OPEN ACCESS

Quantum communication using a bounded-size quantum reference frame

New Journal of Physics
The open-access journal for physics

Quantum communication using a bounded-size quantum reference frame

Stephen D Bartlett[1], Terry Rudolph[2,3], Robert W Spekkens[4] and Peter S Turner[5]

[1] School of Physics, The University of Sydney, Sydney, NSW 2006, Australia
[2] Optics Section, Blackett Laboratory, Imperial College London, London SW7 2BZ, UK
[3] Institute for Mathematical Sciences, Imperial College London, London SW7 2BW, UK
[4] Perimeter Institute for Theoretical Physics, 31 Caroline St. North, Waterloo, ON N2L 2Y5, Canada
[5] Department of Physics, Graduate School of Science, University of Tokyo, Tokyo 113-0033, Japan
E-mail: bartlett@physics.usyd.edu.au

New Journal of Physics **11** (2009) 063013 (30pp)
Received 31 December 2008
Published 8 June 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/6/063013

Abstract. Typical quantum communication schemes are such that to achieve perfect decoding the receiver must share a reference frame (RF) with the sender. Indeed, if the receiver only possesses a bounded-size quantum token of the sender's RF, then the decoding is imperfect, and we can describe this effect as a noisy quantum channel. We seek here to characterize the performance of such schemes, or equivalently, to determine the effective decoherence induced by having a bounded-size RF. We assume that the token is prepared in a special state that has particularly nice group-theoretic properties and that is near-optimal for transmitting information about the sender's frame. We present a decoding operation, which can be proven to be near-optimal in this case, and we demonstrate that there are two distinct ways of implementing it (corresponding to two distinct Kraus decompositions). In one, the receiver measures the orientation of the RF token and reorients the system appropriately. In the other, the receiver extracts the encoded information from the virtual subsystems that describe the relational degrees of freedom of the system and token. Finally, we provide

explicit characterizations of these decoding schemes when the system is a single qubit and for three standard kinds of RF: a phase reference, a Cartesian frame (representing an orthogonal triad of spatial directions), and a reference direction (representing a single spatial direction).

Contents

1. Introduction **2**
1.1. Mathematical preliminaries . . . 6
2. Encoding **7**
2.1. Quantum reference frames . . . 7
2.2. Relational subsystems . . . 10
3. Decoding **14**
3.1. 'Measure and re-orient' implementation of decoding . . . 14
3.2. 'Extract from the relational subsystems' implementation of decoding . . . 15
3.3. Comparison of implementations . . . 16
3.4. Post-selectively perfect decoding . . . 17
4. Example: phase reference **18**
4.1. Effective decoherence . . . 18
4.2. Relational subsystems . . . 19
5. Example: Cartesian frame **20**
5.1. Effective decoherence . . . 20
5.2. Relational subsystems . . . 22
6. Example: direction indicator **25**
6.1. Effective decoherence . . . 26
6.2. Relational subsystems . . . 27
Acknowledgments **29**
References **29**

1. Introduction

Many communication protocols implicitly require that the communicating parties share a reference frame (RF) [1]. For instance, if one party, Alice, transmits qubits to another party, Bob, using spin-1/2 particles, the quantum state of the collection can only be recovered by Bob if he and Alice share a RF for orientation. Lacking such a shared RF (for instance, by lacking knowledge of the relation between their local RFs) is equivalent to having a noisy channel; the density operator relative to Bob's local frame is the average over rotations of the density operator relative to Alice's local frame. For a single qubit, such an average over rotations yields complete decoherence—no information about the quantum state survives. Nonetheless, Alice and Bob can still achieve perfect classical and quantum communication by encoding the information into the rotationally invariant degrees of freedom of many qubits [2]. Indeed, in the limit of large numbers, the cost of not sharing a RF is only logarithmic in the number of systems. Similarly, if Alice and Bob lack a phase reference, they can still encode classical and quantum information in phase-invariant states of composite systems [1]. However, such communication schemes are

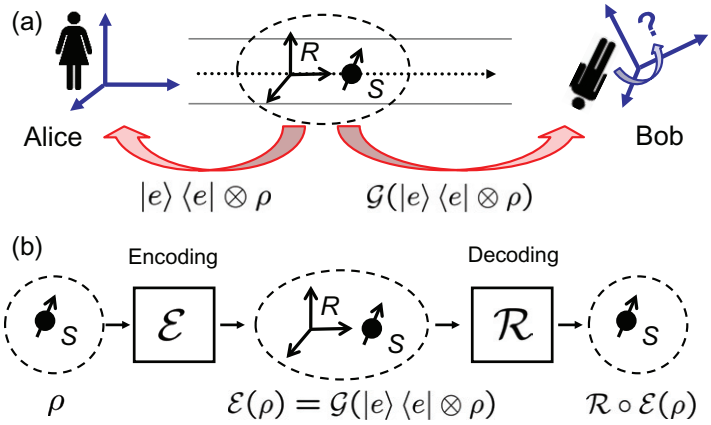

Figure 1. (a) Alice describes the RF token R by the state $|e\rangle\langle e|$ and the system S by the state ρ. Bob, who is not correlated with Alice's RF, describes the joint state of R and S as the twirling of Alice's description, namely $\mathcal{G}(|e\rangle\langle e| \otimes \rho)$. (b) We can consider Alice's act of adjoining the RF token to the system together with the twirling as an encoding operation $\mathcal{E}$. Composing this with Bob's decoding operation R, the resulting channel can be described as an effective $\mathcal{R} \circ \mathcal{E}$.

technically challenging to implement because they make use of highly entangled states of many qubits [3, 4]. Such schemes will be referred to here as 'calibration-free'.

A more straightforward strategy for coping with the lack of a shared RF is for Alice and Bob to begin their communication protocol by setting up a shared RF, that is, they begin by calibrating or aligning their local RFs. Thereafter Alice transmits her quantum systems normally. This strategy is illustrated in figure 1. The problem of aligning RFs using finite communication resources has been well studied [1], [5]–[9]. If only finite communication resources are devoted to the task, then the token of Alice's RF that is transmitted to Bob will be of bounded size. Assuming the RF in question is associated with a continuous degree of freedom, this bound leads to a nonzero probability of error in the decoding of messages. Nonetheless, this scheme has two advantages over its calibration-free counterpart: (i) Alice does not need to implement any entangling operations to encode classical bits or logical qubits into the physical qubits, nor does Bob require such operations to decode (they may require entangling operations to prepare and measure the RF token, but the preparation and measurement they require is always the same and their effort does not scale with the size of the message). (ii) If Alice wishes to communicate a classical bit string or a string of logical qubit states, she can encode one logical bit or qubit per physical qubit, and Bob can decode one logical bit or qubit per physical qubit (in other words, the blocks of physical qubits into which they encode and decode their logical bits and qubits can be as small as one, unlike the calibration-free scheme). By virtue of (ii), Alice does not need to know the entire message string at the outset to achieve her optimal communication rate, nor does Bob need to store all of the systems coherently until he has received the entire sequence of physical qubits, whereas such capabilities are required to achieve the optimal rate of communication in the calibration-free scheme. We are therefore motivated to explore how well Alice can communicate quantum information to Bob after supplying him with a bounded-size token of her RF.

The general case we consider is that of a RF associated with a compact Lie group G. If the system is prepared in the state ρ and the RF token in the state $|e\rangle$ relative to Alice's local RF,

then relative to Bob's local RF, the pair is in the state

$$\mathcal{E}[\rho] = \mathcal{G}(|e\rangle\langle e| \otimes \rho)\,, \tag{1}$$

where $\mathcal{G}$ averages over the collective action of the group and is termed the G-twirling operation (see figure 1). This state encodes ρ. We consider the case where the RF token is prepared in a particular state $|e\rangle$, suggested by previous investigations [9, 10], which is near-optimal for transmitting information about the group element and which makes the mathematics particularly simple. We then determine how well Bob can reconstruct the state ρ. It turns out that the recovery (or decoding) operation $\mathcal{R}$ that is equal to the Hilbert–Schmidt adjoint of $\mathcal{E}$, normalized to be trace-preserving, is provably near-optimal (in a sense we will define later). The composition of encoding and decoding yields an effective decoherence of the form

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \int \mathrm{d}g\; p(g) U_S(g) \rho U_S^\dagger(g)\,, \tag{2}$$

where

$$p(g) \propto |\langle e|U_R(g)|e\rangle|^2 \tag{3}$$

is a probability distribution over the group with $\mathrm{d}g$ the group-invariant measure, U_S and U_R are unitary representations of G on the system S and the RF token R, respectively. With our particular choice of reference state $|e\rangle$, we find that $p(hgh^{-1}) = p(g)$ for all $h \in G$, ensuring that $\mathcal{R} \circ \mathcal{E}$ is a G-invariant map (it commutes with the action of every $g \in G$). The figure of merit relative to which the decoding operation is judged to be near-optimal is the entanglement fidelity.

We also demonstrate two distinct ways of implementing this decoding operation. The first is an obvious scheme: Bob estimates the orientation of the token relative to his local frame and then re-orients the system appropriately. We call this the 'measure and re-orient' scheme. The second is less intuitive, but reveals more about the structure of the problem: Bob projects into the virtual subsystems that support the representation of the group induced by *relative* transformations of the system and token and implements an isometry that maps these onto a single Hilbert space. We call this the 'extract from the relational subsystems' scheme. These relational subsystems are the places in the Hilbert space of the combined token and system where the quantum information associated with ρ is to be found. Their characterization is the key technical result of the paper. The second scheme is also particularly interesting because, with a slight modification, it can yield a decoding that is probabilistically perfect, that is, one which sometimes fails but which yields a perfect decoding when it succeeds.

We work out the explicit form of the recovery operation $\mathcal{R}$ and the effective decoherence $\mathcal{R} \circ \mathcal{E}$ for several interesting examples: (i) a phase reference, (ii) a Cartesian frame (representing an orthogonal triad of spatial directions)[6] and (iii) a reference direction (representing a single spatial direction). In each case, we consider a system consisting of a single qubit. The explicit form of the decoherence map is actually quite simple in this case. Because $\mathcal{R} \circ \mathcal{E}$ is a G-invariant map, it follows from the results of [11] that it is a sum of irreducible G-invariant maps called moments. But in the case of a qubit, there is only a single nontrivial moment—the G-twirling map $\mathcal{G}$. Thus, we have

$$\mathcal{R} \circ \mathcal{E} = (1 - p)\mathcal{I} + p\mathcal{G}\,, \tag{4}$$

[6] Note that although the term 'Cartesian frame' is commonly used to refer to a RF for *both* orientation of the axes of an object as well as the object's position, it is here used only for orientation.

where $\mathcal{I}$ is the identity map. We show that for our examples, p is inversely proportional to the size of the RF token,

$$p \propto \frac{1}{\text{size of RF}}, \tag{5}$$

where the size of the RF is given by the quantum number of the highest irreducible representation appearing in the state of the token. It is also shown that in probabilistically perfect decoding schemes, the probability of failure is inversely proportional to the size of the RF token. These results are specific to the special form of RF state that we consider here.

The idea that bounded-size quantum RFs induce an effective decoherence is not new. The effect of a bounded-size clock, which is a kind of phase reference, has been considered previously by many authors [12]–[15] and that of a bounded-size directional frame has been considered by Poulin [16]. Our results go beyond this work in several ways. For one, the case of a Cartesian frame, which is particularly significant given that it is representative of the general non-Abelian case, has not been examined before. More significantly, we consider many different sorts of RFs within a unified framework and we provide insight into the structure of the problem. It should be noted that although our method can be applied to a system of arbitrary dimension, we here obtain explicit expressions for the effective decoherence only in the case of the simplest possible system: a qubit. We hope to provide a discussion of the foundational implications of modeling bounded-size RFs by effective decoherence in a subsequent paper.

Finally, it is worth pointing out that the problem of communication in the presence of a bounded-size RF has interesting connections with a disparate set of topics in quantum information theory and the theory of quantum RFs:

Partially correlated RFs. When some information is known about the relative orientation of Alice and Bob's local RFs, they are said to share partially correlated RFs. This is a resource that interpolates between having and lacking a shared RF. Its quality can be characterized by the probability distribution over the relative orientation—the more peaked the distribution, the better the correlation. What can be achieved with this resource is an interesting question that has only begun to be addressed. We gain some insight into the question in this paper because the 'measure and re-orient' implementation of the recovery operation begins with a RF alignment protocol [1], [5]–[9] that leaves Alice and Bob holding partially correlated RFs.

Programmable operations. There have been many investigations into the possibility of encoding an operation into a quantum state such that the state can subsequently be used to implement the operation on another system. If the system into which the operation is encoded is bounded in size, then it is known that one can only achieve an approximate version of the operation or a perfect version with non-unit probability [17]–[19]. The token of the quantum RF in our communication protocol is an instance of a program that encodes the unitary that relates Alice's local RF to Bob's. Bob subsequently uses it to implement the inverse of this unitary on the system. Our results therefore provide interesting examples of both approximate and unambiguous programmable operations.

Measures of the quality of a quantum RF. Our results also contribute to the project of quantifying the extent to which a quantum RF of bounded size can stand in for one of unbounded size [20]–[22], an important element of a resource theory of quantum RFs. For instance, a measure of the strength of the effective decoherence associated with the bounded-size RF may serve as an operational measure of its quality.

Private channels. If no party besides Bob has a sample of Alice's RF, then Alice and Bob are said to possess a *private*-shared RF. These have been shown to constitute a novel kind of key that is useful for private communication schemes [23]. Our results establish a lower bound on the fidelity between input and output in private communication schemes that rely on Bob possessing a bounded-size token of Alice's RF. They also establish a bound on the probability of achieving perfect fidelity by post-selection. This cryptographic application provides a particularly useful perspective on Bob's recovery operation: the message is encoded in the relative orientation between the system and the token of Alice's RF in the same way that the plain-text in classical cryptography is encoded in the bit-wise parity of the cypher-text message and the key. Bob decodes by using the token of Alice's frame as a key.

Dense coding. As noted above in point (ii), the calibration-free communication scheme requires Alice to know the entire message to be sent prior to transmitting any systems to Bob if she is to achieve the maximum rate. In the communication scheme that first sets up a bounded-size RF, Alice can transmit to Bob the quantum token of her local RF prior to knowing anything about the message. Consequently, Alice can use the quantum channel at an early time, when it is perhaps cheaper, to enhance the communication capacity at a future time, when it is known what message is to be sent. Sending the frame token is therefore akin to establishing entanglement in a dense coding scheme [24]. One difference, however, is that the fidelity of communication is never perfect for a bounded-size token, whereas a single maximally entangled state allows for perfect communication of one qubit.

1.1. Mathematical preliminaries

In this section, we present some formal mathematical tools that are useful for describing classical and quantum RFs. We follow the notation of [1], to which we refer the reader for further details. Suppose Alice and Bob are considering a single quantum system described by a Hilbert space $\mathcal{H}$. Let this system transform via a representation of a group G relative to some RF. We will restrict our attention to Lie groups that are compact, so that they possess a group-invariant (Haar) measure $\mathrm{d}g$, and act on $\mathcal{H}$ via a *unitary* representation U, ensuring that they are completely reducible [25].

Let $g \in G$ be the group element that describes the passive transformation from Alice's to Bob's RF. Furthermore, suppose that g is completely unknown, i.e. that Alice's RF and Bob's are uncorrelated. It follows that if Alice prepares a system in the state ρ on $\mathcal{H}$ relative to her frame, then it is represented relative to Bob's frame by the state

$$\mathcal{G}[\rho] = \int_G \mathrm{d}g\, U(g)\rho U^\dagger(g)\,. \tag{6}$$

The action of the representation U of the (compact Lie) group G on $\mathcal{H}$ yields a very useful structure. It allows for a decomposition of the Hilbert space into a direct sum of *charge sectors*, labeled by an index q, where each charge sector carries an inequivalent representation $U^{(q)}$ of G. Each sector can be further decomposed into a tensor product of a subsystem $\mathcal{M}^{(q)}$ carrying an irreducible representation (irrep) of G and a subsystem $\mathcal{N}^{(q)}$ carrying a trivial representation of G. That is,

$$\mathcal{H} = \bigoplus_q \mathcal{M}^{(q)} \otimes \mathcal{N}^{(q)}. \tag{7}$$

Note that this tensor product does not correspond to the standard tensor product obtained by combining multiple qubits: it is *virtual* [26]. The spaces $\mathcal{M}^{(q)}$ and $\mathcal{N}^{(q)}$ are therefore *virtual subsystems*.

Expressed in terms of this decomposition of the Hilbert space, the map $\mathcal{G}$ takes a particularly simple form, given by

$$\mathcal{G}[\rho] = \sum_q (\mathcal{D}_{\mathcal{M}^{(q)}} \otimes \mathcal{I}_{\mathcal{N}^{(q)}})[\Pi^{(q)} \rho \Pi^{(q)}] \,, \tag{8}$$

where $\Pi^{(q)}$ is the projection into the charge sector q, $\mathcal{D}_{\mathcal{M}}$ denotes the trace-preserving operation that takes every operator on the Hilbert space $\mathcal{M}$ to a constant times the identity operator on that space, and $\mathcal{I}_{\mathcal{N}}$ denotes the identity map over operators in the space $\mathcal{N}$. A proof of this result is provided in [1].

Note that the operation $\mathcal{G}$ has the general form of *decoherence*. Whereas decoherence typically describes correlation with an environment to which one does not have access, in this case the decoherence describes correlation with a RF to which one does not have access [27].

2. Encoding

Consider a communication scheme wherein Alice prepares a system R in a pure quantum state $|e\rangle$ and sends it to Bob as a quantum sample of her RF, together with a system S (a collection of qubits for example) that is described by a quantum state ρ relative to her RF. Let R transform via the unitary representation U_R of G, and S via the unitary representation U_S. The lack of a shared RF between Alice and Bob implies that the transmitted composite RS is described relative to Bob's RF by the G-invariant state

$$\mathcal{E}(\rho) = \mathcal{G}_{RS}[|e\rangle\langle e| \otimes \rho] \,, \tag{9}$$

where $\mathcal{G}_{RS}$ is the G-twirling operation of (6) for the representation $U_{RS} = U_R \otimes U_S$ of G. This map $\mathcal{E}$ will be referred to as the *encoding map*. Note that its input space is $\mathcal{B}(\mathcal{H}_S)$ (the bounded operators on $\mathcal{H}_S$), while its output space is $\mathcal{B}(\mathcal{H}_R \otimes \mathcal{H}_S)$. It maps ρ to a G-invariant state of the composite RS.

It is useful to define the set of states

$$\{|g\rangle = U_R(g)|e\rangle | g \in G\} \,, \tag{10}$$

which form the orbit under the representation U_R of G of the fiducial state $|e\rangle$ (associated with the identity element of the group). By expressing the G-twirling operation explicitly and making use of these, we can express the encoding operation as

$$\mathcal{E}(\rho) = \int \mathrm{d}g \, |g\rangle\langle g| \otimes U_S(g) \rho U_S^\dagger(g) \,. \tag{11}$$

The encoding map clearly depends on the choice of the state $|e\rangle$ for the RF. We turn to this choice now.

2.1. Quantum reference frames

We begin by considering what properties of a quantum state make it a good representative of a RF for the group G (the case wherein the RF is associated with a coset space will be considered in section 6); for a more complete discussion, see [1, 10].

States $|g\rangle$ corresponding to different orientations of the RF must be distinct, so at the very least one requires that the fiducial state $|e\rangle$ is not invariant with respect to G or any subgroup thereof. To emulate a perfect RF for G, these states must in fact be perfectly distinguishable,

$$\langle g|g'\rangle = \delta(g^{-1}g') \,, \tag{12}$$

where $\delta(g)$ is the delta-function on G defined by $\int \mathrm{d}g\, \delta(g) f(g) = f(e)$ for any continuous function f of G, where e is the identity element in G. If the states $\{|g\rangle\}$ of equation (10) satisfy these requirements, then U_R is the *left regular representation* of G. In the case of a Lie group, the dimensionality of any system $\mathcal{H}_R$ that carries the regular representation must necessarily be infinite. We refer to such an infinite-dimensional quantum RF as *unbounded*; such systems and states were considered in [10].

If the Hilbert space dimensionality of the system R serving as a quantum RF is finite, then we say that the quantum RF is *of bounded size*. If the RF is associated with a Lie group, having a continuum of elements, then a bound on the size of the RF implies that the condition (12) cannot be satisfied precisely. In this case, a key question is: what state on R is the best approximation to a perfect RF? The answer will depend on the figure of merit for the task at hand, but we will make use of a generic construction [9, 10] that illustrates the key features.

Suppose the representation U_R reduces to a set of irreps $\{U_R^{(q)}\}$,

$$U_R(g) = \bigoplus_q U_R^{(q)}(g) \otimes I\,, \tag{13}$$

where the tensor product is the one appearing in the decomposition (7) of $\mathcal{H}_R$ and where I is the identity on $\mathcal{N}_R^{(q)}$. We are interested in a special subset of these irreps, namely, the $U_R^{(q)}$ that appear in the decomposition of U_R a number of times greater than or equal to their dimension d_q, i.e. those for which

$$d_q \equiv \dim \mathcal{M}_R^{(q)} \leqslant \dim \mathcal{N}_R^{(q)}\,. \tag{14}$$

We denote the set of q that label such irreps by Q_R and, in what follows, we will be restricting our attention to only these irreps. Also, for irreps $q \in Q_R$, choose an arbitrary subspace $\bar{\mathcal{N}}_R^{(q)} \subseteq \mathcal{N}_R^{(q)}$ with dimension d_q, i.e. with dimension equal to that of $\mathcal{M}_R^{(q)}$.

We now define a new Hilbert space $\bar{\mathcal{H}}_R$ as

$$\bar{\mathcal{H}}_R = \bigoplus_{q\in Q_R} \mathcal{M}_R^{(q)} \otimes \bar{\mathcal{N}}_R^{(q)}\,, \tag{15}$$

which is of dimension

$$D_R \equiv \sum_{q\in Q_R} d_q^2\,. \tag{16}$$

The state of R that we will use for our quantum RF is

$$|e\rangle = \sum_{q\in Q_R} \sqrt{\frac{d_q}{D_R}} \sum_{m=1}^{d_q} |q, m\rangle \otimes |\phi_{q,m}\rangle\,, \tag{17}$$

where $\{|q, m\rangle\}$ is an arbitrary basis for $\mathcal{M}^{(q)}$, and $\{|\phi_{q,m}\rangle\}$ an arbitrary basis for $\bar{\mathcal{N}}^{(q)}$. Note that the orbit of $|e\rangle$ under G has support in $\bar{\mathcal{H}}_R$.

The embedding $\bar{\mathcal{N}}_R^{(q)} \subseteq \mathcal{N}_R^{(q)}$ provides a way of embedding $|e\rangle$ in the original Hilbert space $\mathcal{H}_R$, and in addition U_R acts on the Hilbert space $\bar{\mathcal{H}}_R$ in the obvious way. If Q_R contained all irreps of G, then U_R would be the (left) regular representation, and for a Lie group the Hilbert space $\bar{\mathcal{H}}_R$ would be infinite dimensional. If the quantum RF is of bounded size, then a limited set of irreps appear in Q_R.

We note that, for the problem of optimally encoding a RF relative to a maximum likelihood figure of merit, given a general Hilbert space $\mathcal{H}_R$ the optimal states will not have this precise form [1, 9, 28, 29]. However, such optimal states do take the form of equation (17) when restricted to $\bar{\mathcal{H}}_R$. These are the states of interest here.

The restriction to irreps having the special property of equation (14) is in fact critical for our analysis, because only in this case can we define a useful *right* action of G on the Hilbert space [10]. Consider the representation V_R of G defined by its action on the covariant set (10) as

$$V_R(h)|g\rangle = |gh^{-1}\rangle\,, \quad g, h \in G\,. \tag{18}$$

To obtain an explicit form for this right action in terms of the decomposition of equation (15), we make use of the fact that the state $|e\rangle$ is maximally entangled across the virtual tensor products $\mathcal{M}_R^{(q)} \otimes \bar{\mathcal{N}}_R^{(q)}$. Thus, we have for any transformation $U_R^{(q)}(h)$ on a subsystem $\mathcal{M}_R^{(q)}$ the identity

$$\begin{aligned} U_R^{(q)}(h) \otimes I|e\rangle &= I \otimes U_R^{(q)}(h^{-1})^T|e\rangle \\ &= I \otimes U_R^{(q)}(h)^*|e\rangle\,, \end{aligned} \tag{19}$$

where ^{T} denotes the transpose, * the complex conjugate, and we have made use of the fact that $U_R^{(q)}$ is unitary. Given that the complex conjugate of a representation $U_R^{(q)}$ of G is also a representation of G (called the conjugate representation and denoted by $U_R^{(q^*)}$), we can define a representation V_R by

$$V_R(h) = \bigoplus_{q \in Q_R} I \otimes V_R^{(q^*)}(h)\,. \tag{20}$$

In contrast to U_R, the representation V_R acts on the subsystems $\bar{\mathcal{N}}_R^{(q)}$ irreducibly according to the conjugate representation q^*, and leaves the subsystems $\mathcal{M}_R^{(q)}$ invariant. Clearly, the two actions U_R and V_R commute. Furthermore, it is easy to verify that V_R satisfies equation (18).

As the states of the RF are restricted to the Hilbert space $\bar{\mathcal{H}}_R$, it is useful to consider our encoding operation $\mathcal{E}$ of equation (11) with fiducial state $|e\rangle$ of equation (17) as a map from $\mathcal{B}(\mathcal{H}_S)$ to $\mathcal{B}(\bar{\mathcal{H}}_R \otimes \mathcal{H}_S)$. For the remainder of this paper, we consider the encoding map to be defined thus.

Finally, we note that the map $\mathcal{E}$ with the fiducial state $|e\rangle$ chosen to be of the form (17) is unital. (Because the input and output spaces of $\mathcal{E}$ are of differing dimension, we define *unital* for such a trace-preserving map as one which maps the (normalized) completely mixed state to the completely mixed state.) This result is seen as

$$\begin{aligned} \mathcal{E}(I_S/d_S) &= \int \mathrm{d}g\, |g\rangle\langle g| \otimes I_S/d_S \\ &= \frac{1}{D_R} \sum_{q \in Q_R} I_{\mathcal{M}_R^{(q)}} \otimes I_{\bar{\mathcal{N}}_R^{(q)}} \otimes I_S/d_S \\ &= \frac{I_{\bar{\mathcal{H}}_R}}{D_R} \otimes \frac{I_S}{d_S}\,, \end{aligned} \tag{21}$$

where d_S is the dimension of $\mathcal{H}_S$. Here, we have used the fact that the maximally entangled states $\sum_{m=1}^{d_q} |q, m\rangle \otimes |\phi_{q,m}\rangle$ in equation (17) have reduced density matrices on $\bar{\mathcal{N}}_R^{(q)}$ that are proportional to the identity.

2.2. Relational subsystems

It is illustrative to investigate the action of the encoding map (11) (the fiducial state $|e\rangle$ will be assumed to be given by equation (17) except in the final section of the paper) and to explicitly identify the subsystems of $\bar{\mathcal{H}}_{RS} \equiv \bar{\mathcal{H}}_R \otimes \mathcal{H}_S$ into which the system's state is encoded. The details of this section require extensive use of the virtual tensor product structure of $\bar{\mathcal{H}}_{RS}$ induced by the unitary representation U_{RS} of G, given in equation (7), as well as an application of the Stinespring theorem for covariant maps [31]; this section may be skipped on first reading. To facilitate this, we first state the main result of this section prior to our detailed investigation of the encoding map.

Main result: According to equation (7), the joint Hilbert space $\bar{\mathcal{H}}_{RS}$ can be decomposed under the representation U_{RS} of G as

$$\bar{\mathcal{H}}_{RS} = \bigoplus_{q \in Q_{RS}} \mathcal{M}_{RS}^{(q)} \otimes \bar{\mathcal{N}}_{RS}^{(q)} , \tag{22}$$

where Q_{RS} are the set of irreps q of G that appear in the decomposition of U_{RS}. The encoding map (11) yields G-invariant density operators which, in terms of the decomposition (22), are block-diagonal in the irreps $q \in Q_{RS}$ and, within each block, have the form of a tensor product of the completely mixed state on the subsystem $\mathcal{M}_{RS}^{(q)}$ and some nontrivial state on the subsystem $\bar{\mathcal{N}}_{RS}^{(q)}$. Thus, the action of the encoding can be expressed as

$$\mathcal{E}(\rho) = \sum_{q \in Q_{RS}} (d_q^{-1} I_{\mathcal{M}_{RS}^{(q)}}) \otimes \mathcal{E}^{(q)}(\rho) , \tag{23}$$

where $I_{\mathcal{M}_{RS}^{(q)}}$ is the identity operator on $\mathcal{M}_{RS}^{(q)}$, and $\mathcal{E}^{(q)}$ is a trace-decreasing map from states on $\mathcal{H}_S$ to states on $\bar{\mathcal{N}}_{RS}^{(q)}$. We show below that, under the assumption that $\mathcal{H}_S$ is an irrep of G, each of these encodings $\mathcal{E}^{(q)}$ takes the form

$$\mathcal{E}^{(q)}(\rho) = \frac{d_q}{D_R} A^{(q)\dagger} (I_{\mathcal{K}^{(q)}} \otimes \rho) A^{(q)} , \tag{24}$$

where $I_{\mathcal{K}^{(q)}}$ is the identity operator on a Hilbert space $\mathcal{K}^{(q)}$ carrying an irrep q^* of G, and $A^{(q)} : \bar{\mathcal{N}}_{RS}^{(q)} \to \mathcal{K}^{(q)} \otimes \mathcal{H}_S$ is a linear map satisfying $A^{(q)\dagger} A^{(q)} = I_{\bar{\mathcal{N}}_{RS}^{(q)}}$. In addition, each map $A^{(q)}$ takes a very simple form, which depends on the irrep q. Specifically, there is a subset of irreps $Q_{RS}^{\text{ok}} \subset Q_{RS}$ such that, for $q \in Q_{RS}^{\text{ok}}$, the map $A^{(q)}$ is a bijective isometry, that is, a unitary; in these instances, the map $\mathcal{E}^{(q)}$ can be inverted and ρ can be recovered perfectly. For q not in Q_{RS}^{ok}, the map $A^{(q)}$ is an isometry that is not surjective, i.e. it maps onto a *proper subspace* of $\mathcal{K}^{(q)} \otimes \mathcal{H}_S$. The map $\mathcal{E}^{(q)}$ is not invertible in these cases.

We can identify the relational degrees of freedom in which the message is encoded by investigating how relational transformations act on the Hilbert space $\bar{\mathcal{H}}_{RS}$. The subsystems $\mathcal{M}_{RS}^{(q)}$ carry an irreducible representation of G corresponding to the collective action U_{RS} and describe collective degrees of freedom. In contrast, the subsystems $\bar{\mathcal{N}}_{RS}^{(q)}$ are relational. However, not all degrees of freedom in $\bar{\mathcal{N}}_{RS}^{(q)}$ describe relations of the system S to the RF R; some of these describe relations among the parts of R (or among the parts of S if the latter are composite systems). We seek to identify, for each irrep q, the precise subsystem of $\bar{\mathcal{N}}_{RS}^{(q)}$ into which the message state ρ is encoded.

The system Hilbert space $\mathcal{H}_S$ carries a representation U_S of G. If we act with G on the system but not on the RF, this will induce a relative transformation of the two; however, this

action alone is not G-invariant. While it is possible to construct a G-invariant action of U_S by using the techniques of [1, 10], it is much more straightforward to make use of the right action V_R of G defined in equation (18). This action commutes with the left action U_R, and thus also commutes with the collective action U_{RS} of G. By acting with $V_R(h)$ for $h \in G$ on a state $\rho_{RS} = \mathcal{E}(\rho)$ of the form (9), we have

$$\begin{aligned} V_R(h)\mathcal{E}(\rho)V_R^\dagger(h) &= \int \mathrm{d}g\, |gh^{-1}\rangle\langle gh^{-1}| \otimes U_S(g)\rho U_S^\dagger(g) \\ &= \int \mathrm{d}g'\, |g'\rangle\langle g'| \otimes U_S(g'h)\rho U_S^\dagger(g'h) \\ &= \mathcal{E}(U_S(h)\rho U_S^\dagger(h))\,, \end{aligned} \tag{25}$$

where we have used the invariance of the Haar measure. The action of $V_R(h)$ on ρ_{RS} yields another invariant state, but one which is now an encoding of the transformed state $U_S(h)\rho U_S^\dagger(h)$. Thus, $V_R(h)$ acts as a transformation of the relation between S and R. A map $\mathcal{E}$ satisfying equation (25) is called *G-covariant*.

As V_R is a relational action, it acts on the subsystems $\bar{\mathcal{N}}_{RS}^{(q)}$ in equation (22); we now decompose these subsystems according to the irreps of G under the action of V_R, and in doing so identify the subsystems in which we find the image of ρ under the encoding map.

At this stage, we restrict our attention to the case where U_S is an irrep of G, labeled q_S. It appears straightforward (although with substantially more burdensome notation) to extend our results to the general case wherein this restriction is relaxed. Indeed, the $U(1)$ example considered in section 4 provides evidence of the generality of our theorem. However, we do not consider the general case here.

Recall that the RF R has a Hilbert space given by equation (15), and the system's Hilbert space is $\mathcal{H}_S = \mathcal{M}_S^{(q_S)}$. Thus,

$$\begin{aligned} \bar{\mathcal{H}}_{RS} &= \bar{\mathcal{H}}_R \otimes \mathcal{H}_S \\ &= \bigoplus_{q' \in Q_R} \left(\mathcal{M}_R^{(q')} \otimes \mathcal{M}_S^{(q_S)}\right) \otimes \bar{\mathcal{N}}_R^{(q')} \\ &= \bigoplus_{q' \in Q_R} \left(\bigoplus_{q|(q',q_S)\to q} \mathcal{M}_{RS}^{(q)} \otimes \mathcal{V}_q^{q',q_S} \right) \otimes \bar{\mathcal{N}}_R^{(q')} \\ &= \bigoplus_{q \in Q_{RS}} \mathcal{M}_{RS}^{(q)} \otimes \left(\bigoplus_{q' \in Q_R|(q',q_S)\to q} \bar{\mathcal{N}}_R^{(q')} \otimes \mathcal{V}_q^{q',q_S} \right)\,, \end{aligned} \tag{26}$$

where $(q', q_S) \to q$ denotes that the irreps q' and q_S couple to the irrep q, $\mathcal{V}_q^{q',q_S}$ is the multiplicity space for the irrep q in tensor representation $U_R^{(q')} \otimes U_S$, and where Q_{RS} is the set of all irreps that are obtained by coupling some irrep $q' \in Q_R$ to q_S. Comparing the expression above with equation (22), the subsystems $\bar{\mathcal{N}}_{RS}^{(q)}$ are given by

$$\bar{\mathcal{N}}_{RS}^{(q)} = \bigoplus_{q' \in Q_R|(q',q_S)\to q} \bar{\mathcal{N}}_R^{(q')} \otimes \mathcal{V}_q^{q',q_S}\,. \tag{27}$$

We use the fact that if $(q', q_S) \to q$, then $(q^*, q_S) \to (q')^*$ [31], and that $\mathcal{V}_q^{q',q_S} \simeq \mathcal{V}_{(q')^*}^{q^*,q_S}$ [10]. Thus,

$$\bar{\mathcal{N}}_{RS}^{(q)} = \bigoplus_{q' \in Q_R | (q^*, q_S) \to (q')^*} \bar{\mathcal{N}}_R^{(q')} \otimes \mathcal{V}_{(q')^*}^{q^*,q_S} . \tag{28}$$

where each subsystem $\bar{\mathcal{N}}_R^{(q')}$ on the right-hand side carries an irrep $(q')^*$ of G under the action V_R. (We note that in the examples presented in the latter sections, with groups $U(1)$ and $SU(2)$, the subsystems $\mathcal{V}$ are trivial and can be ignored.)

At this stage, we will make use of the G-covariance of the encoding map $\mathcal{E}$, given by equation (25), to determine how the message is encoded into the relational subsystems $\bar{\mathcal{N}}_{RS}^{(q)}$. As the state $\mathcal{E}(\rho)$ is G-invariant under the action of U_{RS} for any ρ, it can be expressed according to the Hilbert space decomposition (22) as

$$\mathcal{E}(\rho) = \sum_{q \in Q_{RS}} \left(d_q^{-1} I_{\mathcal{M}_{RS}^{(q)}} \right) \otimes \mathcal{E}^{(q)}(\rho) , \tag{29}$$

where $I_{\mathcal{M}_{RS}^{(q)}}$ is the identity operator on $\mathcal{M}_{RS}^{(q)}$ and $\mathcal{E}^{(q)}(\rho)$ is an (unnormalized) density operator on $\bar{\mathcal{N}}_{RS}^{(q)}$. This expression defines a set of trace-decreasing superoperators $\mathcal{E}^{(q)} : \mathcal{B}(\mathcal{H}_S) \to \mathcal{B}(\bar{\mathcal{N}}_{RS}^{(q)})$; note that the latter can be naturally embedded in the full multiplicity spaces $\mathcal{N}_{RS}^{(q)}$ of the combined system. From equation (21), we see that the maps $\mathcal{E}^{(q)}$ are also unital in that $\mathcal{E}^{(q)}(I_S)$ is proportional (because $\mathcal{E}^{(q)}$ is trace-decreasing) to the identity on $\bar{\mathcal{N}}_{RS}^{(q)}$. Also, as V_R commutes with U_{RS}, we have that each term $\mathcal{E}^{(q)}$ is itself G-covariant, satisfying $V_R^{(q^*)}(h)\mathcal{E}^{(q)}(\rho)V_R^{(q^*)\dagger}(h) = \mathcal{E}^{(q)}(U_S(h)\rho U_S^\dagger(h))$.

We now make use of the Stinespring theorem for covariant CP maps [30]; in particular, we use a form due to Keyl and Werner [31] for unital covariant CP maps. There exists another unitary representation $W^{(q^*)}$ of G on a space $\mathcal{K}^{(q)}$ and an *intertwiner* (linear map)

$$A^{(q)} : \bar{\mathcal{N}}_{RS}^{(q)} \to \mathcal{K}^{(q)} \otimes \mathcal{H}_S , \tag{30}$$

satisfying $A^{(q)\dagger}A^{(q)} = I_{\bar{\mathcal{N}}_{RS}^{(q)}}$ with

$$A^{(q)} V_R^{(q^*)}(h) = W^{(q^*)}(h) \otimes U_S(h) A^{(q)} , \tag{31}$$

such that

$$\mathcal{E}^{(q)}(\rho) = \frac{d_q}{D_R} A^{(q)\dagger}(I_{\mathcal{K}^{(q)}} \otimes \rho) A^{(q)} . \tag{32}$$

The form of equation (28) allows us to identify a suitable Stinespring extension. The representation $V_R^{(q^*)}$ acts on $\bar{\mathcal{N}}_{RS}^{(q)}$ through what appears to be (ignoring the limits on the sum $q' \in Q_R$) a tensor representation of an irrep q^* with an irrep q_S. Thus, we can choose our Stinespring extension in a minimal way such that $W^{(q^*)}$ acts on $\mathcal{K}^{(q)}$ irreducibly as the irrep q^* of G. The operators $A^{(q)}$ intertwine the representation $V_R^{(q^*)}$ with the collective representation $W^{(q^*)} \otimes U_S$ on $\mathcal{K}^{(q)} \otimes \mathcal{H}_S$. We now consider two cases:

Case A: If $q \in Q_{RS}$ is such that, for all q' obtained via $(q^*, q_S) \to q'$ then $q' \in Q_R$ (i.e., Q_R contains all of the irreps q' that one can obtain by $(q^*, q_S) \to (q')^*$), then the direct sum Hilbert space in equation (28) is given by

$$\bar{\mathcal{N}}_{RS}^{(q)} \simeq \mathcal{K}^{(q)} \otimes \mathcal{H}_S , \tag{33}$$

where $\simeq$ denotes that these spaces are unitarily equivalent; that is, the map $A^{(q)}$ is a bijective isometry and simply represents the Clebsch–Gordan transformation relating the tensor product of two irreps with the direct sum decomposition of $\bar{\mathcal{N}}_{RS}^{(q)}$ given in (28). Let $Q_{RS}^{\text{ok}} \subseteq Q_{RS}$ denote the set of irreps satisfying this condition.

Case B: If, however, $q \in Q_{RS}$ is such that the condition of case A fails (i.e. Q_R does *not* contain all of the irreps q' that one can obtain by coupling q^* and q_S), then the intertwiner is no longer surjective. Rather, the intertwiner maps $\bar{\mathcal{N}}_{RS}^{(q)}$ onto a proper subspace of $\mathcal{K}^{(q)} \otimes \mathcal{H}_S$, specifically the subspace defined by the carrier space of the irreps $(q')^*$, with $q' \in Q_R$, obtained through the coupling of the irrep q^* on $\mathcal{K}^{(q)}$ with the irrep q_S on $\mathcal{H}_S$. (This space is necessarily a proper subspace of $\mathcal{K}^{(q)} \otimes \mathcal{H}_S$ because, by the conditions of case B, Q_R does not contain all irreps obtained in this coupling.) A set of basis states for this subspace can be calculated explicitly in any particular instance using the Clebsch–Gordan coefficients for the group G.

We now turn to the probabilities of each of these cases. We note that $p_q = \text{Tr}[\Pi_q \mathcal{E}(\rho)] = \text{Tr}[\mathcal{E}^{(q)}(\rho)]$ is the probability that the system is encoded into the irrep q. We now prove that, for the case where $\mathcal{H}_S$ carries an irrep U_S of G, this probability is independent of ρ. Using equation (32), we have

$$\begin{aligned} p_q &= \frac{d_q}{D_R} \text{Tr}_{\bar{\mathcal{N}}_{RS}^{(q)}} \left[A^{(q)\dagger} (I_{\mathcal{K}^{(q)}} \otimes \rho) A^{(q)} \right] \\ &= \int \text{d}g \frac{d_q}{D_R} \text{Tr}_{\bar{\mathcal{N}}_{RS}^{(q)}} \left[V^{(q^*)}(g) A^{(q)\dagger} (I_{\mathcal{K}^{(q)}} \otimes \rho) A^{(q)} V^{(q^*)}(g)^{-1} \right] \\ &= \frac{d_q}{D_R} \text{Tr}_{\bar{\mathcal{N}}_{RS}^{(q)}} \left[A^{(q)\dagger} (I_{\mathcal{K}^{(q)}} \otimes \int \text{d}g \, U_S(g) \rho U_S(g)^{-1}) A^{(q)} \right], \end{aligned} \tag{34}$$

where in the second line we have used the G-invariance of $\mathcal{E}^{(q)}$ and in the third line we have used equation (31). Because $\mathcal{H}_S$ is an irrep, it follows that $\int \text{d}g \, U_S(g) \rho U_S(g)^{-1} = I_S/d_S$ where $d_S = \dim \mathcal{H}_S$, and therefore p_q is independent of ρ for all q. The $SU(2)$ case, presented in section 5, provides an explicit example of this.

We note that for the general case, where the system does not carry an irrep of G, then this probability can be state-dependent. For example, if $\mathcal{H}_S$ is a direct sum of irreps q_S, then $\int \text{d}g \, U_S(g) \rho U_S(g)^{-1} = \sum_{q_S} \text{Tr}(\rho \Pi_S^{(q_S)}) \Pi_S^{(q_S)}$ where $\Pi_S^{(q_S)}$ is the projector onto the q_S irrep of $\mathcal{H}_S$. In this case, for $q \in Q_{RS}^{\text{ok}}$ (where A^q is unitary), we have $p_q = d_q^2/D_R$, independent of ρ. However, for $q \notin Q_{RS}^{\text{ok}}$, the weight p_q can depend on ρ. This occurs for the $U(1)$ case, as seen explicitly in section 4.

With each map $\mathcal{E}^{(q)}$ now defined through equation (32), we can explicitly express $\mathcal{E}$ in Kraus operator form as $\mathcal{E}(\rho) = \sum_{q,m,\mu} K_{q,m,\mu} \rho K_{q,m,\mu}^\dagger$, where

$$K_{q,m,\mu} = \frac{1}{\sqrt{D_R}} |q, m\rangle \otimes A^{(q)\dagger} |q, \mu\rangle \,, \tag{35}$$

and where $|q, m\rangle$ is a basis for $\mathcal{M}_{RS}^{(q)}$ and $|q, \mu\rangle$ is a basis for $\mathcal{K}^{(q)}$.

Finally, we point out a useful expression for $\mathcal{E}^{(q)}$ (which applies regardless of whether $\mathcal{H}_S$ carries an irrep of G). From equation (29), it is clear that

$$\mathcal{E}^{(q)}(\rho) = \text{Tr}_{\mathcal{M}_{RS}^{(q)}} (\Pi_q \mathcal{E}(\rho) \Pi_q) \,. \tag{36}$$

Combining this with the expression for $\mathcal{E}$ in equation (9) and making use of equation (8), we obtain

$$\mathcal{E}^{(q)}(\rho) = \mathrm{Tr}_{\mathcal{M}_{RS}^{(q)}}\left[\Pi_q(|e\rangle\langle e| \otimes \rho)\Pi_q\right]. \tag{37}$$

This form will be used frequently when working out explicit examples.

3. Decoding

In the communication protocol we are considering, Bob's task is to recover the quantum message ρ by implementing a decoding map $\mathcal{R}\colon \mathcal{B}(\bar{\mathcal{H}}_R \otimes \mathcal{H}_S) \to \mathcal{B}(\mathcal{H}_S)$. A useful recovery map to consider is the following:

$$\mathcal{R} = D_R \mathcal{E}^\dagger, \tag{38}$$

where the adjoint for superoperators is defined relative to the Hilbert–Schmidt inner product, $\mathrm{Tr}(A\mathcal{E}^\dagger[B]) = \mathrm{Tr}(\mathcal{E}[A]B)$. The map $\mathcal{R}$ is completely positive and linear, because the superoperator adjoint preserves these features. It is also trace-preserving. To see this fact, observe that $\mathcal{E}(I_S) = (I_R/D_R) \otimes I_S$, where $I_R = D_R \int \mathrm{d}g |g\rangle\langle g|$ is the identity operator on $\bar{\mathcal{H}}_R$; consequently, for $\rho_{RS} \in \mathcal{B}(\bar{\mathcal{H}}_R \otimes \mathcal{H}_S)$, we have $\mathrm{Tr}[\mathcal{R}(\rho_{RS})] = \mathrm{Tr}[\rho_{RS}\mathcal{R}^\dagger(I_S)] = \mathrm{Tr}[\rho_{RS}]$. We have therefore verified that $\mathcal{R}$ is a valid quantum operation that can be implemented deterministically.

Assuming that there is no prior information about the input state to $\mathcal{E}$, the map $D_R\mathcal{E}^\dagger$ is precisely the 'approximate reversal' operation for $\mathcal{E}$ proposed by Barnum and Knill [32], which yields an error no more than twice that of the optimal reversal operation. The error here is defined in terms of the deviation from unity of the average entanglement fidelity for an arbitrary input ensemble.

3.1. 'Measure and re-orient' implementation of decoding

Given a superoperator $\mathcal{A}$, the adjoint $\mathcal{A}^\dagger$ is easily determined through a Kraus decomposition of $\mathcal{A}$. Specifically, if $\mathcal{A}[\rho] = \sum_i K_i \rho K_i^\dagger$ then $\mathcal{A}^\dagger[\rho] = \sum_i K_i^\dagger \rho K_i$. The expression (11) for the encoding map $\mathcal{E}$ provides one Kraus decomposition: the covariant set of operators $\{K(g), g \in G\}$, where $K(g) = |g\rangle \otimes U_S(g)$. It follows that a covariant set of Kraus operators for $\mathcal{E}^\dagger$ is $\{K^\dagger(g), g \in G\}$ where $K^\dagger(g) = \langle g| \otimes U_S^\dagger(g)$ and consequently

$$\mathcal{R}[\rho_{RS}] = D_R \int \mathrm{d}g (\langle g| \otimes U_S^\dagger(g))\rho_{RS}(|g\rangle \otimes U_S(g)). \tag{39}$$

From this expression, we see that one way in which $\mathcal{R}$ can be implemented is as follows: measure the covariant positive operator-valued measure (POVM) $\{D_R|g\rangle\langle g|\mathrm{d}g\}$ on R, then implement the unitary $U_S(g^{-1})$ on S, and finally discard R and the measurement result g. We refer to this as the 'measure and re-orient' implementation of the decoding map. (It is the adjoint of the 'prepare and G-twirl' implementation of the encoding map.)

So we see that the decoding map we are considering is in fact the most obvious recovery scheme one can imagine! Bob simply estimates the relative orientation between Alice's RF and his own by measuring how the sample R of Alice's RF is oriented, then re-orients the system appropriately (i.e. in such a way that it is finally oriented relative to his RF in precisely the way that it was initially oriented relative to Alice's RF). One can view the system R as a cryptographic key or calibrating system that contains the information for how to recover the

quantum state of S. It is noteworthy that this implementation of Bob's decoding map does not require any entangling operations between R and S. Bob can achieve it with local operations and classical communication (LOCC) between R and S. Because Bob does not need to possess S to implement the appropriate measurement on R, it follows that Alice can subsequently transmit an arbitrary number of systems and Bob can decode these with the same fidelity as the first.

3.1.1. Effective decoherence. Consider the action of the decoding map on states $\rho_{RS} = \mathcal{E}(\rho)$, i.e. on states of the form of equation (11). After a measurement on R having outcome g', followed by a transformation $U_S(g')^{-1}$ to system S, the reduced density operator on S is

$$\begin{aligned}\mathcal{R}\circ\mathcal{E}[\rho] &= D_R \int \mathrm{d}g\, |\langle g|g'\rangle|^2\, U_S((g')^{-1}g)\rho U_S^\dagger((g')^{-1}g) \\ &= D_R \int \mathrm{d}g\, |\langle e|g\rangle|^2\, U_S(g)\rho U_S^\dagger(g)\,, \end{aligned} \tag{40}$$

where the simplification occurs because $\mathrm{d}g$ is invariant. Note that the result is independent of the outcome g'. It is straightforward to check that this state is normalized, as $D_R^{-1} = \int \mathrm{d}g\, |\langle e|g\rangle|^2$. This is precisely how a state ρ relative to Alice's frame would be redescribed relative to Bob's frame if their relative orientation g was known to be distributed according to the probability distribution $p(g) = D_R|\langle e|g\rangle|^2$. If $|\langle g|e\rangle|^2$ as a function of g is highly peaked around the identity group element e, then the only unitary that will contribute significantly in the integral will be the identity operation, and we will have $\mathcal{R}\circ\mathcal{E}[\rho] \simeq \rho$. It is the narrowness of the distribution $|\langle g|e\rangle|^2$, a measure of the quality of the quantum RF, that determines the degree to which one can recover the quantum information.

We see that for bounded-size samples of Alice's RF, the decoding map we have described achieves *approximate error correction*. Further on, we will show that the degree to which it deviates from perfect error correction is inversely proportional to the size of the quantum RF.

3.2. 'Extract from the relational subsystems' implementation of decoding

Recall that the 'measure and re-orient' implementation of the recovery operation $\mathcal{R}$ was inferred from the adjoint of the Kraus decomposition $\{|g\rangle \otimes U_S(g) \mid g \in G\}$ of $\mathcal{E}$. We exhibited a different Kraus decomposition of the encoding operation in equation (35). The adjoint of the latter provides a novel Kraus decomposition of $\mathcal{R}$ and therefore also a new way of implementing the recovery operation. We will refer to it as the 'extract from the relational subsystems' implementation. We find that $\mathcal{R} = D_R\mathcal{E}^\dagger$ can be written as

$$\mathcal{R}(\rho_{RS}) = \sum_{q\in Q_{RS}} \mathcal{R}^{(q)}\left(\mathrm{Tr}_{\mathcal{M}_{RS}^{(q)}}\left[\Pi^{(q)}\rho_{RS}\Pi^{(q)}\right]\right), \tag{41}$$

where we define

$$\mathcal{R}^{(q)}(\cdot) = \mathrm{Tr}_{\mathcal{K}^{(q)}}\left[A^{(q)}(\cdot)A^{(q)\dagger}\right], \tag{42}$$

as a map from $\mathcal{B}(\bar{\mathcal{N}}_{RS}^{(q)})$ to $\mathcal{B}(\mathcal{H}_S)$. Recalling the form of the encoding map $\mathcal{E}^{(q)}$ of equation (24), we see that $\mathcal{R}^{(q)} = d_q\mathcal{E}^{(q)\dagger}$.

This implementation of the decoding map $\mathcal{R}$ differs from the 'measure and re-orient' scheme in that it requires joint (i.e. non-separable) operations on R and S. Specifically, it is implemented via a joint unitary on RS followed by a trace on R.

Finally, we highlight another decomposition of $\mathcal{R}^{(q)}$ that will be useful to us further on. It is the one obtained by taking the adjoint of equation (37),

$$\mathcal{R}^{(q)}(\cdot) = d_q \langle e| I_{\mathcal{M}_{RS}^{(q)}} \otimes (\cdot) |e\rangle \,. \tag{43}$$

3.2.1. Effective decoherence. Given equations (23) and (41), the composition $\mathcal{R} \circ \mathcal{E}$ can be written as

$$\mathcal{R} \circ \mathcal{E}[\rho] = \sum_{q \in Q_{RS}} \mathcal{R}^{(q)} \circ \mathcal{E}^{(q)}[\rho] \,. \tag{44}$$

Substituting the expressions for $\mathcal{E}^{(q)}$ and $\mathcal{R}^{(q)}$ in equations (32) and (42), we obtain

$$\mathcal{R} \circ \mathcal{E}[\rho] = \sum_{q \in Q_{RS}} \frac{d_q}{D_R} \mathrm{Tr}_{\mathcal{K}^{(q)}} \left[A^{(q)} A^{(q)\dagger} (I_{\mathcal{K}^{(q)}} \otimes \rho) A^{(q)} A^{(q)\dagger} \right] . \tag{45}$$

We now consider the two subsets of Q_{RS} from section 2.2. In case A, where $q \in Q_{RS}^{\mathrm{ok}}$, the intertwiner $A^{(q)}$ is a bijective isometry, and consequently $A^{(q)} A^{(q)\dagger}$ is the identity and $\mathcal{R}^{(q)} \circ \mathcal{E}^{(q)}[\rho] = (d_q^2 / D_R)\rho$. Therefore, in this case the quantum information is perfectly recovered by the decoding map. In case B, however, $P^{(q)} = A^{(q)} A^{(q)\dagger}$ is a nontrivial projection on $\mathcal{K}^{(q)} \otimes \mathcal{H}_S$ and the recovery is not perfect. We can express equation (45) as

$$\mathcal{R} \circ \mathcal{E}[\rho] = \left(\sum_{q \in Q_{RS}^{\mathrm{ok}}} \frac{d_q^2}{D_R} \right) \rho + \sum_{q \notin Q_{RS}^{\mathrm{ok}}} \frac{d_q}{D_R} \mathrm{Tr}_{\mathcal{K}^{(q)}} \left[P^{(q)} (I_{\mathcal{K}^{(q)}} \otimes \rho) P^{(q)} \right] . \tag{46}$$

This is just an alternative Kraus decomposition of the effective decoherence map of equation (40).

3.3. Comparison of implementations

We have shown two very distinct ways of implementing one and the same decoding operation. If we describe the RF token R as an ancilla, then what we have is an example wherein a single map can be implemented either by a joint unitary followed by a trace on the ancilla, or by a measurement of the ancilla followed by a unitary rotation on the system that depends on the outcome of the measurement. The existence of many different implementations of an operation is familiar in quantum information theory. For instance, Griffiths and Niu have made use of a similar multiplicity of possibilities for the optimal eavesdropping strategies in quantum cryptography [33].

The multiplicity of ways of implementing a single operation is analogous to the multiplicity of mixtures that lead to the same density operator. Two Kraus decompositions of our G-invariant recovery operation differ in their transformation properties under the group: one is a G-covariant set of operators (a continuous set in the case of a Lie group) and the other is a discrete set of G-invariant operators. Similarly, a G-invariant density operator ρ on a finite-dimensional Hilbert space admits two sorts of convex decompositions: a spectral decomposition with a discrete number of G-invariant elements, and the decomposition induced by ρ-distortion of a G-covariant POVM (continuous if G is a Lie group) [34].

Recognizing this multiplicity of convex decompositions and the fact that no particular decomposition is preferred has been important for resolving many conceptual confusions [35]. Furthermore, each decomposition may yield important insights. In quantum optics, for example,

a Poissonian mixture of number eigenstates is equivalent to a uniform mixture over coherent states with the same mean number but differing in phase. The decomposition into states with well-defined phase is particularly useful for making predictions about wave-like phenomena, such as interference experiments, whereas the number state decomposition is best for particle-like phenomena, such as determining number statistics [36].

Similarly, each of the two decompositions we have provided of our decoding operation provides some insight into our problem. The 'measure and re-orient' scheme is clearly the most intuitive and demonstrates that joint operations on reference token and system are not necessary to implement our recovery map. The 'extract from relational subsystems' scheme demonstrates that if Bob begins by measuring the irrep of the composite of R and S, he learns whether the state was in a 'good' irrep or not and consequently whether or not he has achieved a perfect decoding. This sort of post-selectively perfect decoding operation is discussed in the following section.

3.4. Post-selectively perfect decoding

Thus far we have only judged decoding schemes by their average performance. It is also possible to say something about the best and worst case performance. The 'measure and re-orient' scheme is not particularly interesting in this regard: one achieves precisely the same fidelity of recovery regardless of the outcome of the covariant measurement on the RF token, so that the best and worst case recoveries are equivalent to the average. On the other hand, in the 'extract from the relational subsystems' scheme, we found that the fidelity of the recovery depends on the irrep of the composite of RF token and system into which the input state was encoded. Furthermore, given that the decoding operation was incoherent over these irreps, it is always possible to make a projective measurement that distinguishes these. Depending on the measurement outcome, one can achieve decodings with fidelities that are sometimes better and sometimes worse than the average.

Indeed, by enhancing the 'extract from the relational subsystems' scheme with such a measurement, Bob can achieve *perfect* decoding with some probability. Specifically, if he finds one of the 'good' irreps, $q \in Q_{RS}^{\text{ok}}$, then $\mathcal{E}^{(q)}$ is invertible and the decoding operation $\mathcal{R}^{(q)}$ of equation (42) recovers the quantum message perfectly. (Of course, if he achieves one of the 'bad' irreps, $q \notin Q_{RS}^{\text{ok}}$, then he achieves a decoding that is worse than the average.) Recalling equation (46) and making use of equation (16), the probability of perfect recovery is

$$p_{\text{perfect}} = \frac{1}{D_R} \sum_{q \in Q_{RS}^{\text{ok}}} d_q^2 = \frac{\sum_{q \in Q_{RS}^{\text{ok}}} d_q^2}{\sum_{q' \in Q_R} d_{q'}^2}. \tag{47}$$

Such a decoding scheme achieves post-selectively perfect error correction [37]. It is akin to achieving unambiguous discrimination of a set of non-orthogonal quantum states [38].

For this implementation of the decoding, note that Bob must be able to store the quantum token of Alice's RF coherently until the time when he receives the message systems. Another point worth noting: if Alice is sending a large number of systems and Bob wishes to implement probabilistically perfect error correction on some subset of them, he must wait until he has collected all of the systems in that subset. The reason is that he must perform a joint measurement on the composite of these and the RF token. Furthermore, after his measurement is complete, he has disrupted the state of the RF token and he can no longer achieve perfect

error correction for any other systems. The tradeoffs involved in such post-selectively perfect decoding schemes are an interesting topic for future research.

Finally, we can consider modifying the encoding operation rather than the decoding in a similar way. Note that if, immediately after implementing her encoding operation, Alice implements a projective measurement of the irrep of the composite of RF token and system, she can come to know whether a subsequent decoding operation will achieve a perfect recovery or not. In addition, if it happens that Alice has a classical description of the quantum message rather than merely having a sample, then she can prepare the quantum state many times and only initiate transmission when her measurement finds one of the 'good' irreps. In this case, the quantum message is perfectly encoded into a pure G-invariant state of the composite of system and RF token. Such a scheme therefore achieves a relational encoding akin to the one presented in Bartlett *et al* [2]. The precise connection of our results to the latter encoding is an interesting topic for future research (as is the application of the mathematical tools developed here to the general problem of calibration-free communication schemes discussed in the introduction).

4. Example: phase reference

The quantum state of a harmonic oscillator is always referred to some phase reference [35]. In this example, we consider using one quantum harmonic oscillator (a single mode) as a phase reference for another, and investigate the effect of bounding the maximum number N_R of excitations in the phase reference. Specifically, consider the single-mode RF to be prepared in the bounded-size phase eigenstate

$$\left|e_{N_R}\right\rangle = \frac{1}{\sqrt{N_R+1}} \sum_{n=0}^{N_R} |n\rangle \ , \tag{48}$$

where $|n\rangle$ is the Fock state with n excitations. This state is of the form of our general state (17) for the case of $G = U(1)$. For the system, we consider a qubit encoded in the two-dimensional subspace spanned by $|0\rangle$ and $|1\rangle$. Note that the system we consider does not carry an irrep of $U(1)$, and in fact $U(1)$ has only one-dimensional irreps. Because our main result concerning the representation of the encoding map, presented in section 2.2, was only proven under the assumption that $\mathcal{H}_S$ is an irrep, the $U(1)$ example cannot be presented as a special case of this result. Nonetheless, we find the $U(1)$ example to be in accord with the general result, suggesting that our theorem applies more generally.

For simplicity, we consider a system prepared in an arbitrary pure state

$$\rho = |\psi\rangle\langle\psi| \,, \qquad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle. \tag{49}$$

Our results will directly extend to the mixed-state case via the linearity of convex combination.

4.1. Effective decoherence

The overlap of the RF state $|e_{N_R}\rangle$ with its rotated version is

$$|\langle e_{N_R}|U_R(\theta)|e_{N_R}\rangle|^2 = \left|\sum_{n=0}^{N_R} \mathrm{e}^{\mathrm{i}\theta n}\right|^2 = \frac{1-\cos\,(N_R+1)\,\theta}{1-\cos\,\theta} \,. \tag{50}$$

Rotations in $U(1)$ act on the qubit system state as

$$U_S(\theta)\rho U_S(\theta)^\dagger = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* e^{i\theta} \\ \alpha^*\beta e^{-i\theta} & |\beta|^2 \end{pmatrix}. \tag{51}$$

Evaluating equation (40) then gives

$$\mathcal{R}\circ\mathcal{E}(\rho) \propto \int \frac{d\theta}{2\pi}\frac{1-\cos[(N_R+1)\theta]}{1-\cos\theta}\begin{pmatrix} |\alpha|^2 & \alpha\beta^* e^{i\theta} \\ \alpha^*\beta e^{-i\theta} & |\beta|^2 \end{pmatrix}. \tag{52}$$

Noting that

$$\int \frac{d\theta}{2\pi}\frac{1-\cos[(N_R+1)\theta]}{1-\cos\theta} = N_R+1\,, \tag{53}$$

$$\int \frac{d\theta}{2\pi}\frac{1-\cos[(N_R+1)\theta]}{1-\cos\theta}e^{i\theta} = N_R\,, \tag{54}$$

which also gives the normalization, we have

$$\begin{aligned}\mathcal{R}\circ\mathcal{E}(\rho) &= \frac{N_R}{N_R+1}\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} + \frac{1}{N_R+1}\begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix} \\ &= \left(\frac{N_R}{N_R+1}\mathcal{I} + \frac{1}{N_R+1}\mathcal{G}\right)[\rho]\,,\end{aligned} \tag{55}$$

where $\mathcal{G}$ here denotes the $U(1)$-twirling operation (the dephasing map). It follows that in the 'measure and re-orient' scheme for decoding, regardless of the outcome of the measurement, the reduced density operator is with probability $N_R/(N_R+1)$ the state $\alpha|0\rangle+\beta|1\rangle$, while with probability $1/(N_R+1)$ it is completely dephased in the $|0\rangle, |1\rangle$ basis. The overall effect of encoding and decoding is to implement a partial dephasing.

4.2. Relational subsystems

Because the irreps of $U(1)$ are all one-dimensional, we have $\dim \mathcal{M}_{RS}^{(N)} = 1$ and consequently, by equation (23), the encoding operation $\mathcal{E}$ may be expressed simply as $\mathcal{E}(\rho) = \sum_N \mathcal{E}^{(N)}(\rho)$. By virtue of equation (37), each operation $\mathcal{E}^{(N)}(\rho)$ may in turn be expressed as

$$\mathcal{E}^{(N)}(\rho) = \Pi^{(N)}[|e_{N_R}\rangle\langle e_{N_R}|\otimes\rho]\Pi^{(N)}\,, \tag{56}$$

which evaluates for different values of N as:

$$\mathcal{E}^{(N)}(\rho) = \begin{cases} \alpha\,|0,0\rangle\,, & N=0, \\ \alpha\,|N,0\rangle + \beta\,|N-1,1\rangle\,, & 0<N<N_R+1, \\ \beta\,|N_R,1\rangle\,, & N=N_R+1\,. \end{cases} \tag{57}$$

The decoding operation has the form $\mathcal{R}=\sum_N \mathcal{R}^{(N)}$ where $\mathcal{R}^{(N)} \propto \mathcal{E}^{(N)\dagger}$. One easily verifies that $\mathcal{R}^{(N)}$ maps $|N,0\rangle$ to $|0\rangle$ and $|N-1,1\rangle$ to $|1\rangle$, so that

$$(\mathcal{R}^{(N)}\circ\mathcal{E}^{(N)})[\rho] \propto \begin{cases} |0\rangle\,, & N=0, \\ \alpha\,|0\rangle+\beta\,|1\rangle\,, & 0<N<N_R+1, \\ |1\rangle\,, & N=N_R+1\,. \end{cases} \tag{58}$$

The probability of the outcome $N=0$ is $|\alpha|^2/(N_R+1)$, of $N=N_R+1$ is $|\beta|^2/(N_R+1)$, and of each of the other outcomes is $1/(N_R+1)$. Weighting the decoded states $\mathcal{R}^{(N)}\circ\mathcal{E}^{(N)}(\rho)$ by these probabilities, we can verify that equation (55) is recovered.

In this particular example, taking the adjoint of the encoding operation as one's recovery operation is actually optimal. The proof is as follows. For $0 < N < N_R + 1$, the recovery operation is perfect and consequently optimal. Otherwise, the action of the encoding map is to measure the system in the $\{|0\rangle, |1\rangle\}$ basis and update it to one of two orthogonal states [as can be inferred from equation (58)]. It is a well-known result that the update map that maximizes the entanglement fidelity is simply the Lüders rule (or projection postulate) [39], and this is precisely what the composition of the encoding with the recovery operation achieves.

The fact that the optimal recovery operation can be achieved using a 'measure and reorient' scheme shows that having the classical resource of partially correlated RFs that is obtained by this scheme is just as good as having the quantum RF token, at least for the purpose of optimizing average-case performance in decoding. This is a surprising result because one might have expected the quantum resource to always do better.

Finally, by implementing a projective measurement of the total number and post-selecting on finding $N \neq 0, N_R + 1$, it is clear that Bob can achieve perfect decoding. This occurs with probability

$$p_{\text{perfect}} = \frac{N_R}{N_R + 1}. \tag{59}$$

5. Example: Cartesian frame

For a Cartesian frame, the relevant group is the rotation group[7]. The charge sectors (irreps) are labeled by a non-negative integer or half-integer j, and the irreps are $(2j+1)$-dimensional with the standard basis $\{|j, m\rangle, m = -j, \ldots, j\}$. We bound the size of our RF token by bounding j. Recall that the fiducial state for the frame, equation (17), requires us to work in a subspace $\mathcal{H}'_R \subseteq \mathcal{H}_R$ satisfying equation (14). In the Cartesian case, we are confined to j values such that $\dim \mathcal{N}_R^{(j)} \geqslant 2j+1$. We denote the largest such value by j_R. (As an example, for an even number N of spin-1/2 particles, only the highest irrep, $j = N/2$, fails to satisfy equation (14), and consequently $j_R = N/2 - 1$. See [1, 9].) For simplicity, we restrict our attention to integer values of j_R (similar results can be obtained if one also allows non-integer values). The fiducial state of the RF token is

$$|e_{j_R}\rangle = \sum_{j=0}^{j_R} \sqrt{\frac{2j+1}{D_R}} \sum_{m=-j}^{j} |j, m\rangle \otimes |\phi_{j,m}\rangle, \tag{60}$$

where

$$D_R = \sum_{j=0}^{j_R} (2j+1)^2 = \frac{1}{3}(2j_R+1)(2j_R+3)(j_R+1). \tag{61}$$

The system is taken to be a spin-1/2 particle. Because this is an irrep of $SU(2)$, the general results of section 2.2 apply.

5.1. *Effective decoherence*

We choose the following parametrization of $SU(2)$,

$$U(\omega, \theta, \phi) = \mathrm{e}^{\mathrm{i}\omega \mathbf{n} \cdot \mathbf{J}} \tag{62}$$

[7] We use $SU(2)$ rather than $SO(3)$ to allow for spinor representations of the rotation group.

describing a rotation by angle ω about the unit vector $\mathbf{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. Let

$$|(\omega,\theta,\phi)_{j_R}\rangle = U_R(\omega,\theta,\phi)\left|e_{j_R}\right\rangle, \tag{63}$$

where $|e_{j_R}\rangle$ is the fiducial RF state of equation (60). Then

$$\langle e_{j_R}|(\omega,\theta,\phi)_{j_R}\rangle = \sum_j \sum_m \frac{2j+1}{D_R}\langle j,m|\,U^{(j)}(\omega,\theta,\phi)\,|j,m\rangle \tag{64}$$

$$= \frac{1}{D_R}\sum_j (2j+1)\chi^{(j)}(\omega,\theta,\phi), \tag{65}$$

where $U^{(j)}$ is the spin-j irrep of $SU(2)$, and $\chi^{(j)}(\omega,\theta,\phi) = \mathrm{Tr}[U^{(j)}(\omega,\theta,\phi)]$ are the characters of $SU(2)$. These characters are independent of θ and ϕ. They are given by

$$\chi^{(j)}(\omega) = \frac{\sin[(j+1/2)\omega]}{\sin[\omega/2]}. \tag{66}$$

Using the following identity:

$$\frac{\sin[(n+1/2)\omega]}{2\,\sin[\omega/2]} = 1/2 + \sum_{k=1}^{n}\cos(k\omega), \tag{67}$$

we find that

$$|\langle e_{j_R}|(\omega,\theta,\phi)_{j_R}\rangle|^2 = \left(\frac{\sin[\omega(j_R+1)](1+\cos\,\omega)}{\sin\,\omega(1-\cos\,\omega)} - 2(j_R+1)\frac{\cos[\omega(j_R+1)]}{(1-\cos\,\omega)}\right)^2. \tag{68}$$

In terms of this parametrization, the $SU(2)$ invariant measure is

$$\mathrm{d}\,\Omega = \frac{1}{2\pi^2}\,\sin^2\frac{\omega}{2}\,\sin\,\theta\,\mathrm{d}\phi\,\mathrm{d}\theta\,\mathrm{d}\omega, \tag{69}$$

where $0 \leqslant \phi < 2\pi$, $0 \leqslant \theta \leqslant \pi$, and $0 \leqslant \omega \leqslant \pi$. For the rotation $U_S(\omega,\theta,\phi)$ on the qubit system in this parametrization, we have

$$U_S(\omega,\theta,\phi) = \begin{pmatrix} \cos\frac{\omega}{2} + \mathrm{i}\sin\frac{\omega}{2}\cos\theta & \mathrm{i}\mathrm{e}^{-\mathrm{i}\phi}\sin\frac{\omega}{2}\,\sin\,\theta \\ \mathrm{i}\mathrm{e}^{\mathrm{i}\phi}\,\sin\frac{\omega}{2}\sin\theta & \cos\frac{\omega}{2} - \mathrm{i}\,\sin\frac{\omega}{2}\,\cos\theta \end{pmatrix}. \tag{70}$$

It follows that the composition of encoding and decoding maps, given by equation (40), is

$$\mathcal{R}\circ\mathcal{E}(\rho) = \begin{pmatrix} 2j_R+3 \\ 3 \end{pmatrix}^{-1}\int \mathrm{d}\Omega\,|\langle e_{j_R}|(\omega,\theta,\phi)_{j_R}\rangle|^2 U_S(\omega,\theta,\phi)\rho U_S(\omega,\theta,\phi)^\dagger$$

$$= \frac{j_R}{j_R+1}\rho + \frac{1}{j_R+1}I/2 \tag{71}$$

$$= \left(\frac{j_R}{j_R+1}\mathcal{I} + \frac{1}{j_R+1}\mathcal{G}\right)[\rho], \tag{72}$$

where $\mathcal{G}$ is the $SU(2)$-twirling operation (which is completely decohering for a single qubit).

5.2. Relational subsystems

Next, we determine the precise nature of the relational subsystems where the quantum information is encoded. In this example, the multiplicity spaces play a key role. We begin by describing the group-induced structure of the Hilbert spaces, both for the RF and the total system. Under the action of the representation U_R of $SU(2)$, the Hilbert space for the RF is decomposed as

$$\mathcal{H}_R = \bigoplus_{j=0}^{j_R} \mathcal{M}_R^{(j)} \otimes \bar{\mathcal{N}}_R^{(j)}. \tag{73}$$

The joint system RS, consisting of the RF plus a spin-1/2 qubit, carries a collective representation $U_{RS} = U_R \otimes U_S$ of $SU(2)$ which can easily be determined using standard angular momentum coupling. For coupling a spin-j irrep to a spin-1/2 irrep, we have $\mathcal{M}_R^{(j)} \otimes \mathcal{M}_S^{(1/2)} = \mathcal{M}_{RS}^{(j+1/2)} \oplus \mathcal{M}_{RS}^{(j-1/2)}$. Thus, the Hilbert space of the joint system RS has a similar decomposition under the action of U_{RS}, given by

$$\mathcal{H}_{RS} = \bigoplus_{J=1/2}^{j_R+1/2} \mathcal{M}_{RS}^{(J)} \otimes \bar{\mathcal{N}}_{RS}^{(J)}. \tag{74}$$

The multiplicity spaces for the joint system RS are related to those of the RF as

$$\bar{\mathcal{N}}_{RS}^{(J)} = \begin{cases} \bar{\mathcal{N}}_R^{(J+1/2)} \oplus \bar{\mathcal{N}}_R^{(J-1/2)}, & J < j_R + \frac{1}{2}, \\ \bar{\mathcal{N}}_R^{(j_R)}, & J = j_R + \frac{1}{2}. \end{cases} \tag{75}$$

For simplicity, we consider the qubit state to be pure, expressed in the standard angular momentum basis as

$$|\psi\rangle = \sum_{s=\pm 1/2} \alpha_s |1/2, s\rangle. \tag{76}$$

The encoded state within the Jth irrep is

$$\Pi^{(J)}(|e_{j_R}\rangle\langle e_{j_R}| \otimes |\psi\rangle\langle\psi|)\Pi^{(J)}. \tag{77}$$

To evaluate this expression, we first evaluate

$$\langle J, M|(|e_{j_R}\rangle|\psi\rangle), \tag{78}$$

where we recall that $|J, M\rangle$ is defined on the subsystem $\mathcal{M}_{RS}^{(J)}$. Therefore, the state (78) is an unnormalized vector on $\bar{\mathcal{N}}_{RS}^{(J)}$. We transform $|e_{j_R}\rangle|\psi\rangle$ to a coupled basis using Clebsch–Gordan coefficients $(j_1, m_1; j_2, m_2|j, m)$. In terms of the bases used in (60) and (76), we have

$$|j, m\rangle|\tfrac{1}{2}, s\rangle|\phi_{j,m}\rangle = \sum_{b=\pm 1/2} |J{=}j{+}b, M{=}m{+}s\rangle|\phi_{j,m}\rangle(j, m; \tfrac{1}{2}, s|j + b, m + s)\,. \tag{79}$$

We note that the states $\{|\phi_{j,m}\rangle\,, m = -j, \ldots, j\}$ for $j = J + 1/2$ $(J - 1/2)$ form a basis of $\bar{\mathcal{N}}_R^{(J-1/2)}$ $(\bar{\mathcal{N}}_R^{(J+1/2)})$. It follows that the full set of states $\{|\phi_{j,m}\rangle\,, j = J \pm \frac{1}{2}, m = -j, \ldots, j\}$ form

a basis of $\bar{\mathcal{N}}_{RS}^{(J)}$. We have

$$\langle J, M|(|e_{j_R}\rangle|\psi\rangle) = \sum_{j=0}^{j_R}\sum_{m=-j}^{j}\sum_{s,b=\pm 1/2}\sqrt{\frac{2j+1}{D_R}}\alpha_s|\phi_{j,m}\rangle(j, m; \tfrac{1}{2}, s|j+b, m+s)\delta_{J,j+b}\delta_{M,m+s}$$

$$= \sum_{s,b\,=\,\pm 1/2}\sqrt{\frac{2(J-b)+1}{D_R}}\alpha_s|\phi_{J-b,M-s}\rangle(J-b, M-s; \tfrac{1}{2}, s|J, M)\,. \tag{80}$$

We use the following Clebsch–Gordan identity:

$$(j_1, m_1; j_2, m_2|j, m) = (-1)^{j_2+m_2}\sqrt{\frac{2j+1}{2j_1+1}}(j, -m; j_2, m_2|j_1, -m_1)\,, \tag{81}$$

to obtain

$$\langle J, M|(|e_{j_R}\rangle|\psi\rangle) = \sqrt{\frac{2J+1}{D_R}}\sum_{s,b=\pm 1/2}\alpha_s(-1)^{s-b+1}|\phi_{J-b,M-s}\rangle(J, M; \tfrac{1}{2}, -s|J-b, M-s)\,. \tag{82}$$

We now consider two cases for J separately.

For $J < j_R + 1/2$, we note that the multiplicity space $\bar{\mathcal{N}}_{RS}^{(J)}$ is unitarily equivalent to the tensor product of a spin-J and a spin-1/2 system coupled to total angular momentum $J \pm 1/2$. That is,

$$\bar{\mathcal{N}}_{RS}^{(J)} = \bar{\mathcal{N}}_{R}^{(J+1/2)} \oplus \bar{\mathcal{N}}_{R}^{(J-1/2)} \simeq \mathcal{K}^{(J)} \otimes \mathcal{H}_S\,, \tag{83}$$

where $\mathcal{K}^{(J)}$ carries an irrep J of $SU(2)$ and $\simeq$ denotes unitary equivalence. We explicitly define the bijective isometry $A^{(J)}\colon \bar{\mathcal{N}}_{RS}^{(J)} \to \mathcal{K}^{(J)} \otimes \mathcal{H}_S$ via its adjoint action on a basis for $\mathcal{K}^{(J)} \otimes \mathcal{H}_S$ as

$$A^{(J)\dagger}|J, M\rangle_{\mathcal{K}^{(J)}}|\tfrac{1}{2}, s\rangle_{\mathcal{H}_S} = (-1)^{s+1/2}\sum_{b=\pm 1/2}(-1)^{b-1/2}(J, M; \tfrac{1}{2}, s|J+b, M+s)|\phi_{J+b,M+s}\rangle\,. \tag{84}$$

In terms of this new subsystem structure for the multiplicity spaces, we can express (82) as

$$\langle J, M|(|e_{j_R}\rangle|\psi\rangle) = \sqrt{\frac{2J+1}{D_R}}\sum_{s=\pm 1/2}\alpha_s A^{(J)\dagger}|J, M\rangle_{\mathcal{K}^{(J)}}|\tfrac{1}{2}, s\rangle_{\mathcal{H}_S}$$

$$= \sqrt{\frac{2J+1}{D_R}}A^{(J)\dagger}|J, M\rangle_{\mathcal{K}^{(J)}}|\psi\rangle_{\mathcal{H}_S}\,, \tag{85}$$

where $|\psi\rangle_{\mathcal{H}_S}$ is defined by equation (76). It follows that the encoded state for an irrep J where $J < j_R + 1/2$ is

$$\mathcal{E}^{(J)}(\rho) = \mathrm{Tr}_{\mathcal{M}_{RS}^{(J)}}\left[\Pi^{(J)}(|e_{j_R}\rangle\langle e_{j_R}| \otimes \rho)\Pi^{(J)}\right]$$

$$= \sum_{M=-J}^{J}\langle J, M|(|e_{j_R}\rangle\langle e_{j_R}| \otimes \rho)|J, M\rangle$$

$$= \frac{2J+1}{D_R}A^{(J)\dagger}(I_{\mathcal{K}^{(J)}} \otimes \rho)A^{(J)}\,, \qquad J < j_R + \tfrac{1}{2}\,. \tag{86}$$

Because $A^{(J)}$ is bijective, (specifically, because the set of states $\{A^{(J)\dagger}|J,\, M\rangle_{\mathcal{K}^{(J)}}|1/2,\, s\rangle_{\mathcal{H}_S}\,;\, M = -J,\ldots,J\,,\ s=\pm 1/2\}$ are orthogonal) we find the qubit faithfully encoded into the relational subsystem whenever $J < j_R + 1/2$.

However, for the result $J = j_R + 1/2$, the multiplicity space $\bar{\mathcal{N}}_{RS}^{(J)}$ is exceptional; see (75). We cannot factorize $\bar{\mathcal{N}}_{RS}^{(J)}$ as in equation (83). Nonetheless, we can still introduce a Hilbert space $\mathcal{K}^{(j_R+1/2)}$, which carries an irrep $j_R + 1/2$ of $SU(2)$ and in terms of it we can define an isometry $A^{(j_R+1/2)} : \bar{\mathcal{N}}_{RS}^{(j_R+1/2)} \to \mathcal{K}^{(j_R+1/2)} \otimes \mathcal{H}_S$, by modifying equation (84) to include only the $b = -1/2$ term in the sum. This isometry is simply not surjective. It follows that the set of states $\{A^{(j_R+1/2)\dagger}|j_R+1/2,\, M\rangle_{\mathcal{K}^{(j_R+1/2)}}|1/2,\, s\rangle_{\mathcal{H}_S}\,;\, M = -j_R-1/2,\ldots,j_R+1/2\,,\ s=\pm 1/2\}$ are no longer orthogonal. Therefore, the map

$$\mathcal{E}^{(j_R+1/2)}(\rho) = \frac{2j_R+2}{D_R} A^{(j_R+1/2)\dagger}(I_{\mathcal{K}^{(j_R+1/2)}} \otimes \rho) A^{(j_R+1/2)} \tag{87}$$

is no longer invertible. The action of $A^{(j_R+1/2)}$ can be viewed as a projection of uncoupled states on $\mathcal{K}^{(j_R+1/2)} \otimes \mathcal{H}_S$ onto the subspace of states which couple to total angular momentum j_R.

The probability assigned to each irrep J is

$$\begin{aligned} p_J &= \mathrm{Tr}\big[\Pi^{(J)}(|e_{j_R}\rangle\langle e_{j_R}| \otimes |\psi\rangle\langle\psi|)\Pi^{(J)}\big] \\ &= \begin{cases} \dfrac{(2J+1)^2}{D_R}\,, & J < j_R + \frac{1}{2}\,, \\ \dfrac{(2j_R+1)(j_R+1)}{D_R}\,, & J = j_R + \frac{1}{2}\,. \end{cases} \end{aligned} \tag{88}$$

We note that these probabilities satisfy $\sum_{J=1/2}^{j_R+1/2} p_J = 1$.

The decoding map within each irrep J takes the form

$$\begin{aligned} \mathcal{R}^{(J)}(\cdot) &= \mathrm{Tr}_{\mathcal{K}^{(J)}}[A^{(J)}(\cdot)A^{(J)\dagger}] \\ &= (2J+1)\langle e_{j_R}|I_{\mathcal{M}_{RS}^{(J)}} \otimes (\cdot)|e_{j_R}\rangle\,. \end{aligned} \tag{89}$$

For $J < j_R + 1/2$, equation (86) gives

$$(\mathcal{R}^{(J)} \circ \mathcal{E}^{(J)})(\rho) = \rho\,. \tag{90}$$

For $J = j_R + 1/2$, we make use of equation (87) and find

$$(\mathcal{R}^{(j_R+1/2)} \circ \mathcal{E}^{(j_R+1/2)})(\rho) = \frac{(2j_R+1)(j_R+1)}{D_R}\left(\frac{2j_R}{6(j_R+1)}\mathcal{I} + \frac{(2j_R+3)}{3(j_R+1)}\mathcal{G}\right)[\rho]\,, \tag{91}$$

where $\mathcal{G}$ is the $SU(2)$-twirling operation (complete decoherence). Averaging over the irreps with the weights given in equation (88), we find the decoded state to be

$$\begin{aligned} (\mathcal{R}\circ\mathcal{E})(\rho) &= \sum_{J=1/2}^{j_R-1/2} \frac{(2J+1)^2}{D_R}\mathcal{I}[\rho] + \frac{(2j_R+1)(j_R+1)}{D_R}\left(\frac{2j_R}{6(j_R+1)}\mathcal{I} + \frac{(2j_R+3)}{3(j_R+1)}\mathcal{G}\right)[\rho] \\ &= \left(\frac{j_R}{j_R+1}\mathcal{I} + \frac{1}{j_R+1}\mathcal{G}\right)[\rho]\,, \end{aligned} \tag{92}$$

thereby verifying that equation (71) is recovered.

We note that our recovery operation is perfect in the non-exceptional irreps and therefore optimal there. In the exceptional irrep, the error incurred in recovery is at most twice that of the optimal recovery, as described in section 3, by virtue of being of the form of Barnum and Knill's approximate reversal. We leave it as an open problem to prove whether this recovery is in fact optimal, or if not, to identify what form an optimal recovery map would take.

Post-selectively perfect decoding is achieved if Bob implements a projective measurement that distinguishes the irreps and obtains $J \neq j_R + 1/2$. By equations (88) and (61) (or by equation (47) directly), we see that the probability for this to occur is

$$p_{\text{perfect}} = \frac{1}{D_R} \sum_{J=1/2}^{j_R-1/2} (2J+1)^2 = \frac{\sum_{J=1/2}^{j_R-1/2} (2J+1)^2}{\sum_{j=0}^{j_R} (2j+1)^2}$$
$$= \frac{2j_R}{2j_R+3}\,. \tag{93}$$

6. Example: direction indicator

A directional RF identifies only a single direction in space, as opposed to a full set of axes. Such an RF is not associated directly with a Lie group, but rather with a coset space. Specifically, although $SU(2)$ may provide a group of transformations between all possible directional RFs, any one directional RF is invariant under $U(1)$ rotations about its axis of symmetry; the relevant coset is then $SU(2)/U(1)$.

Because of this distinction, we expect this example to proceed differently from the other two. The distinction is immediately apparent because there is no obvious candidate for a fiducial reference state as in equation (17). Instead, we take the directional RF to be in an $SU(2)$-coherent state of size j_R, so that the fiducial state is

$$|e_{j_R}\rangle = |j_R, m = j_R\rangle\,. \tag{94}$$

We consider a qubit system that is described relative to Alice's local Cartesian frame by the state

$$\rho = |\psi\rangle\langle\psi| \quad \text{where} \quad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{95}$$

where $|0(1)\rangle = |j_R = 1/2, m = \pm 1/2\rangle$. Note first of all that even if Bob shared a classical reference direction with Alice, her $\hat{z}$-axis for instance, his description of the system is still related to Alice's by a dephasing operation. The reason is that he *only* shares Alice's $\hat{z}$-axis, and so the rotation about $\hat{z}$ that relates his local $\hat{x}$-axis to hers is completely unknown. Averaging over rotations $R_z(\theta) = \exp(-\mathrm{i}\,\theta\,J_z)$ yields the dephasing operation

$$\mathcal{U}[\rho] = \int_0^{2\pi} \frac{\mathrm{d}\,\theta}{2\pi} R_z(\theta)\rho R_z^\dagger(\theta) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\,. \tag{96}$$

Consequently, if Bob has a bounded-size token of Alice's $\hat{z}$ -axis, his decoding will yield a state that approaches $\mathcal{U}(\rho)$ rather than ρ as one increases the size of the token.

6.1. Effective decoherence

Define $|\Omega_{j_R}\rangle = U_R(\Omega)|e_{j_R}\rangle$ where $\Omega \in SU(2)$. The encoding of ρ relative to Bob's local Cartesian frame is the following state of the composite of RF token and system

$$\mathcal{E}(\rho) = \int \mathrm{d}\Omega |\Omega_{j_R}\rangle\langle\Omega_{j_R}| \otimes U_S(\Omega)\rho U_S^\dagger(\Omega)\,. \tag{97}$$

To decode, Bob measures the covariant POVM $\{D_R|\Omega'_{j_R}\rangle\langle\Omega'_{j_R}|\mathrm{d}\Omega'\}$ on the RF token and reorients the system accordingly. The net result is

$$\mathcal{R}\circ\mathcal{E}(\rho) = D_R \int \mathrm{d}\Omega |\langle e_{j_R}|\Omega_{j_R}\rangle|^2 U_S(\Omega)\rho U_S^\dagger(\Omega)\,. \tag{98}$$

The effect of this map will be particularly simple given that $|e_{j_R}\rangle$ is invariant under $U(1)$ rotations about the z-axis.

For this calculation, it will be easiest to use Euler angles to parametrize $SU(2)$:

$$U(\Omega) = \mathrm{e}^{-\mathrm{i}aJ_z}\mathrm{e}^{-\mathrm{i}bJ_y}\mathrm{e}^{-\mathrm{i}cJ_z}\,, \tag{99}$$

where $a, b, c \in [0, 2\pi]$. (We note this parametrization is different from that used in section 5.) With this parametrization,

$$\begin{aligned}\langle e_{j_R}|\Omega_{j_R}\rangle &= \langle j_R, j_R|U_R^{(j_R)}(\Omega)|j_R, j_R\rangle \\ &= \mathrm{e}^{-\mathrm{i}(a+c)j_R}[\cos(b/2)]^{2j_R}\,,\end{aligned} \tag{100}$$

and thus $|\langle e_{j_R}|\Omega_{j_R}\rangle|^2 = [\cos(b/2)]^{4j_R}$. We can express $U_S(\Omega)$ as a 2×2 matrix in the z-basis as

$$U_S(\Omega) = \begin{pmatrix}\mathrm{e}^{-\mathrm{i}a/2} & 0\\ 0 & \mathrm{e}^{\mathrm{i}a/2}\end{pmatrix}\begin{pmatrix}\cos b/2 & -\sin b/2\\ \sin b/2 & \cos b/2\end{pmatrix}\begin{pmatrix}\mathrm{e}^{-\mathrm{i}c/2} & 0\\ 0 & \mathrm{e}^{\mathrm{i}c/2}\end{pmatrix}\,, \tag{101}$$

and our qubit system in Bloch vector notation as

$$\rho = \frac{1}{2}\begin{pmatrix}1+z & x-\mathrm{i}y\\ x+\mathrm{i}y & 1-z\end{pmatrix}. \tag{102}$$

Using the identities

$$\int_0^\pi \mathrm{d}b\,\sin b\,\cos^{4j_R}(b/2) = \frac{2}{2j_R+1}\,, \tag{103}$$

$$\int_0^\pi \mathrm{d}b\,\sin b\,\cos^{4j_R}(b/2)\,\cos^2(b/2) = \frac{1}{j_R+1}\,, \tag{104}$$

we find that

$$\begin{aligned}\mathcal{R}\circ\mathcal{E}(\rho) &= (2j_R+1)\int \mathrm{d}\Omega\,\cos^{4j_R}(b/2)\,U_S(\Omega)\rho U_S(\Omega)^{-1}\\ &= \frac{1}{2}\begin{pmatrix}1+\frac{j_R}{j_R+1}z & 0\\ 0 & 1-\frac{j_R}{j_R+1}z\end{pmatrix}\\ &= \left(\left(\frac{j_R}{j_R+1}\mathcal{I}+\frac{1}{j_R+1}\mathcal{G}\right)\circ\mathcal{U}\right)[\rho]\,,\end{aligned} \tag{105}$$

where $\mathcal{G}$ is the $SU(2)$-twirling operation, and $\mathcal{U}$ is the dephasing operator defined in equation (96).

6.2. Relational subsystems

First, we note that the RF token, consisting of only a spin-j_R system, does not possess a multiplicity space. When coupling this spin-j_R system to the spin-1/2 qubit, the resulting collective system is described by

$$\mathcal{H}_{RS} = \mathcal{M}_R^{(j_R)} \otimes \mathcal{M}_S^{(\frac{1}{2})} = \mathcal{M}_{RS}^{(j_R+1/2)} \oplus \mathcal{M}_{RS}^{(j_R-1/2)}, \tag{106}$$

and does not possess any multiplicity spaces either.

Given that the fiducial state, equation (94), is not of the form of equation (17), the derivation of equation (23) is no longer valid. Nonetheless, the encoding map defined by equation (97) may still be written in the form of equation (23), namely,

$$\mathcal{E}(\rho) = \sum_{J=j_R-1/2}^{j_R+1/2} d_J^{-1} I_{\mathcal{M}_{RS}^{(J)}} \otimes \mathcal{E}^{(J)}(\rho), \tag{107}$$

where

$$\mathcal{E}^{(J)}(\rho) = \mathrm{Tr}_{\mathcal{M}_{RS}^{(J)}}\left[\Pi^{(J)}(|e_{j_R}\rangle\langle e_{j_R}| \otimes \rho)\Pi^{(J)}\right], \tag{108}$$

which is of the same form as equation (37). To see that this decomposition exists, simply express equation (97) as $\mathcal{E}(\rho) = \mathcal{G}(|e_{j_R}\rangle\langle e_{j_R}| \otimes \rho)$ where $\mathcal{G}$ is the $SU(2)$-twirling operation. Then, using equations (8) and (106), we have

$$\mathcal{E}(\rho) = \sum_{J=j_R-1/2}^{j_R+1/2} \mathcal{D}_{\mathcal{M}_{RS}^{(J)}}\left[\Pi^{(J)}(|e_{j_R}\rangle\langle e_{j_R}| \otimes \rho)\Pi^{(J)}\right], \tag{109}$$

which is equivalent to equations (107) and (108). Note that $\mathcal{E}^{(J)}$ is still a map from $\mathcal{B}(\mathcal{H}_S)$ to $\mathcal{N}_{RS}^{(J)}$, but in this case $\mathcal{N}_{RS}^{(J)} = \mathbb{C}$, so that it maps density operators to scalars. Specifically,

$$\mathcal{E}^{(J)}(\rho) = \begin{cases} \dfrac{2j_R}{2j_R+1}|\alpha|^2 + \dfrac{1}{2j_R+1}, & J = j_R + \frac{1}{2}, \\ \dfrac{2j_R}{2j_R+1}|\beta|^2, & J = j_R - \frac{1}{2}. \end{cases} \tag{110}$$

We see that the encoding operation in this case can be described as follows: after adjoining the RF token to the system, destructively measure the total angular momentum $\mathbf{J}^2$ of the composite and upon obtaining quantum number J, reprepare the system in the associated $SU(2)$-invariant state $d_J^{-1} I_{\mathcal{M}_{RS}^{(J)}}$.

The decoding operation defined in equation (98) is clearly proportional to the Hilbert–Schmidt adjoint of the encoding operation. Consequently, it admits a decomposition into irreps via the adjoints of equation (107), namely,

$$\mathcal{R}(\rho_{RS}) = \sum_{J=j_R-1/2}^{j_R+1/2} \mathcal{R}^{(J)}\left[\mathrm{Tr}_{\mathcal{M}_{RS}^{(J)}}(\Pi^{(J)}\rho_{RS}\Pi^{(J)})\right], \tag{111}$$

where $\mathcal{R}^{(J)} \propto \mathcal{E}^{(J)\dagger}$ is a map from $\mathbb{C}$ to $\mathcal{B}(\mathcal{H}_S)$. This is of the same form as equation (41). To determine $\mathcal{R}^{(J)}$, we calculate the adjoint of equation (108) and determine the normalization by

requiring that $\mathrm{Tr}[\mathcal{R}^{(J)}(1)] = 1$ for all J. We obtain

$$\mathcal{R}^{(J)}(p) = \frac{2j_R+1}{2J+1}\langle e_{j_R}|I_{\mathcal{M}_{RS}^{(J)}}|e_{j_R}\rangle \times p\,, \tag{112}$$

where $p \in \mathbb{C}$. Except for the constant of proportionality, this has the form of equation (43). It evaluates to

$$\mathcal{R}^{(J)}(p) = p \times \begin{cases} \dfrac{2j_R+1}{2j_R+2}|0\rangle\langle 0| + \dfrac{1}{2j_R+2}|1\rangle\langle 1|\,, & J = j_R + \frac{1}{2}\,, \\ |1\rangle\langle 1|\,, & J = j_R - \frac{1}{2}, \end{cases} \tag{113}$$

[which one could also infer by taking the adjoint of equation (110)]. Consequently, the decoding operation may be described as follows: destructively measure the total angular momentum (squared), $\mathbf{J}^2$, on the composite of RF token and system and upon obtaining quantum number $j_R \pm 1/2$, reprepare the system in one of the two states in equation (113).

The composition of encoding and decoding yields

$$\begin{aligned} \mathcal{R}\circ\mathcal{E}(\rho) &= \sum_{J=j_R-1/2}^{j_R+1/2} \mathcal{R}^{(J)}\circ\mathcal{E}^{(J)}(\rho) \\ &= \frac{1}{j_R+1}\left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right) + \frac{j_R}{j_R+1}(|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|) \\ &= \left(\left(\frac{j_R}{j_R+1}\mathcal{I} + \frac{1}{j_R+1}\mathcal{G}\right)\circ\mathcal{U}\right)[\rho]\,, \end{aligned} \tag{114}$$

in agreement with equation (105). We note that this coincides with the result obtained by Poulin [16].

This recovery operation is of the form of the approximate reversal operation described by Barnum and Knill [32] and is therefore near-optimal in the sense described in section 3. Although it is not itself the optimal recovery map, the latter is easy to find in this example and we do so presently.

Given that the only pure states of the system that one can hope to reconstruct in the limit of an unbounded RF token are the J_z eigenstates, denoted here by $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, it is natural to take as our figure of merit the average input–output fidelity equally weighted over these two input states (because then one can achieve fidelity 1 in the limit of an unbounded RF token). The only information about the state of the system that is encoded in $\mathcal{E}(\rho)$ is encoded in the relative weights of its two $SU(2)$-invariant terms. Consequently, the optimal decoding operation must consist of a determination of J followed by a repreparation of the system state.

We make use of previous work on the optimal estimation of the relative angle between a spin-1/2 system and a spin-j_R RF [23]. These results show that a measurement of $\mathbf{J}^2$ on the composite is in fact optimal for estimating whether the system state was $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$ given a uniform prior over the two. It is also shown there that the posterior probabilities one ought to assign to these two states upon obtaining outcomes $j_R + 1/2$ and $j_R - 1/2$ are

$$\begin{aligned} p(0|+) &= \tfrac{2j+1}{2j+2}\,, & p(1|+) &= \tfrac{1}{2j+2}\,, \\ p(0|-) &= 0\,, & p(1|-) &= 1\,. \end{aligned} \tag{115}$$

In order to optimize the fidelity, one must reprepare the state that is most likely given the outcome, so that one should reprepare $|0\rangle\langle 0|$ given the '+' outcome and $|1\rangle\langle 1|$ given the '−' outcome. $\mathcal{R}$ falls short of this optimal recovery because, by equation (113), it does not reprepare $|0\rangle\langle 0|$ given the '+' outcome; instead, it prepares a mixed state reflecting Bob's knowledge of the state given the measurement outcome.

Finally, we note that there is no possibility for post-selectively perfect recovery of $\mathcal{U}(\rho)$ from $\mathcal{E}(\rho)$. Both irreps, $j_R \pm 1/2$, encode the state of the system imperfectly.

Acknowledgments

We thank Robin Blume-Kohout, J-C Boileau, Matthias Christandl and Renato Renner for helpful discussions. SDB acknowledges the support of the Australian Research Council. RWS acknowledges support from the Royal Society. PST acknowledges the support of the AIF, iCORE, MITACS and JSPS.

References

[1] Bartlett S D, Rudolph T and Spekkens R W 2007 *Rev. Mod. Phys.* **79** 555
[2] Bartlett S D, Rudolph T and Spekkens R W 2003 *Phys. Rev. Lett.* **91** 027901
[3] Banaszek K, Dragan A, Wasilewski W and Radzewicz C 2004 *Phys. Rev. Lett.* **92** 257901
[4] Bourennane M, Eibl M, Gaertner S, Kurtsiefer C, Cabello A and Weinfurter H 2004 *Phys. Rev. Lett.* **92** 107901
[5] Gisin N and Popescu S 1999 *Phys. Rev. Lett.* **83** 432
[6] Peres A and Scudo P F 2001 *Phys. Rev. Lett.* **86** 4160
[7] Peres A and Scudo P F 2001 *Phys. Rev. Lett.* **87** 167901
[8] Bagan E, Baig M and Munoz-Tapia R 2004 *Phys. Rev.* A **70** 030301
[9] Chiribella G, D'Ariano G M, Perinotti P and Sacchi M F 2004 *Phys. Rev. Lett.* **93** 180503
[10] Kitaev A, Mayers D and Preskill J 2004 *Phys. Rev.* A **69** 052326
[11] Boileau J-C, Sheridan L, Laforest M and Bartlett S D 2008 *J. Math. Phys.* **49** 032105
[12] Page D N and Wootters W K 1983 *Phys. Rev.* D **27** 2885
[13] Gambini R, Porto R A and Pullin J 2004 *Phys. Rev. Lett.* **93** 240401
[14] Gambini R, Porto R A and Pullin J 2004 *New J. Phys.* **6** 45
[15] Milburn G J and Poulin D 2006 *Int. J. Quantum Inf.* **4** 151
[16] Poulin D 2006 *Int. J. Theor. Phys.* **45** 1189
[17] Vidal G and Cirac I 2000 arXiv:quant-ph/0012067v1
[18] Dušek M and Bušek V 2002 *Phys. Rev.* A **66** 022112
[19] Fiurášek J, Dušek M and Filip R 2002 *Phys. Rev. Lett.* **89** 190401
[20] Bartlett S D, Rudolph T, Spekkens R W and Turner P S 2006 *New J. Phys.* **8** 58
[21] Bartlett S D, Rudolph T, Sanders B C and Turner P S 2007 *J. Mod. Opt.* **54** 2211
[22] Gour G and Spekkens R W 2008 *New J. Phys.* **10** 033023
[23] Bartlett S D, Rudolph T and Spekkens R W 2004 *Phys. Rev.* A **70** 032321
[24] Bennett C and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[25] Sternberg S 1994 *Group Theory and Physics* (Cambridge: Cambridge University Press)
[26] Zanardi P, Lidar D and Lloyd S 2004 *Phys. Rev. Lett.* **92** 060402
[27] Bartlett S D, Rudolph T and Spekkens R W 2004 *Phys. Rev.* A **70** 032307
[28] Chiribella G, D'Ariano G M, Perinotti P and Sacchi M F 2004 *Phys. Rev.* A **70** 062105
[29] Chiribella G, D'Ariano G M, Perinotti P and Sacchi M F 2006 *Int. J. Quantum Inf.* **4** 453
[30] Scutaru H 1979 *Rep. Math. Phys.* **16** 79

[31] Keyl M and Werner R F 1999 *J. Math. Phys.* **40** 3283
[32] Barnum H and Knill E 2002 *J. Math. Phys.* **43** 2097
[33] Niu C-S and Griffiths R B 1999 *Phys. Rev.* A **60** 2764
[34] Hughston L P, Jozsa R and Wootters W K 1993 *Phys. Lett.* A **183** 14
[35] Bartlett S D, Rudolph T and Spekkens R W 2006 *Int. J. Quantum Inf.* **4** 17
[36] Sanders B C, Bartlett S D, Rudolph T and Knight P L 2003 *Phys. Rev.* A **68** 042329
[37] Poulin D and Blume-Kohout R in preparation
[38] Ivanovic I D 1987 *Phys. Lett.* A **123** 257
Dieks D 1988 *Phys. Lett.* A **126** 303
Peres A 1988 *Phys. Lett.* A **128** 19
[39] Barnum H 2002 arXiv:quant-ph/0205155v1