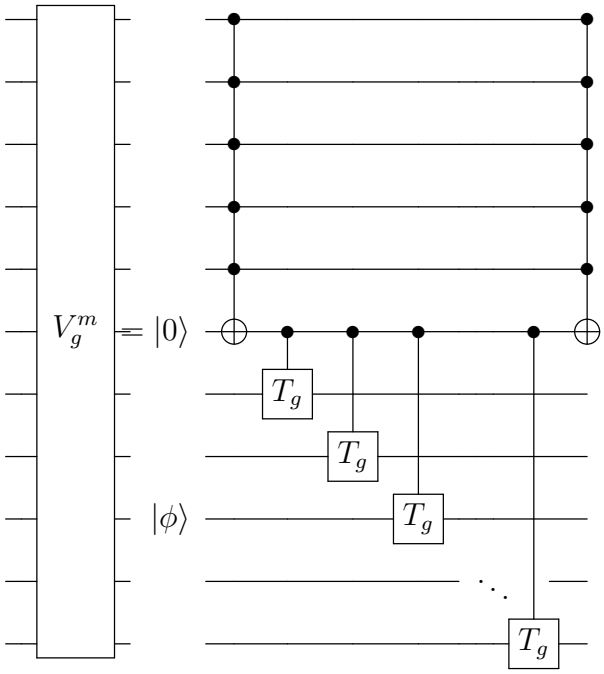

Figure 4.1: The quantum circuit implementation of the encoding operation V_g^m.

controlled-T_g gates with different target qubits in between two r'-controlled-σ_x gates (see Fig. 4.1). Thus,

$$f(r') \equiv 40(r'-2) + m \tag{4.36}$$

elementary gates are required to implement V_g^m, and using another r' operations for local basis change in the control register a total of

$$M \equiv 40(r'-2) + m + r' \tag{4.37}$$

gates are required to implement W_g^m [2]. As a total of $|G|$ different gates W_g^m need to be applied to implement W (see Fig. 4.3) one finds that the total number of elementary gates is

$$|G|M = |G|(41r' - 80 + m), \tag{4.38}$$

[2]Note that the r' operations after V_g^m can be combined with the first set of r' operation of the subsequent gate W_h^m.

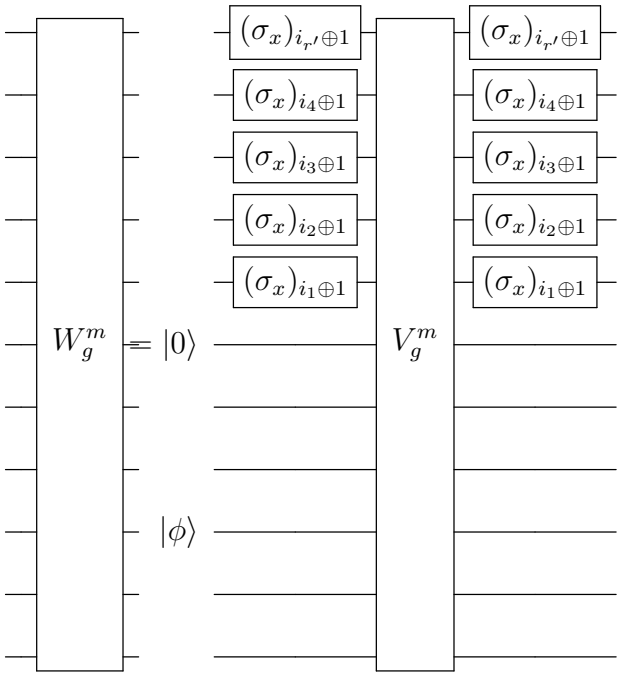

Figure 4.2: The quantum circuit for W_g^m for any state $|g\rangle = |i_{r'} \dots i_1\rangle$. The gate $(\sigma_x)_{i_m\oplus 1}$ flips the m^{th} qubit of the input state, if the m^{th} digit, i_m, in the binary representation of $g \in G$ is zero. After implementing the gate V_g^m the bit string is restored to its original value.

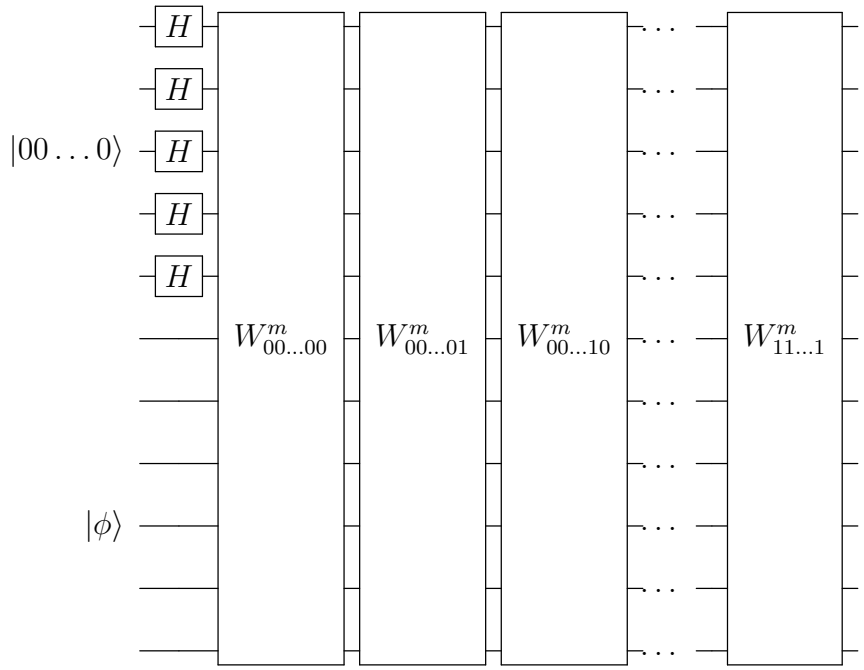

Figure 4.3: The circuit implementation of the encoding circuit $W = \sum_{g\in G} W_g^m$, where $g \in G$ is written in binary notation.

where $|G| = 2^{r'}$. That is, the resources required to encode the quantum data are *linear* in the number of logical qubits, m, and scale as $|G|\log|G|$.

The decoding of the quantum data can also be performed efficiently as Bob simply measures in the basis $\{|\psi(g)\rangle\}$ and applies, depending on the outcome, one of the operations $T_{g^{-1}}^{\otimes m}$ in order to retrieve the state $|\phi\rangle \in \mathcal{H}_2^{\otimes m}$. In practice this can be done by implementing the inverse of the unitary operation $A \otimes \mathbb{1}$ appearing in Eq. (4.23); i.e. $A^\dagger \otimes \mathbb{1}$, followed by r' single qubit measurements in the computational basis.

Finally, note that if $T : G \to \mathrm{GL}(\mathcal{H}_d)$ then the number of elementary gates required to implement W of Eq. (4.26) only increases by a factor which is independent of m and $|G|$. In this case the unitary transformation, $A \otimes \mathbb{1}$, requires at most $\mathcal{O}(d^r)$ elementary gates in order to be implemented. In the following I consider some special groups and show that the required resources can be significantly reduced.

4.2.1 Abelian groups

I now discuss a method to implement the gate W (Eq. (4.26)) for the case of quantum channels whose collective noise is associated with a finite abelian group. Denoting by $g_1, \ldots, g_n$ the generators of the group then for any $g \in G$ there exists a string $(l_1(g), \ldots, l_n(g))$, with $l_i(g) \in N$, such that $g = g_1^{l_1(g)} \cdots g_n^{l_n(g)}$. As the group is finite it follows that for any $i \in (0, \ldots, n)$ there exists an L_i such that $l_i(g) \leq L_i$ for any $g \in G$. Writing $|g\rangle = |l_1(g) \ldots l_n(g)\rangle$, where $l_i(g)$ is represented in binary notation, the gate W becomes

$$W = \prod_{i=1}^{n} T_i \equiv \prod_{i=1}^{n} \left(\sum_{l_i=0}^{L_i} |l_i\rangle\langle l_i| \otimes (T_{g_i}^{l_i})^{\otimes m} \right). \tag{4.39}$$

Note that each T_i in Eq. (4.39) is acting on an L_i-dimensional control system (i.e. $\log L_i$ control qubits) and m target qubits, where the first control system determines how often g_1 is applied the second how often g_2 is applied and so on. Hence, the number of elementary gates required to implement each T_i is at most $L_i f(\log L_i) = L_i[40(\log L_i - 2) + m]$ (see Eq. (4.36)) and the total number of elementary gates is

$$\sum_{i=1}^{n} L_i f(\log L_i) \leq n \max_i \{L_i(f(\log L_i)\}, \tag{4.40}$$

which might be substantially smaller than $|G|(41r' - 80 + m)$ gates required in the general case.

4.2.2 Cyclic groups

I now consider the case where the collective noise of the channel is associated with a general cyclic group, a group with only one generating element $h \equiv g_1$. The group elements are given by h^i where $1 \leq i \leq L = 2^{r'}$. To each group element h^i associate the number $i = \sum_{n=1}^{r'} 2^{n-1} i_n$ written in binary notation and

$$T_{h^i} = \prod_{k=1}^{r'} U^{2^{k-1} i_k}. \tag{4.41}$$

Eq. (4.41) is the key to an efficient implementation of the operation W in Eq. (4.26). Rather than implementing a product of $2^{r'}$ controlled-unitary operations W_g^m (Eq. (4.27)) it suffices to perform r' controlled-unitary operations that use the n^{th} qubit of the first register as the control, and perform the operation $(T^{2^n i_n})^{\otimes m}$ on the message qubits if the bit value is one. This leads to the implementation of the operation $T_g^{\otimes m}$ if the control state is given by $|g\rangle = |i_{r'} \dots i_2 i_1\rangle$ corresponding exactly to the operation W. As each of these gates consists of m two-qubit gates the total number of elementary gates is $m \log L = mr'$. Hence, for a cyclic group with $M = 2^{r'} \in \mathbb{N}$ elements one only requires $m \log M$ gates.

In addition, the unitary operation $A \otimes \mathbb{1}$ in Eq. (4.23) can be done much more efficiently than the upper bound of $\mathcal{O}(d^r)$ operations. For simplicity, let $d = 2$ and note that for a cyclic group of M elements the required number of auxiliary qubits is $r = M - 1$ whereas only $r' = \log_2 M$ qubits are required to label the group elements. The implementation of $A \otimes \mathbb{1}$ then consists of the transformation that maps the computational basis states to the block diagonal basis $\{|k, \alpha\rangle\}$ (see Eq. (3.41)) followed by the Fourier transform. Notice that the order of the operations can be exchanged and, furthermore, the Fourier transformation just acts on standard basis states of $r' < r$ qubits and can be implemented using $\mathcal{O}(r' \log r')$ elementary gates.

For cyclic groups of M elements the transformation that maps the computational basis to the block diagonal basis can be implemented using only $r + r'$ elementary gates as I now show. As the irreps of abelian groups are one-dimensional [78] one simply needs to construct one state, $|k, \alpha\rangle$ for each $\mathcal{H}^{(k)}$, that is a computational basis state containing k ones. In order to do so take r' qubits (the first register) containing the computational basis states $|i_{r'}, i_{r'-1}, \dots, i_1\rangle$, and an additional $r = 2^{r'} - 1$ qubits (the second register) that is partitioned into r' groups B_m. Each group, B_m, in the second register corresponds to the m^{th} qubit of the first register and contains 2^{m-1} qubits (corresponding to its value

in binary representation).

The construction of the required states proceeds in two steps. First, m CNOT operations are performed with the m^{th} qubit in the first register as the control and the 2^{m-1} qubits in the group B_m of the second register as targets. The m CNOT operations cause all qubits within the group B_m in the second register to flip if the m^{th} qubit in the first register is in the state $|i_m\rangle = |1\rangle$. After the first m CNOT operations an additional r' CNOT operations are applied with one of the qubits in B_m of the second register as the control qubit and the m^{th} qubit of the first register as the target. This ensures that the first register is in the state $|0\rangle^{\otimes r'}$ while the state of the second register contains a total number of ones corresponding to the value of the bit-string $i_{r'} i_{r'-1} \dots i_1$.

Thus, for the case of cyclic groups of M elements the overhead for implementing the operation $A \otimes \mathbb{1}$ in Eq. (4.23) is

$$r + r' + \mathcal{O}(r' \log r') = M - 1 + \log_2 M + \mathcal{O}(\log_2 M \log(\log_2 M)) = \mathcal{O}(M), \qquad (4.42)$$

i.e. only *linear* with the number of group elements M. Together with the efficient implementation of the operation W discussed above the encoding of quantum information using the protocol of Sec. 4.1 for the case of finite cyclic groups of M elements requires $\mathcal{O}(m \log M, M)$ elementary gates.

Chapter 5

Discussion

In this chapter I discuss the results of chapters 3, and 4. In particular, I discuss the weak and strong additivity of the alignment rate in Sec. 5.1, and the rate of transmission of quantum information as well as the logical depth of the reference-frame independent quantum communication protocol in Sec. 5.2.

5.1 Additivity of the alignment rate

In chapter 3 I analyzed reference frame alignment where the success of the protocol was quantified by the accessible information. I defined the alignment rate as the amount of information Bob learns per bounded-sized token of Alice's reference frame. I showed that for the case where the reference frame is associated with a G-SSR, where $G = U(1)$ and $G = \mathbb{Z}_M$, the alignment rate is equal to the linearized, regularized G-asymmetry $A_G^{(\mathrm{reg})}$.

From its definition $A_G^{(reg)}$ (see Eq. (3.9)) is weakly additive; i.e.

$$A_G^{(reg)}(\psi^{\otimes 2}) = 2A_G^{(reg)}(\psi). \tag{5.1}$$

As $R_G(\psi) = A_G^{(reg)}(\psi)$ for $G = U(1)$ and $G = \mathbb{Z}_M$ it follows that for these groups $R_G(\psi)$ is also a deterministic frameness monotone that is weakly additive as one would intuitively expect. The question I address in this section is whether R_G is also strongly additive; that is, for any two pure states $|\psi\rangle$ and $|\phi\rangle$ is it true that

$$R_G(\psi \otimes \phi) = R_G(\psi) + R_G(\phi)\ ? \tag{5.2}$$

In the case where $G = U(1)$ Eq. (5.2) is true. Indeed, as was shown in Sec. 3.3 for $G = U(1)$ the alignment rate $R_{U(1)}(\psi) = 4\pi V(\psi)$, where $V(\psi)$ is the photon-number

variance of the state $|\psi\rangle$. It was shown in [79] that the variance is strongly additive; i.e. for any two states $|\psi\rangle$, $|\phi\rangle$, $V(\psi\otimes\phi) = V(\psi) + V(\phi)$. Note that one cannot infer the strong additivity of $R_{U(1)}(\psi)$ from its definition without the explicit calculation in Sec. 3.3. $R_{U(1)}(\psi)$ is strongly additive because it is equal to the photon-number variance.

However, for some groups the alignment rate is not strongly additive even for two distinct *pure* states as I now show. Suppose Alice and Bob lack a shared frame of reference associated with the group $\mathbb{Z}_M$. Consider two bounded-size tokens of a reference frame

$$\begin{aligned} |\psi\rangle &= \sum_{k=0}^{M-1} \sqrt{p_k}|k\rangle, \\ |\phi\rangle &= \sum_{k=0}^{M-1} \sqrt{q_k}|k\rangle. \end{aligned} \tag{5.3}$$

From Theorem 5 of Sec. 3.4 the alignment rates for the two states in Eq. (5.3) are $R_{\mathbb{Z}_M}(|\psi\rangle) = -2\log r_{\max}$ and $R_{\mathbb{Z}_M}(|\phi\rangle) = -2\log l_{\max}$ respectively, where

$$r_{\max} = \max_{n\in\{1,\ldots,M-1\}} \left|\sum_{m=0}^{M-1} e^{\frac{\imath 2\pi nm}{M}} p_m\right|, \qquad l_{\max} = \max_{n\in\{1,\ldots,M-1\}} \left|\sum_{m=0}^{M-1} e^{\frac{\imath 2\pi nm}{M}} q_m\right|.$$

Up to Z_M-invariant unitaries $|\psi\rangle\otimes|\phi\rangle$ can be written as

$$|\psi\rangle\otimes|\phi\rangle = \sum_{k_1,k_2=0}^{M-1} \sqrt{p_{k_1}q_{k_2}}|k_1\rangle\otimes|k_2\rangle = \sum_k \sqrt{c_k}|k\rangle, \tag{5.4}$$

where

$$c_k = \sum_{k_1,k_2} p_{k_1}q_{k_2}, \tag{5.5}$$

and the sum is over all k_1, k_2 such that $k_1+k_2 = k_{\mathrm{mod}M}$. Computing the Fourier transform of the coefficients c_k one obtains

$$\omega_n = \sum_{m=0}^{M-1} e^{\frac{\imath 2\pi mn}{M}} c_m = \sum_{m=0}^{M-1} \sum_{k_1+k_2=m} e^{\frac{\imath 2\pi n(k_1+k_2)}{M}} p_{k_1}q_{k_2}. \tag{5.6}$$

Noting that $\sum_{m=0}^{M-1}\sum_{k_1+k_2=m} = \sum_{k_1=0}^{M-1}\sum_{k_2=0}^{M-1}$, Eq. (5.6) reduces to

$$\omega_n = \sum_{k_1=0}^{M-1} e^{\frac{\imath 2\pi k_1 n}{M}} p_{k_1} \sum_{k_2=0}^{M-1} e^{\frac{\imath 2\pi k_2 n}{M}} q_{k_2} \equiv r_n l_n e^{\imath(\theta_n+\phi_n)}\ , \tag{5.7}$$

where r_n and l_n are the absolute values of the Fourier transforms of $\{p_k\}$ and $\{q_k\}$, respectively. Therefore,

$$\begin{aligned} R_{\mathbb{Z}_M}(\psi \otimes \phi) &= \max_{n\in\{1,\ldots,M-1\}} (-2\log r_n - 2\log l_n) \\ &\geq -2\log r_{\max} - 2\log l_{\max} \\ &= R_{\mathbb{Z}_M}(\psi) + R_{\mathbb{Z}_M}(\phi). \end{aligned} \tag{5.8}$$

Hence, $R_{\mathbb{Z}_M}$ is not strongly additive in general.

For the case where $M = 2$ $R_{\mathbb{Z}_M}$ is strongly additive as there is only a single n, namely $n = 1$. For the case where $M = 3$ $R_{\mathbb{Z}_M}$ is again strongly additive as there are only two values for n which turn out to satisfy $\omega_1 = \omega_2^*$ and thus $|\omega_1| = |\omega_2|$. However, for $M \geq 4$ $R_{\mathbb{Z}_M}$ is super-additive as the following example shows. Consider the following bounded-size tokens of Alice's $\mathbb{Z}_4$ reference frame

$$\begin{aligned} |\psi\rangle &= \sqrt{\frac{13}{64}}|0\rangle + \sqrt{\frac{18}{64}}|1\rangle + \sqrt{\frac{19}{64}}|2\rangle + \sqrt{\frac{14}{64}}|3\rangle, \\ |\phi\rangle &= \sqrt{\frac{7}{20}}|0\rangle + \sqrt{\frac{3}{20}}|1\rangle + \sqrt{\frac{6}{20}}|2\rangle + \sqrt{\frac{4}{20}}|3\rangle. \end{aligned} \tag{5.9}$$

Computing the Fourier transforms one obtains

$$\begin{aligned} r_1 = r_3 = 0.113,\ r_2 = 0 \\ l_1 = l_3 = 0.07,\ l_2 = 0.3. \end{aligned} \tag{5.10}$$

Thus, $r_{\max} = r_1 = 0.113$ and $l_{\max} = l_2 = 0.3$. Moreover, $|\omega_1| = 0.008$, $|\omega_2| = 0$, and $|\omega_3| = 0.008$. Therefore, $|\omega_{\max}| = r_1 l_1$ which is smaller than $r_{\max} l_{\max}$. Hence, $R_{\mathbb{Z}_4}(|\psi\rangle \otimes |\phi\rangle)$ is strictly greater than $R_{\mathbb{Z}_4}(|\psi\rangle) + R_{\mathbb{Z}_4}(|\phi\rangle)$.

The alignment rate quantifies how well a quantum state can serve as a bounded-sized token of the missing reference frame. The super-additivity of R_G implies that if Bob holds $N \gg 1$ copies of two bounded-sized token states, $|\psi\rangle$ and $|\phi\rangle$, then Bob obtains

more information about Alice's reference frame if he performs a joint measurement on the bounded-sized tokens rather than measuring each token separately.

From its definition the alignment rate is a regularized quantity (see Eq. (3.10)); it is defined an the ratio of linearized accessible information per physical system transmitted in the limit where the latter is asymptotically large. Several other important quantities in quantum information, such as the classical capacity of a quantum channel [85, 86] and the entanglement cost [87], are regularized quantities. In the resource theory of entanglement the entanglement cost is defined as the rate at which one can convert, by local means, many copies of pure bipartite maximally entangled states (singlets) to many copies of another bipartite state ρ^{AB}.

An important open problem in quantum information is whether quantities such as the classical capacity or the entanglement cost are strongly additive. As I showed above the alignment rate is not strongly additive for the case of finite cyclic groups of order greater than three even under the tensor product of two distinct *pure* states . The alignment rate is unique in that it is the first quantity to my knowledge whose regularization does not yield an additive quantity.

In the next section I discuss the results of chapter 4 pertaining to reference-frame independent communication of quantum information.

5.2 Transmission rate and logical depth of reference frame independent protocol

In chapter 4 I introduced a new reference-frame independent communication protocol. I showed that the number of elementary gates required to implement the encoding and decoding circuit for the protocol scale as $\mathcal{O}(m, |G| \log |G|, d^r)$, where r is an integer that depends solely on $T : G \to \mathrm{GL}(\mathcal{H}_d)$. For the case of finite cyclic groups $\mathbb{Z}_M$ I

showed that the encoding and decoding operations can be efficiently implemented with at most $m \log M + \mathcal{O}(M)$ operations. As the required number of elementary gates scale only linearly in the number of logical qudits my protocol is more efficient than the best currently known DFS protocols [68, 69, 88]. Moreover, the linear scaling in the number of elementary gates makes the physical implementation of my protocol feasible.

The rate of transmission of quantum information, R, using the protocol in Sec. 4.1 is given by

$$R \equiv \frac{m}{r+m}; \tag{5.11}$$

i.e. m logical qudits can be perfectly transmitted using $r+m$ physical qudits. As the number of qudits, r, required to construct the set of states $S^{(T)}_{(r,|\psi\rangle)}$ is finite and depends only on $T : G \to \mathrm{GL}(\mathcal{H})$, where G is a finite group, in the limit $m \to \infty$ Eq. (5.11) tends to unity. Thus, if Alice possesses asymptotically many quantum systems the rate of transmission of quantum information given Eq. (5.11) is optimal.

However, if Alice possesses only a finite number of systems the rate of transmission, Eq. (5.11), is less than that achieved by the DFS protocol of [68, 69] as I now explain. Consider the case where Alice possess three physical qubits and lacks a shared frame of reference associate with the finite cyclic group $\mathbb{Z}_3$ with Bob. Let $T : \mathbb{Z}_3 \to \mathrm{GL}(\mathcal{H}_2)$ be given by

$$T_g = \sum_{n=0}^{1} \omega^{ng} |n\rangle\langle n| \quad g \in (0,1,2), \tag{5.12}$$

where $\omega = e^{i2\pi/3}$. As $\mathbb{Z}_3$ is abelian it has three one-dimensional inequivalent irreps. Using the orthogonality relations of irreps (theorem 1) it can be shown that $T^{\otimes 2} : \mathbb{Z}_3 \to \mathrm{GL}(\mathcal{H}_2^{\otimes 2})$ contains the regular representation of $\mathbb{Z}_3$ as a sub-representation. Thus, using the protocol of Sec. 4.1 Alice can communicate one logical qubit using three physical qubits.

On the other hand, under the action of $T^{\otimes 3} : \mathbb{Z}_3 \to \mathrm{GL}(\mathcal{H}_2^{\otimes 3})$, the total Hilbert space

of three qubits can be conveniently written as

$$H^{\otimes 3} \cong \bigoplus_{k=0}^{2} \mathcal{H}^{(k)}, \tag{5.13}$$

where $\mathcal{H}^{(0)} = \text{span}\{|000\rangle, |111\rangle\}$, $\mathcal{H}^{(1)} = \text{span}\{|001\rangle, |010\rangle, |100\rangle\}$, and $\mathcal{H}^{(2)} = \text{span}\{|110\rangle, |101\rangle, |011\rangle\}$. The sub-spaces $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$ are three-dimensional DFS and can thus be used to transmit $\log_2 3 > 1$ logical qubits. It is easy to show that if Alice has a finite number of quantum systems at her disposal the protocol of Sec. 4.1 achieves a lower rate of transmission of quantum information compared to the DFS-based protocol of [68, 69] for any finite group G. Despite the lower transmission rate the implementation of the encoding and decoding circuit is more efficient for the protocol in Sec. 4.1 compared to that of [68, 69].

More importantly the encoding and decoding circuits outlined in Sec. 4.2 have a constant logical depth as I now explain. The *logical depth* of a circuit is the amount of time required by the circuit to generate the desired state. As all the control gates in V_g^m of Eq. (4.33), acting on m qubits originally prepared in $|\phi\rangle \in \mathcal{H}_2^{\otimes m}$, can be implemented in parallel the logical depth of the circuit implementing W (Eq. (4.26)) is *constant* and given by $|G|(41r' - 80 + 1)$. Moreover, as the unitary basis change $A \otimes \mathbb{1}$ in Eq. (4.23) requires at most $\mathcal{O}(2^r)$ gates, where r depends only on $T : G \to \text{GL}(\mathcal{H}_d)$, the logical depth is *independent* of m in contrast to the DFS-based communication scheme put forward in [68, 69]. This allows for a very efficient implementation of the gate W.

Chapter 6

Summary and future work

In this thesis I introduced a new operational measure for quantifying the frameness resource of a bounded-sized token of a classical frame of reference as well as an alternative, reference-frame independent protocol for communicating quantum information. More precisely, In chapter 3 I showed how the rate of alignment of a reference frame communication protocol provides an operational interpretation of the G-asymmetry which was thus far lacking in the literature. In chapter 4, I showed how m logical qudits can be transmitted using $m + r$ physical qudits in the absence of a shared frame of reference associated with an arbitrary finite group G.

Unlike all other reference-frame alignment protocols to date I used an information theoretic measure, namely the accessible information, to quantify the success of a reference-frame alignment protocol. I showed that for the case where parties lack a shared frame of reference associated with the groups $U(1)$ and $\mathbb{Z}_M$ the alignment rate is equal to the linearized, regularized G-asymmetry for $G = U(1)$ and $G = \mathbb{Z}_M$. This result establishes a connection between the resource theory of quantum reference frames and reference-frame alignment protocols.

Furthermore, for the case of finite cyclic groups of more than three elements the alignment rate is not additive under the tensor product of two distinct pure states. Possible future work in this area is the analysis of reference frame alignment for general groups, in particular non-abelian groups, as well as strong additivity of the alignment rate for these groups. I conjecture that $R_G = A_G^{(reg)}$ for all finite or compact Lie groups. An interesting question that arises is the degree of violation of strong additivity. For the case of finite cyclic groups of order greater than three the amount of information that

Bob gains by measuring many copies of two bounded-sized reference frame tokens jointly rather than separately is exponentially small. Does there exist a group, G, for which the amount of information gained by performing joint measurements on many copies of two bounded-sized tokens is significantly larger than when measuring the tokens separately? I believe that for the case of non-abelian groups, such as SU(2), the amount of information gained by performing joined measurements will be significantly larger.

In chapter 4 I made use of ideas both from DFS and error correction to construct a reference-frame independent protocol for communicating quantum information for the case where parties lack a shared frame of reference associated with a finite group G. I showed how m logical qudits can be transmitted with perfect fidelity and can be efficiently encoded and decoded using $\mathcal{O}(m, |G| \log |G|, d^r)$ elementary gates, where r is an integer that depends solely on $T : G \to \mathrm{GL}(\mathcal{H}_d)$. For certain groups, such as finite cyclic groups, I showed that the encoding and decoding operations can be efficiently implemented with at most $m \log M + \mathcal{O}(M)$ operations. Moreover, the logical depth of the encoding and decoding circuit for finite groups is independent of the number of logical qudits, m. As the required number of elementary gates scales only linearly in the number of logical qudits my protocol is more efficient than the best currently known DFS protocols [68, 69, 88]. However, this decrease in the number of elementary gates comes at the cost of achieving a lower rate of transmission of quantum information if only a finite number of quantum systems are available.

I am currently in the process of extending the protocol in Sec. 4.1 to the case where Alice and Bob lack a shared frame of reference associated with a continuous group. Specifically, for a reference frame associated with the group $U(1)$ one can use the approximation $\lim_{M\to\infty} \mathrm{Z}_M \to U(1)$ and apply the protocol of Sec. 4.1 for the case where $G = \mathbb{Z}_M$. However, due to the approximation of a continuous group by a discreet group the transmission of quantum information occurs at non-unit fidelity. Furthermore, this

technique seems applicable only to the $U(1)$ case, and I am confident that this method will yield asymptotically optimal transmission of quantum information at high fidelity with less cost in encoding and decoding resources. In the case of non-abelian continuous groups, such as SU(2), a different approach based on design theory seems more promising. Both of these problems are currently under investigation.

In addition, whereas the implementation of the reference-frame independent protocol for finite abelian groups is very efficient it is not obvious if an efficient implementation is feasible for the case of non-abelian groups. This is due to the fact that in general an $\mathcal{O}(d^r)$ overhead is required to implement the unitary operator in Eq. (4.23). For a group with $|G|$ elements $r' = \log_2|G|$ qubits are required to label the elements yet $r \geq r'$ qubits are needed to construct the set of states $S^{(T)}_{(r,|\psi\rangle)}$ with the required properties. In the case of finite cyclic groups, $r = (|G| - 1)/(d - 1)$ is exponentially larger than r'. Despite this exponential increase I have shown that the unitary operator in Eq. (4.23) can be efficiently implemented using $\mathcal{O}(r)$ operations, i.e. with an overhead that scales only linear in the number of group elements, in the case of finite cyclic groups. Whether such an exponential overhead also occurs for other groups and whether this can also be compensated by a more efficient implementation of the operation in Eq. (4.23) is presently unknown.

Bibliography

[1] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[2] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.

[3] C. H. Bennett and G. Brassard. Quantum cryptography:public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[4] P. W. Shor. Polynomial-time algorithms for prime factorization and discreet logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.

[5] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pages 212–219, New York, NY, USA, 1996.

[6] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Decoherence-full subsystems and the cryptographic power of a private shared reference frame. *Phys. Rev. A*, 70:032307, Sep 2004.

[7] G. C. Wick, A. S. Wightman, and E. P. Wigner. The intrinsic parity of elementary particles. *Phys. Rev.*, 88:101–105, Oct 1952.

[8] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, 1955.

[9] Y. Aharonov and L. Susskind. Charge superselection rule. *Phys. Rev.*, 155:1428–1431, Mar 1967.

[10] R. Mirman. Coherent superposition of charge states. *Phys. Rev.*, 186:1380–1383, Oct 1969.

[11] R. Mirman. Nonexistence of superselection rules: Definition of term frame of reference. *Foundations of Physics*, 9:283–299, 1979.

[12] D. Kershaw and C. H. Woo. Experimental test for the charge superselection rule. *Phys. Rev. Lett.*, 33:918–921, Oct 1974.

[13] Y. Castin and J. Dalibard. Relative phase of two Bose-Einstein condensates. *Phys. Rev. A*, 55:4330–4337, Jun 1997.

[14] W. Hoston and L. You. Interference of two condensates. *Phys. Rev. A*, 53:4254–4256, Jun 1996.

[15] J. Javanainen and S. M. Yoo. Quantum phase of a Bose-Einstein condensate with an arbitrary number of atoms. *Phys. Rev. Lett.*, 76:161–164, Jan 1996.

[16] S. M. Yoo, J. Ruostekoski, and J. Javanainen. Interference of two Bose-Einstein condensates. *Journal of Modern Optics*, 44(10):1763–1774, 1997.

[17] M. R. Dowling, S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Observing a coherent superposition of an atom and a molecule. *Phys. Rev. A*, 74:052113, Nov 2006.

[18] J. Dunningham, L. Rico Gutiérrez, and V. Palge. Observing superpositions of different number states. *Optics and Spectroscopy*, 111:528–534, 2011.

[19] K. Mølmer. Optical coherence: A convenient fiction. *Phys. Rev. A*, 55:3195–3203, Apr 1997.

[20] B. C. Sanders, S. D. Bartlett, T. Rudolph, and P. L. Knight. Photon-number superselection and the entangled coherent-state representation. *Phys. Rev. A*, 68:042329, Oct 2003.

[21] R. J. Glauber. Coherent and incoherent states of the radiation field. *Phys. Rev.*, 131:2766–2788, Sep 1963.

[22] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Dialogue concerning two views on quantum coherence: factist and fictionist. *International Journal of Quantum Information*, 4:17–43, 2006.

[23] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79(2):555–609, Apr 2007.

[24] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Hiding bits in Bell states. *Phys. Rev. Lett.*, 86:5807–5810, Jun 2001.

[25] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *Information Theory, IEEE Transactions on*, 48(3):580 –598, mar 2002.

[26] F. Verstraete and J. I. Cirac. Quantum nonlocality in the presence of superselection rules and data hiding protocols. *Phys. Rev. Lett.*, 91:010404, Jul 2003.

[27] A. Kitaev, D. Mayers, and J. Preskill. Superselection rules and quantum protocols. *Phys. Rev. A*, 69:052326, May 2004.

[28] S. J. van Enk. Single-particle entanglement. *Phys. Rev. A*, 72:064306, Dec 2005.

[29] H. M. Wiseman and J. A. Vaccaro. Entanglement of indistinguishable particles shared between two parties. *Phys. Rev. Lett.*, 91:097902, Aug 2003.

[30] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[31] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[32] S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner. Degradation of a quantum reference frame. *New Journal of Physics*, 8(4):58, 2006.

[33] D. Poulin and J. Yard. Dynamics of a quantum reference frame. *New Journal of Physics*, 9(5):156, 2007.

[34] S. D. Bartlett, T. Rudolph, B. C. Sanders, and P. S. Turner. Degradation of a quantum directional reference frame as a random walk. *Journal of Modern Optics*, 54(13-15):2211–2221, 2007.

[35] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[36] N. Schuch, F. Verstraete, and J. I. Cirac. Nonlocal resources in the presence of superselection rules. *Phys. Rev. Lett.*, 92:087904, Feb 2004.

[37] N. Schuch, F. Verstraete, and J. I. Cirac. Quantum entanglement theory in the presence of superselection rules. *Phys. Rev. A*, 70:042310, Oct 2004.

[38] G. Gour, I. Marvian, and R. W. Spekkens. Measuring the quality of a quantum reference frame: The relative entropy of frameness. *Phys. Rev. A*, 80:012307, Jul 2009.

[39] S. J. van Enk. Quantifying the resource of sharing a reference frame. *Phys. Rev. A*, 71:032339, Mar 2005.

[40] J. A. Vaccaro, F. Anselmi, H. M. Wiseman, and K. Jacobs. Tradeoff between extractable mechanical work, accessible entanglement, and ability to act as a reference

system, under arbitrary superselection rules. *Phys. Rev. A*, 77:032114, Mar 2008.

[41] A. S. Holevo. Statistical problems in quantum physics. In G. Maruyama and Y. Prokhorov, editors, *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, volume 330 of *Lecture Notes in Mathematics*, pages 104–119. Springer Berlin / Heidelberg, 1973.

[42] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, 1998.

[43] M. Horodecki, J. Oppenheim, and R. Horodecki. Are the laws of entanglement theory thermodynamical? *Phys. Rev. Lett.*, 89(24):240403, Nov 2002.

[44] A. S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory.* North-Holland Series in Statistics and Probability, 1980.

[45] A. Peres and W. K. Wootters. Optimal detection of quantum information. *Phys. Rev. Lett.*, 66:1119–1122, Mar 1991.

[46] S. Massar and S. Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74:1259–1263, Feb 1995.

[47] R. Derka, V. Buzěk, and A. K. Ekert. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. *Phys. Rev. Lett.*, 80:1571–1575, Feb 1998.

[48] R. Tarrach and G. Vidal. Universality of optimal measurements. *Phys. Rev. A*, 60:R3339–R3342, Nov 1999.

[49] N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Phys. Rev. Lett.*, 83:432–435, Jul 1999.

[50] S. Massar. Collective versus local measurements on two parallel or antiparallel spins. *Phys. Rev. A*, 62:040101, Sep 2000.

[51] G. Chiribella, G. M. D'Ariano, and M. F. Sacchi. Optimal estimation of group transformations using entanglement. *Phys. Rev. A*, 72:042338, Oct 2005.

[52] A. Peres and P. F. Scudo. Transmission of a cartesian frame by a quantum system. *Phys. Rev. Lett.*, 87:167901, Sep 2001.

[53] E. Bagan, M. Baig, and R. Muñoz Tapia. Aligning reference frames with quantum states. *Phys. Rev. Lett.*, 87:257903, Nov 2001.

[54] A. Acìn, E. Janè, and G. Vidal. Optimal estimation of quantum dynamics. *Phys. Rev. A*, 64:050302, Oct 2001.

[55] E. Bagan, M. Baig, and R. Muñoz Tapia. Entanglement-assisted alignment of reference frames using a dense covariant coding. *Phys. Rev. A*, 69:050303, May 2004.

[56] E. Bagan, M. Baig, and R. Muñoz Tapia. Quantum reverse engineering and reference-frame alignment without nonlocal correlations. *Phys. Rev. A*, 70:030301, Sep 2004.

[57] 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.

[58] P. Zanardi. Virtual quantum subsystems. *Phys. Rev. Lett.*, 87:077901, Jul 2001.

[59] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79:3306–3309, Oct 1997.

[60] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, Mar 2000.

[61] P. Zanardi. Stabilizing quantum information. *Phys. Rev. A*, 63:012301, Dec 2000.

[62] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293(5537):2059–2063, 2001.

[63] C. P. Yang and J. Gea-Banacloche. Three-qubit quantum error-correction scheme for collective decoherence. *Phys. Rev. A*, 63:022311, Jan 2001.

[64] D. A. Lidar, I. L. Chuang, and K. B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81:2594–2597, Sep 1998.

[65] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley. Theory of decoherence-free fault-tolerant universal quantum computation. *Phys. Rev. A*, 63(4):042307, Mar 2001.

[66] M. S. Byrd. Implications of qudit superselection rules for the theory of decoherence-free subsystems. *Phys. Rev. A*, 73:032330, Mar 2006.

[67] C. A. Bishop and M. S. Byrd. Compatible transformations for a qudit decoherence-free/noiseless encoding. *Journal of Physics A: Mathematical and Theoretical*, 42(5):055301, 2009.

[68] D. Bacon, I. L. Chuang, and A. W. Harrow. Efficient quantum circuits for Schur and Clebsch-Gordan transforms. *Phys. Rev. Lett.*, 97(17):170502, Oct 2006.

[69] D. Bacon, I. L. Chuang, and A. W Harrow. The quantum Schur transform: I. efficient qudit circuits, 2006. quant-ph/0601001.

[70] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Classical and quantum communication without a shared reference frame. *Phys. Rev. Lett.*, 91:027901, Jul 2003.

[71] A. Cabello. Greenberger-Horne-Zeilinger-like proof of Bell's theorem involving observers who do not share a reference frame. *Phys. Rev. A*, 68:042104, Oct 2003.

[72] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens. Robust polarization-based quantum key distribution over a collective-noise channel. *Phys. Rev. Lett.*, 92:017901, Jan 2004.

[73] T. Y. Chen, J. Zhang, J C. Boileau, X. M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J. W. Pan. Experimental quantum communication without a shared reference frame. *Phys. Rev. Lett.*, 96:150504, Apr 2006.

[74] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich. Decoherence-free subspaces in quantum key distribution. *Phys. Rev. Lett.*, 91:087901, Aug 2003.

[75] J. L. Ball and K. Banaszek. Decoherence-free subspaces and subsystems for a collectively depolarizing bosonic channel. *Open Systems and Information Dynamics*, 12:121–131, 2005. 10.1007/s11080-005-5723-1.

[76] J. L. Ball and K. Banaszek. Hybrid noiseless subsystems for quantum communication over optical fibres. *Journal of Physics A: Mathematical and General*, 39(1):L1, 2006.

[77] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory.* Springer, Verlag, 1983.

[78] J.-Q. Chen. *Group Representation Theory for Physicists.* World Scientific, Singapore, 1989.

[79] G. Gour and R. W. Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics*, 10(3):033023, 2008.

[80] M. Marvian and R. W. Spekkens, 2011. arXiv:1105.1816v1; arXiv:1104.0018v1.

[81] R. Durrett. *Probability Theory and Examples*. Cambringe University Press, New York, 2010.

[82] S. D. Bartlett, Rudolph T., R. W. Spekkens, and P. S. Turner. Quantum communication using a bounded-size quantum reference frame. *New Journal of Physics*, 11(6):063013, 2009.

[83] W. Burnside. *Theory of Groups of Finite Order, 2nd Edition*. Cambridge University Press, London U.K., 1911.

[84] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[85] A. S. Holevo. The capacity of the quantum channel with general signal states. *Information Theory, IEEE Transactions on*, 44(1):269 –273, jan 1998.

[86] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56:131–138, Jul 1997.

[87] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996.

[88] C. K. Li, M. Nakahara, Y. T. Poon, N. S. Sze, and H. Tomita. Recursive encoding and decoding of noiseless subsystem and decoherence free subspace, 2011. arXiv:1106.5210v1.