Scalable protocol for identification of correctable codes

M. Silva,[1,2] E. Magesan,[1,3] D. W. Kribs,[1,4] and J. Emerson[1,3]
[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*
[2]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*
[3]*Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*
[4]*Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario, Canada, N1G 2W1*
(Received 1 October 2007; revised manuscript received 17 February 2008; published 24 July 2008)

The task of finding a correctable encoding that protects against some physical quantum process is in general hard. Two main obstacles are that an exponential number of experiments are needed to gain complete information about the quantum process, and known algorithmic methods for finding correctable encodings involve operations on exponentially large matrices. However, we show that in some cases it is possible to find such encodings with only partial information about the quantum process. Such useful partial information can be systematically extracted by averaging the channel under the action of a set of unitaries in a process known as twirling. In this paper we prove that correctable encodings for a twirled channel are also correctable for the original channel. We investigate the particular case of twirling over the set of Pauli operators and qubit permutations, and show that the resulting quantum operation can be characterized experimentally in a scalable manner. We also provide a postprocessing scheme for finding unitarily correctable codes for these twirled channels which does not involve exponentially large matrices, and which is robust against uncertainties in the experimental estimates.

DOI: 10.1103/PhysRevA.78.012347 PACS number(s): 03.67.Pp, 03.67.Hk, 03.67.Lx

I. INTRODUCTION

The coherent experimental manipulation of quantum systems, and their application to various quantum information tasks, confronts significant limitations in the presence of noise, and in particular, decoherence. The discovery of quantum error correction codes enables methods for overcoming these limitations whenever the decoherence satisfies various well-defined sets of conditions. Specifically, the applicability of particular codes depends crucially on the details of the physical noise model affecting a particular system. The standard approach for experimentally characterizing the full noise model and then assessing the usefulness of a given code are costly procedures. Indeed, full quantum process tomography requires a number of experiments [1,2] that grows exponentially with the number of subsystems, and the dimension growth of matrices involved in (classical) postprocessing [3,4] is also exponential. These limitations make the standard approach infeasible for the kinds of quantum information systems required in practical applications. In this paper we describe a general method that can be used to overcome these issues, and we apply the approach to an experimentally relevant class of noise models.

We first show how partial information about the noise can be sufficient to construct correctable encodings. This is motivated by the recent demonstration that valuable partial information about the noise can be extracted by symmetrizing or "twirling" a quantum channel [5–7]. Twirling consists of averaging the action of a sequence of gates over some distribution of unitaries, in effect randomizing aspects of the channel. This leads to scalable protocols that answer questions of practical interest about the noise. In particular, it is possible to experimentally estimate the average gate fidelity between a quantum operation and the identity map [6], as well as to obtain information about noise correlations in a quantum process [7].

We then focus on a particular type of twirl, the Pauli twirl, which has a number of special features that make finding noiseless and unitarily correctable encodings more tractable than the general case. First, the partial information obtained via a Pauli twirl can be accessed with only a polynomial number of experiments, making such experimental characterization strictly scalable. Then, we discuss how this partial information lends itself to an algebraic algorithm for finding correctable encodings. This new approach does not require the manipulation of exponentially large matrices. We also discuss how these encodings can be verified experimentally in an efficient manner.

II. TWIRLED QUANTUM OPERATIONS

Consider a trace preserving linear quantum operation $\Lambda(\rho)=\Sigma_{i,j}[\chi]_{ij}P_i\rho P_j$ acting on n qubits, where the $P_{i,j}\in\mathcal{P}_n$ are all Pauli operators acting on n qubits. Trace-preservation requires that $\Sigma_{i,j}[\chi]_{ij}P_jP_i=\mathbb{1}$ (in particular, tr $\chi=1$), while Hermiticity-preservation requires $[\chi]_{ij}=[\chi]^*_{ji}$. Completely-positive (CP) operations have the additional requirement that $\chi\geq 0$, which follows from the fact that CP maps can be written as a Choi-Kraus sum $\Lambda(\rho)=\Sigma_k A_k\rho A_k^\dagger$ [10]. This implies that for CP maps $\forall\ i\ [\chi]_{ii}\geq 0$ and hence the $[\chi]_{ii}$ can be interpreted as probabilities.

Quantum operations require $O(2^{4n})$ parameters to be fully described, and thus require an exponential number of experiments to be fully characterized [1,2]. Due to this exponential cost, it is impractical to obtain a complete description about noise and decoherence acting on even a moderately large system of qubits. Useful partial information about the noise can be obtained by averaging the action of the quantum operation under the composition $\mathcal{U}\circ\Lambda\circ\mathcal{U}^\dagger$ for unitary operations $\mathcal{U}(\rho)=U\rho U^\dagger$ randomly chosen according to some distribution [6,7]. This averaging is known as a "twirl," and the averaged

channel $\bar{\Lambda}(\rho)=\int d\mu(\mathcal{U})\mathcal{U}\circ\Lambda\circ\mathcal{U}^{\dagger}(\rho)$ is known as the "twirled channel." The case where the distribution over unitaries is discrete is of particular interest. In that case, the twirled channel is given by $\bar{\Lambda}(\rho)=\Sigma\Pr(\mathcal{U}_i)\mathcal{U}_i\circ\Lambda\circ\mathcal{U}_i^{\dagger}(\rho)$, where $\Pr(\mathcal{U}_i)$ is a probability distribution over the $\mathcal{U}_i$. This leads us to our first result. We use the general definition from [8] for a quantum error correcting (subsystem) code: If A and B are subsystems of a Hilbert space $\mathcal{H}=\mathcal{H}_A\otimes\mathcal{H}_B\oplus\mathcal{H}_K$, and we have some channel $\Lambda:\mathcal{B}(\mathcal{H})\rightarrow\mathcal{B}(\mathcal{H})$, then $\mathcal{H}_A$ is correctable for Λ if there is a recovery operation $\mathcal{R}$ acting on $\mathcal{B}(\mathcal{H})$ such that $\forall\ \sigma_A\in\mathcal{B}(\mathcal{H}_A)$ and $\forall\ \sigma_B\in\mathcal{B}(\mathcal{H}_B)$ there exists a $\tau_B\in\mathcal{B}(\mathcal{H}_B)$ for which $(\mathcal{R}\circ\Lambda)(\sigma_A\otimes\sigma_B)=\sigma_A\otimes\tau_B$.

Lemma. Any correctable code for a twirled channel $\bar{\Lambda}$ is a correctable code for the original channel Λ up to an additional unitary correction.

Proof. Without loss of generality, consider $\Lambda(\rho)=\Sigma_k A_k\rho A_k^{\dagger}$ and a twirl with unitaries $\{U_j\}$, where $U_1=\mathbb{1}$. Any unitary twirl is unitarily equivalent to a twirl that includes the identity, and this unitary equivalence leads to the additional unitary correction. A set of Choi-Kraus operators for $\bar{\Lambda}$ is then $\{U_j^{\dagger}A_kU_j\}$. As shown in Ref. [8], the existence of a correctable code $\mathcal{H}_A$ under the action of $\bar{\Lambda}$, with recovery operations $\mathcal{R}(\rho)=\Sigma_m R_m\rho R_m^{\dagger}$, corresponds to the projector P onto the subspace $\mathcal{H}_A\otimes\mathcal{H}_B$ satisfying $PR_mU_j^{\dagger}A_kU_jP=R_mU_j^{\dagger}A_kU_jP$ and $R_mU_j^{\dagger}A_kU_j|_P\in\mathbb{1}_A\otimes\mathcal{B}(\mathcal{H}_B)$ for all j,k,m. Since $U_1=\mathbb{1}$, this implies $PR_mA_kP=R_mA_kP$ and $R_mA_k|_P\in\mathbb{1}_A\otimes\mathcal{B}(\mathcal{H}_B)$ for all k,m. Thus it follows that $\mathcal{H}_A$ is also correctable under the action of Λ using the same recovery operation $\mathcal{R}$. ■

We now consider some specific twirls that are known to yield twirled channels which can be characterized efficiently via experiments.

III. PAULI TWIRL

It is well known [6,7] that twirling a channel Λ by the Pauli group $\mathcal{P}_n$ yields the effective channel $\bar{\Lambda}$ of the form

$$\bar{\Lambda}(\rho)=\frac{1}{4^n}\sum_{P_i\in\mathcal{P}_n}P_i\Lambda(P_i\rho P_i)P_i=\sum_i[\chi]_{ii}P_i\rho P_i. \tag{1}$$

In other words, the off-diagonal elements of χ are eliminated. Channels of this form are known as Pauli channels. From here on $\bar{\Lambda}$ will denote the result of Pauli twirling Λ, unless stated otherwise.

Pauli channels have a number of useful properties which facilitate the search for some types of correctable codes. However, the description of a general Pauli channel still requires an exponential number of parameters, and such parameters are not realistically accessible due to this exponential overhead. Instead, one can consider an additional twirl by the group Π_n consisting of all qubit permutations. The channel resulting from a combination of a $\mathcal{P}_n$ twirl and a Π_n twirl is what we call a permutation-invariant Pauli (PIP) channel. The result of performing both these twirls on Λ will be denoted $\bar{\Lambda}_{\Pi}$. Such channels can be written in terms of Choi-Kraus operators

$$\bar{\Lambda}_{\Pi}(\rho)=\sum_{\mathbf{w}}p_{\mathbf{w}}\sum_{\nu_{\mathbf{w}}}\frac{1}{K_{\mathbf{w}}^{\nu}}\sum_{\mathbf{i}_{\mathbf{w}}}\frac{1}{K_{\nu_{\mathbf{w}}}^{\mathbf{i}}}P_{w,\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\rho P_{w,\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}, \tag{2}$$

where $\mathbf{w}=(w_x,w_y,w_z)$ labels the number of X, Y, and Z Pauli operators, $\nu_{\mathbf{w}}$ labels the $w_x+w_y+w_z$ qubits over which $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ acts nontrivially, and $\mathbf{i}_{\mathbf{w}}$ labels which single qubit Pauli operator act on each of the qubits. The number K_n of different labels $\mathbf{w}$ needed to describe such a channel is $K_n\equiv\frac{1}{6}n^3+n^2+\frac{11}{6}n+1$, while for a fixed $\mathbf{w}$ there are

$$K_{\mathbf{w}}^{\nu}=\binom{n}{w_x+w_y+w_z}$$

different $\nu_{\mathbf{w}}$, and for fixed $\mathbf{w}$ and $\nu_{\mathbf{w}}$, there are

$$K_{\nu_{\mathbf{w}}}^{\mathbf{i}}=\binom{w_x+w_y+w_z}{w_x}\binom{w_y+w_z}{w_z}$$

different $\mathbf{i}_{\mathbf{w}}$.

Two equivalent descriptions of the channel (with the same number of parameters) are the Choi-Kraus decomposition and the diagonal representation. The Choi-Kraus decomposition (2) can be rewritten as $\bar{\Lambda}_{\Pi}(\rho)=\Sigma_{\mathbf{w}}p_{\mathbf{w}}M_{\mathbf{w}}^{p}(\rho)$, where $M_{\mathbf{w}}^{p}$ are the superoperators

$$M_{\mathbf{w}}^{p}(\rho)=\frac{1}{K_{\mathbf{w}}^{\nu}}\sum_{\nu_{\mathbf{w}}}\frac{1}{K_{\nu_{\mathbf{w}}}^{\mathbf{i}}}\sum_{\mathbf{i}_{\mathbf{w}}}P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\rho P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}. \tag{3}$$

The $M_{\mathbf{w}}^{p}$ are trace-preserving channels which apply each of the $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ for a given $\mathbf{w}$ with the same probability. The $M_{\mathbf{w}}^{p}$ form a basis for PIP channels.

Note that, given some n-fold tensor product of Pauli operators $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$, we have $\bar{\Lambda}_{\Pi}(P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}})=\lambda_{\mathbf{w}}P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ for some real constant $\lambda_{\mathbf{w}}\in[-1,1]$, since Pauli operators either commute or anticommute. Moreover $\bar{\Lambda}_{\Pi}$ is self-dual; i.e., $\bar{\Lambda}_{\Pi}=\bar{\Lambda}_{\Pi}^{\dagger}$, a fact that follows directly from the definition of Pauli channels. Since the $\{P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\}$ form an operator basis, it follows that the $\lambda_{\mathbf{w}}$ are the eigenvalues of $\bar{\Lambda}_{\Pi}$, with high degeneracy, as they depend only on $\mathbf{w}$. Thus, Pauli channels are diagonalizable and Hermitian.

If we define $|A\rangle\rangle\langle\langle B|\,\rho\equiv\frac{1}{2^n}A\ \mathrm{tr}(B^{\dagger}\rho)$ then the diagonal representation of the channel $\bar{\Lambda}_{\Pi}$ in terms of its eigenoperators is $\bar{\Lambda}_{\Pi}(\rho)=\Sigma_{\mathbf{w}=0}^{n}\lambda_{\mathbf{w}}M_{\mathbf{w}}^{\lambda}(\rho)$, where $M_{\mathbf{w}}^{\lambda}$ are the superoperators

$$M_{\mathbf{w}}^{\lambda}(\rho)=\sum_{\nu_{\mathbf{w}}}\sum_{\mathbf{i}_{\mathbf{w}}}|P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\rangle\rangle\langle\langle P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}|\,\rho. \tag{4}$$

The diagonal description of $\bar{\Lambda}_{\Pi}$ allows for straightforward description of the composition of channels. For example, suppose two PIP channels $\bar{\Lambda}_{\Pi}^{(1)}$ and $\bar{\Lambda}_{\Pi}^{(2)}$ are composed to yield $\bar{\Lambda}_{\Pi}^{(1)}\circ\bar{\Lambda}_{\Pi}^{(2)}$. This simply translates to the multiplication of the corresponding eigenvalues for each of the two channels because all Pauli channels commute.

It is crucial to note that, because there is at most a polynomial number of different eigenvalues, they can be estimated efficiently by determining how a Pauli observable in a $\mathbf{w}$ class is scaled under the action of the twirled channel, as

described in Ref. [7]. Thus, all the eigenvalues of a PIP channel can be estimated experimentally in a scalable manner.

IV. UNITARILY CORRECTABLE CODES

A special type of code is one for which a unitary recovery operation $\mathcal{R}=\mathcal{U}$ can be found. That is, $\mathcal{H}_A$ defines a correctable encoding for Λ that can be returned to its initial location within the system Hilbert space with a single unitary operation. The problem of finding such unitarily correctable codes (UCCs) for a unital channel is equivalent to finding the structure of the commutant of the noise algebra of $\Lambda^\dagger\circ\Lambda$ [9]. In terms of the Choi-Kraus operators $\{A_k\}$ for Λ, this "noise commutant" is defined as the set of operators that commute with the operators $\{A_k^\dagger A_j\}$. If Λ is unital and trace preserving, this commutant coincides with the fixed point set of $\Lambda^\dagger\circ\Lambda$ (the set of operators which are invariant under the action of this composed channel) [4]. This result can be refined somewhat for diagonalizable channels.

Proposition 1. Let Λ be a unital, diagonalizable and trace preserving channel with eigenvalues λ_i and eigenoperators L_i. Then, the noise commutant of $\Lambda^\dagger\circ\Lambda$ is the space spanned by eigenoperators L_i with eigenvalues $|\lambda_i|=1$.

Proof. Λ is unital and trace preserving, thus so is $\Lambda^\dagger\circ\Lambda$. Moreover, Λ is diagonalizable, so $\Lambda^\dagger\circ\Lambda$ has eigenoperators L_i with eigenvalues $\lambda_i^*\lambda_i=|\lambda_i|^2$, where the λ_i are the eigenvalues of Λ. Since $\Lambda^\dagger\circ\Lambda$ is unital, its fixed point set and its noise commutant coincide, and both are given by the space spanned by the eigenoperators L_i with $|\lambda_i|^2=1$. ■

This result allows us to relate the parameters of a channel Λ, that can be characterized by experiments, to the parameters of a formal construct $\Lambda^\dagger\circ\Lambda$ which can be used to find correctable encodings. Pauli channels are unital channels, and since they are diagonalizable and Hermitian, these channels have a particularly simple fixed-point set structure. In particular, we immediately obtain the following result.

Corollary 1. Let $\bar{\Lambda}$ be a Pauli channel. Then the noise commutant of $\bar{\Lambda}^\dagger\circ\bar{\Lambda}$ is the space spanned by the eigenoperators with eigenvalues ± 1.

Before continuing, we discuss a special class of UCC codes considered in [11]. We say that a UCC code is unitarily noiseless (UNC) for Λ if it is a UCC of Λ^n for all $n\geq 1$, where Λ^n is the channel Λ composed with itself n times. This includes, for instance, codes for which the recovery operation has the special form $\mathcal{U}=\mathcal{U}_A\otimes\mathcal{R}_B$; that is, a unitary acting only on the subsystem in which information is preserved, and an arbitrary quantum channel on subsystem B. Interestingly, the sets of UCC and UNC codes coincide for Pauli channels.

Corollary 2. A UCC of a Pauli channel $\bar{\Lambda}$ is also a UNC.

Proof. As $\bar{\Lambda}$ is Hermitian, it commutes with its dual $\bar{\Lambda}^\dagger=\bar{\Lambda}$, and thus we have that $(\bar{\Lambda}^n)^\dagger\circ\bar{\Lambda}^n=(\bar{\Lambda}^\dagger\circ\bar{\Lambda})^n$. Since the eigenvalues of $\bar{\Lambda}$ are real, this implies that the fixed point set of $\bar{\Lambda}^\dagger\circ\bar{\Lambda}$ is identical to the fixed point set of $(\bar{\Lambda}^n)^\dagger\circ\bar{\Lambda}^n$. ■

V. PIP CHANNEL PARAMETER SPACE

Considering the Liouville representation of the superoperators $\{M_{\mathbf{w}}^p\}$ and $\{M_{\mathbf{w}}^\lambda\}$, it is easy to show that there is a linear invertible map $\Omega:\mathbb{R}^{K_n}\rightarrow\mathbb{R}^{K_n}$ mapping the $p_{\mathbf{w}}$ to the $\lambda_{\mathbf{w}}$. More explicitly, we have that

$$\lambda_{\mathbf{w}}=\sum_{\mathbf{v}}[\Omega]_{\mathbf{w},\mathbf{v}}p_{\mathbf{v}},\quad [\Omega]_{\mathbf{w},\mathbf{v}}=\frac{\langle M_{\mathbf{w}}^\lambda,M_{\mathbf{v}}^p\rangle}{\langle M_{\mathbf{w}}^\lambda,M_{\mathbf{w}}^\lambda\rangle},\tag{5}$$

where $\langle\ldots,\ldots\rangle$ is the Hilbert-Schmidt inner product in the Liouville representation. This follows directly from the fact that $\langle M_{\mathbf{w}}^\lambda,M_{\mathbf{v}}^\lambda\rangle=\delta_{\mathbf{w},\mathbf{v}}\langle M_{\mathbf{w}}^\lambda,M_{\mathbf{w}}^\lambda\rangle$. Similarly, because $\langle M_{\mathbf{w}}^p,M_{\mathbf{v}}^p\rangle=\delta_{\mathbf{w},\mathbf{v}}\langle M_{\mathbf{w}}^p,M_{\mathbf{w}}^p\rangle$, we have

$$p_{\mathbf{w}}=\sum_{\mathbf{v}}[\Omega^{-1}]_{\mathbf{w},\mathbf{v}}\lambda_{\mathbf{v}},\quad [\Omega^{-1}]_{\mathbf{w},\mathbf{v}}=\frac{\langle M_{\mathbf{w}}^p,M_{\mathbf{v}}^\lambda\rangle}{\langle M_{\mathbf{w}}^p,M_{\mathbf{w}}^p\rangle}.\tag{6}$$

The $\{p_{\mathbf{w}}\}$ form a K_n-1 probability simplex, and the $\{\lambda_{\mathbf{w}}\}$ also form a K_n-1 simplex, which we call the eigenvalue simplex.

Explicitly computing the entries of the Ω matrix from the matrix elements of a Liouville representation for a superoperator is inefficient, as these representations are exponentially large in n. However, one can show that $[\Omega]_{\mathbf{v},\mathbf{w}}=1-2\frac{N(\mathbf{v},\mathbf{w})}{4^n}$, where $N(\mathbf{v},\mathbf{w})$ is the number of Pauli operators in the Kraus decomposition of an extremal channel (i.e., $p_{\mathbf{v}}=1$ for some $\mathbf{v}$) which anticommute with some Pauli operator corresponding to the equivalence class $\mathbf{w}$ [7]. General expressions for $N(\mathbf{v},\mathbf{w})$ can be obtained by simple counting arguments, which can be computed efficiently.

The fixed points of $\bar{\Lambda}_\Pi$ can be thought of as the observables that are conserved under the action of $\bar{\Lambda}_\Pi$ in the Heisenberg picture, as $\bar{\Lambda}_\Pi$ is self-dual. Once the fixed points of these channels are determined, in order to determine possible encodings one needs to compute the possible algebras generated by these fixed points. Note that, because of the degeneracy of the eigenvalues of a PIP channel, the existence of a single weight class with eigenvalue 1 corresponds to a large number of Pauli operators which are fixed points of the channel. We now describe how this allows us to find correctable codes for a PIP channel $\bar{\Lambda}_\Pi$.

VI. FINDING CORRECTABLE CODES

The identification of the fixed point set of a unital channel can be used to find a UCC using the general algorithm described in Refs. [4,9]. However, this algorithm requires the manipulation of exponentially large matrices, a problem shared with numerical algorithms used to search for more general codes [3]. Since the Pauli operators form an eigenbasis for PIP channels, the task of computing the algebra of conserved observables is relatively simpler than in the general case. One simply has to group the conserved Pauli observables into triplets of observables which satisfy the commutation relations for su(2). These commutation relations can be computed without writing the observables explicitly in a particular representation. By choosing the largest set S of mutually exclusive triplets which commute with each other, one implicitly describes how to encode a noiseless Hilbert space of dimension $2^{|S|}$. Before discussing this algorithm, we point out the following result, which can be obtained by direct computation.

Proposition 2. Given Pauli operators $\{P_j,P_k,P_l\}$ satisfying the commutation relations $[P_j,P_k]=2i\Sigma_l\tilde{\epsilon}_{jkl}P_l$, where $\tilde{\epsilon}_{jkl}=\epsilon_{jkl}\frac{s_l}{s_js_k}$, ϵ_{jkl} is the Levi-Civita symbol and $s_j,s_k,s_l\in\{\pm 1,\pm i\}$, then $\{s_jP_j,s_kP_k,s_lP_l\}$ obey the su(2) commutation relations.

It is clear that $\{s_jP_j,s_kP_k,s_lP_l\}$ are unitarily related to $\{X,Y,Z\}$, as all Pauli operators have the same spectrum and proposition 2 guarantees they have the same commutation relations. The unitary which performs the encoding is guaranteed to be in the Clifford group, since it maps a set of Pauli operators to another set of Pauli operators with the same commutation relations. Standard techniques can be applied to determine which Clifford group operations implement a desired encoding [12].

This leads to the following algorithm for finding a correctable encoding given the eigenvalues of the PIP channel $\bar{\Lambda}$. (i) Enumerate the Pauli operators with eigenvalues 1 under the action of $\bar{\Lambda}$, and call this set F. (ii) Choose a triplet of Pauli operators satisfying the commutation relations in proposition 2—if none can be found, the search is over. (iii) Remove this triplet from F, as well as all operators that do not commute with the triplet, and go back to step (ii). The number of mutually exclusive triplets found in this manner corresponds to an allowable number of encoded qubits which can be protected from the action of $\bar{\Lambda}_\Pi$.

Finding unitarily correctable codes is similarly simple. One can easily compute the conserved observables of the channel $\bar{\Lambda}_\Pi^\dagger\circ\bar{\Lambda}_\Pi$ [9]. In the case of PIP channels, this corresponds to finding observables with eigenvalue ± 1 for the channels $\bar{\Lambda}_\Pi$, so that these observables have eigenvalue 1 for $\bar{\Lambda}_\Pi^\dagger\circ\bar{\Lambda}_\Pi=\bar{\Lambda}_\Pi^2$. The same procedure described above can be applied to the ± 1 eigenspace to find a correctable encoding.

Example 1. Consider the two-qubit PIP channel with Kraus operators proportional to $\{\mathbb{1}\mathbb{1},ZZ\}$. The Pauli operators with eigenvalue 1 are $\mathbb{1}\mathbb{1},XX,YY,ZZ,XY,YX$, and $\mathbb{1}Z,Z\mathbb{1}$. Out of this set, $\{XX,XY,\mathbb{1}Z\}$ satisfy the commutation relations, and no other triplets which commute with these can be found, so a single qubit can be encoded noiselessly through this channel. ■

Example 2. Consider the two-qubit PIP channel with Kraus operators proportional to $\{\mathbb{1}\mathbb{1},YX,XY\}$. The eigenoperators with eigenvalue 1 are $\mathbb{1}\mathbb{1},XY,YX$, and ZZ. There are no triplets with the right commutation relations. The eigenoperators with eigenvalues -1 are $\mathbb{1}Z,Z\mathbb{1},XX,YY$. If we consider the ± 1 eigenspace, we obtain the same eigenoperators with eigenvalue 1 as the previous example, and thus there exists a UCC consisting of a single qubit. ■

In the case of the previous examples, we want to map the generating set of Pauli operators $\{\mathbb{1}X,\mathbb{1}Z\}$ to the generating set $\{XX,\mathbb{1}Z\}$, which can be done by a controlled-NOT gate, where the second qubit is the control, and the first qubit is the target. The question as to whether this algorithm can find all unitarily correctable encodings for an arbitrary PIP channel remains open.

VII. ROBUSTNESS

The conditions for error correction are known to be robust against perturbations [13], and a similar result applies to the scheme presented here. Experimental estimates of the eigenvalues λ_w will have an associated uncertainty ϵ. Given generators of the encoded Pauli group with eigenvalues $\lambda_w\geq 1-\epsilon$, the entire encoded Pauli group can be shown to have eigenvalues $\lambda_w>1-m\epsilon$, where m is the number of encoded qubits. This guarantees that the fidelity of the encoded states is also at least $1-m\epsilon$. If ϵ is small enough—e.g., linearly small in n, which can be achieved with a polynomial number of experiments [7]—this also guarantees that the codes constructed in the manner described here are close to being noiseless under the action of $\bar{\Lambda}_\Pi$. As the code cannot be claimed to be exactly noiseless due to the uncertainties in λ_w, our lemma does not necessarily apply. However, the average performance of the code under the action of Λ can be verified experimentally in an efficient manner [7], and if it is worse than the guaranteed performance under $\bar{\Lambda}_\Pi$, the twirled channel can be used instead.

VIII. DISCUSSION

In this paper we have shown that correctable encodings for a quantum operation can be found by searching for correctable encodings using the twirled version of that quantum operation. We investigated in detail the case of channels twirled by Pauli operators and qubit permutations, and demonstrated a simple scheme for identifying encodings with unitary recovery operations. Such twirled channels are important because they are described by a polynomial number of parameters which are experimentally accessible via a scalable protocol. The scheme does not require the manipulation of exponentially large matrices, and the performance of the constructed correctable code can be estimated experimentally in an efficient manner. Further work is needed to determine whether all unitarily correctable codes for PIP channels can be found through the scheme we described. Moreover, it would be interesting to investigate other twirls that yield more information about the channel which may be used to find more correctable codes.

ACKNOWLEDGMENTS

J.E. would like to thank D. Cory for helpful discussions. M.S. was partially supported by NSERC, MITACS, and ARO. E.M. and J.E. were partially supported by NSERC and MITACS. D.W.K. was partially supported by NSERC, ERA, CFI, and ORF.

[1] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997); D. W. Leung, J. Math. Phys. **44**, 528 (2003).
[2] M. Mohseni and D. A. Lidar, Phys. Rev. A **75**, 062331 (2007).
[3] M. Reimpell and R. F. Werner, Phys. Rev. Lett. **94**, 080501 (2005); A. S. Fletcher, P. W. Shor, and M. Z. Win, Phys. Rev. A **75**, 012338 (2007); R. L. Kosur *et al.*, Phys. Rev. Lett. **100**, 020502 (2008).
[4] J. A. Holbrook *et al.*, Quantum Inf. Process. **2**, 381 (2003); D. W. Kribs, Proc. Edinb. Math. Soc. **46**, 421 (2003).
[5] C. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996); D. DiVincenzo *et al.*, IEEE Trans. Inf. Theory **48**, 580 (2002); H. Chau, *ibid.* **51**, 1451 (2005).
[6] C. Dankert *et al.*, e-print arXiv:quant-ph/0606161.
[7] J. Emerson *et al.*, Science **317**, 1893 (2007).
[8] D. W. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[9] D. W. Kribs and R. W. Spekkens, Phys. Rev. A **74**, 042329 (2006).
[10] M.-D. Choi, Linear Algebr. Appl. **10**, 285 (1975); K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory,* Lecture Notes in Physics Vol. 190 (Springer-Verlag, Berlin, 1983).
[11] R. Blume-Kohout *et al.*, e-print arXiv:0705.4282v1.
[12] D. Gottesman e-print arXiv:quant-ph/9807006; S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[13] B. Schumacher and M. D. Westmoreland, e-print arXiv:quant-ph/0112106; R. Klesse, Phys. Rev. A **75**, 062315 (2007).