QUANTUM ERROR CORRECTING CODES FROM THE COMPRESSION FORMALISM

MAN-DUEN CHOI

Department of Mathematics, University of Toronto, ON Canada, M5S 2E4
(e-mail: choi@math.toronto.edu)

DAVID W. KRIBS

Department of Mathematics and Statistics, University of Guelph, Guelph, ON Canada, N1G 2W1
Institute for Quantum Computing, University of Waterloo, ON Canada, N2L 3G1
(e-mail: dkribs@uoguelph.ca)

and

KAROL ŻYCZKOWSKI

Perimeter Institute for Theoretical Physics,
31 Caroline St. North, Waterloo, ON, Canada N2L 2Y5
Institute of Physics, Jagiellonian University, ul. Reymonta 4, 30-059 Cracow, Poland
Center for Theoretical Physics, Polish Academy of Sciences,
Al. Lotników 32/44, 02-668 Warsaw, Poland
(e-mail: karol@tatry.if.uj.edu.pl)

(*Received November 18, 2005*)

We solve the fundamental quantum error correction problem for bi-unitary channels on two-qubit Hilbert space. By solving an algebraic compression problem, we construct qubit codes for such channels on arbitrary dimension Hilbert space, and identify correctable codes for Pauli-error models not obtained by the stabilizer formalism. This is accomplished through an application of a new tool for error correction in quantum computing called the "higher-rank numerical range". We describe its basic properties and discuss possible further applications.

PACS numbers: 03.67.Pp, 03.67.Hk, 03.67.Lx, 03.67.Dd.
Keywords: quantum error correction, noisy quantum channels, algebraic compression, numerical range.

Introduction

Quantum computers will rely on a smorgasbord of error correction techniques to combat harmful effects such as decoherence on bits of information that are physically encoded within quantum systems. The quantum error correction "toolbox" now includes several strategies for accomplishing these feats, but there are still many deep issues to resolve. The standard method for error correction via active intervention in the quantum computing regime has been cleanly phrased in terms of an analysis of operators on Hilbert space. For every quantum channel that arises through the usual system-environment formalism, there is a family of error (or "Kraus") operators that describe the possible corruption by the channel of qubits encoded as states in, or operators on, the system Hilbert space. The main protocol for quantum error correction (QEC) [1–4] depends upon the existence and identification of states and operators on which the error operators are jointly well-behaved in a precise sense.

The stabilizer formalism for QEC [5, 6] gives a constructive framework to find correctable codes for error models of "Pauli type". While there are other successful techniques that can be applied in special cases (for instance, see [7–14]), the landscape of general strategies to find codes for other classes of channels is fairly sparse. In particular, the theory lacks a systematic method that applies to arbitrary quantum channels. Indeed, after spending any time at all on this problem, it becomes clear that this is an extremely daunting challenge.

Nevertheless, in this paper, we introduce an approach based on a "compression formalism" that may lead to such a general method. In particular, we cast the general problem of finding correctable codes for quantum channels into a matrix analysis framework. We then utilize a new tool recently introduced in [15]—called the "higher-rank numerical range"—the study of which was primarily motivated by this problem. As an application, we solve the quantum error correction problem in its entirety for the class of "bi-unitary channels" on two-qubit (i.e. four-dimensional) Hilbert space, and construct qubit codes for such channels in the arbitrary dimension case. In the case of Pauli-error models, we show that this approach captures codes not obtained via the Pauli matrix stabilizer formalism.

The rest of the paper is organized as follows. Next we recall basic properties of quantum channels and the formulation of the active quantum error correction protocol. We follow this by introducing the higher-rank numerical range as a tool in quantum error correction. We then consider randomized unitary channels, and focus on the bi-unitary case. This is followed by a characterization of correctable codes in the two-qubit case, and a consideration of the connection with the stabilizer formalism. We discuss possible further applications and limitations of this approach throughout the paper, and finish with a conclusion.

Quantum channels and active error correction

Consider an open quantum system S represented on a Hilbert space $\mathcal{H}$, and write $\mathcal{B}(\mathcal{H})$ for the set of operators that act on $\mathcal{H}$. A "snapshot" of a Hamiltonian-induced evolution of S is called a *quantum channel*. Mathematically, channels are represented by completely positive, trace preserving maps $\mathcal{E}$ on $\mathcal{B}(\mathcal{H})$. (For experimental reasons, the current focus in quantum computing is on finite-dimensional Hilbert spaces, and thus we shall make this assumption throughout the paper.) The structure theorem [16, 17] for completely positive maps shows that every quantum channel $\mathcal{E}$ on $\mathcal{H}$ has an operator-sum representation of the form $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ for all $\sigma \in \mathcal{B}(\mathcal{H})$, where the "error" operators (or "Kraus" operators) E_a are operators that act on $\mathcal{H}$.

A set of error operators $\{E_a\}$ can always be chosen with cardinality at most $N^2 := \dim(\mathcal{H})^2$. For simplicity, we shall always assume the maximum cardinality holds, by possibly including zero operators as some of the E_a. The trace preservation condition is equivalent to $\sum_a E_a^\dagger E_a = \mathbb{1}$. As a notational convenience, we shall write $\mathcal{E} = \{E_a\}$ when the E_a determine $\mathcal{E}$ through the operator-sum representation, and, as a further convenience, we will also use this notation when scalar multiples of the E_a are error operators for $\mathcal{E}$.

In the context of quantum computing, the operators E_a are the errors induced by the channel $\mathcal{E}$. Thus, error correction protocols in quantum computing are crafted primarily to mitigate the effects of such operators on quantum information encoded in evolving systems. By "active quantum error correction", we mean protocols that involve active intervention into the system to correct errors. The basic method for active quantum error correction [1–4] identifies *quantum codes* with subspaces $\mathcal{C}$ of the system Hilbert space $\mathcal{H}$. Then a code $\mathcal{C}$ is correctable for a channel $\mathcal{E}$ if all states encoded in $\mathcal{C}$ prior to the action of $\mathcal{E}$ can be fully recovered in a manner allowed by quantum mechanics. From the operator perspective, *$\mathcal{C}$ is correctable for $\mathcal{E}$* if there is a quantum channel $\mathcal{R}$ on $\mathcal{H}$ such that

$$\big(\mathcal{R} \circ \mathcal{E}\big)(\sigma) = \sigma, \tag{1}$$

for all operators σ supported on $\mathcal{C}$; that is, all σ of the form $\sigma = P_{\mathcal{C}} \sigma P_{\mathcal{C}}$ where $P_{\mathcal{C}}$ is the projection of $\mathcal{H}$ onto $\mathcal{C}$.

There is a very useful characterization [3, 4] of correctable codes for a given quantum channel $\mathcal{E}$, when a set of error operators $\mathcal{E} = \{E_a\}$ is known. The code $\mathcal{C}$ is correctable for $\mathcal{E} = \{E_a\}$ if and only if there is a scalar matrix $\Lambda = (\lambda_{ab})$ such that

$$P_{\mathcal{C}} E_a^\dagger E_b P_{\mathcal{C}} = \lambda_{ab} P_{\mathcal{C}}, \qquad \forall a, b. \tag{2}$$

Thus, Eq. (2) shows how the physical problem of active quantum error correction can be phrased in terms of a clean mathematical statement that involves relations satisfied by the error operators. The prototypical scenario occurs when $\mathcal{C}$ is correctable and the matrix $\Lambda = \Lambda_C$ is diagonal. Here the error operators take the code space to mutually orthogonal subspaces $E_a \mathcal{C}$. In the case that each of the errors restricted to $\mathcal{C}$ is a scalar multiple of a unitary U_a, the correction operation $\mathcal{R}$ is given by $\mathcal{R} = \{U_a^\dagger P_a\}$, where P_a is the projection of $\mathcal{H}$ onto the subspace $U_a \mathcal{C}$.

Let us note that every matrix Λ_C which satisfies Eq. (2) for some code space $\mathcal{C}$ is necessarily positive. Indeed, define E to be the $N^2 \times N^2$ positive block matrix

$$E = \begin{bmatrix} E_1^\dagger \\ E_2^\dagger \\ \vdots \end{bmatrix} \begin{bmatrix} E_1 \, E_2 \cdots \end{bmatrix} \geq 0, \tag{3}$$

where $E_1, E_2, \ldots$ is (any) enumeration of the set $\{E_a\}$, and $[E_1 \, E_2 \cdots]$ is the operator row matrix mapping from $\mathcal{H}^{(N^2)}$ to $\mathcal{H}$. (So $E_i^\dagger E_j$ is the (i, j) entry of E.)

Then observe that the set of equations from Eq. (2) can be succinctly stated as the single matrix equation

$$0 \leq \tilde{P}_{\mathcal{C}} E \tilde{P}_{\mathcal{C}} = \Lambda_C \otimes P_{\mathcal{C}}, \tag{4}$$

where $\tilde{P}_{\mathcal{C}}$ is the $N^2 \times N^2$ diagonal block matrix with $P_{\mathcal{C}}$ as the operator in each of the diagonal entries. In fact Λ_C is a density matrix when the E_a satisfy the trace preservation constraint (and $\mathcal{C}$ is non-zero);

$$\Big(\sum_a \lambda_{aa}\Big) P_{\mathcal{C}} = \sum_a P_{\mathcal{C}} E_a^\dagger E_a P_{\mathcal{C}} \tag{5}$$

$$= P_{\mathcal{C}} \Big(\sum_a E_a^\dagger E_a\Big) P_{\mathcal{C}} = P_{\mathcal{C}}. \tag{6}$$

Higher-rank numerical range and projections

The characterization from Eq. (2) of correctable codes motivates consideration of the following notion. Let σ belong to $\mathcal{B}(\mathcal{H})$. For $k \geq 1$, define the *rank-k numerical range* of σ to be the subset of the complex plane given by

$$\Lambda_k(\sigma) = \big\{\lambda \in \mathbb{C} \mid P\sigma P = \lambda P \text{ for some } P \in \mathcal{P}_k\big\}, \tag{7}$$

where $\mathcal{P}_k$ is the set of all rank-k projections on $\mathcal{H}$. We refer to elements of $\Lambda_k(\sigma)$ as “compression-values” for σ, since they are obtained through compressions of σ to k-dimensional subspaces. The case $k = 1$ yields the familiar numerical range $W(\sigma)$ for operators [18],

$$\Lambda_1(\sigma) = W(\sigma) = \{\langle \sigma\psi|\psi\rangle \mid |\psi\rangle \in \mathcal{H}, \, ||\, |\psi\rangle \,|| = 1\}. \tag{8}$$

It is clear that

$$\Lambda_1(\sigma) \supseteq \Lambda_2(\sigma) \supseteq \ldots \supseteq \Lambda_N(\sigma). \tag{9}$$

Of course, the cases $k > 1$ are of immediate interest in quantum error correction. We refer to the sets $\Lambda_k(\sigma)$, $k > 1$, as the *higher-rank numerical ranges*. This notion was recently introduced in [15], where a number of mathematical properties were developed. Here we briefly outline the main points. The following facts from [15] apply to arbitrary $\sigma \in \mathcal{B}(\mathcal{H})$.

PROPOSITION 1. *Let $\sigma \in \mathcal{B}(\mathbb{C}^N)$. For all $k \geq 1$, the rank-k numerical range $\Lambda_k(\sigma)$ is a compact subset of the complex plane $\mathbb{C}$. If $2k > N$, then $\Lambda_k(\sigma)$ is either empty or a singleton set. If $\Lambda_k(\sigma) = \{\lambda_0\}$ is a singleton set with $2k > N$, then λ_0 is an eigenvalue of geometric multiplicity at least $2k - N$. In particular, $\Lambda_N(\sigma)$ is non-empty if and only if σ is a scalar matrix.*

The main result of [15] is stated as follows.

THEOREM 1. *If $\sigma = \sigma^\dagger$ is a Hermitian operator on $\mathcal{H} = \mathbb{C}^N$, with eigenvalues (counting multiplicities) given by*

$$a_1 \leq a_2 \leq \ldots \leq a_N, \tag{10}$$

and $k \geq 1$ is a fixed positive integer, then the rank-k numerical range $\Lambda_k(\sigma)$ coincides with the set $[a_k, a_{N-k+1}]$ which is:

(i) *a non-degenerate closed interval if $a_k < a_{N-k+1}$,*
(ii) *a singleton set if $a_k = a_{N-k+1}$,*
(iii) *an empty set if $a_k > a_{N-k+1}$.*

The cases of non-degenerate spectra for $N = 4$ and $N = 6$ are depicted in Fig. 1. We note that the proof from [15] of this result is constructive, in the sense that the projections P associated with each $\lambda \in \Lambda_k(\sigma)$ can be explicitly identified. We shall extend this fact for special cases in the analysis of the next sections.

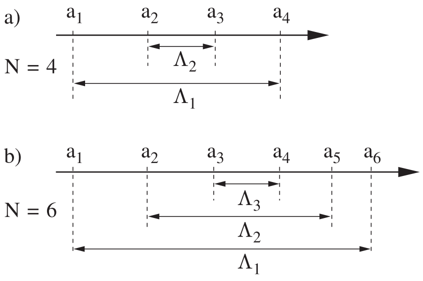

Fig. 1. Numerical range $\Lambda_k(\sigma)$ for a non-degenerate Hermitian operator σ of size a) $N = 4$ and b) $N = 6$ with spectrum $\{a_i\}$

Let us consider the following simple examples for the purpose of illumination.

(1) Let $\sigma = \sigma^\dagger$ be the operator on 2-qubit space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ given by

$$\sigma = |00\rangle\langle 00| + 2|01\rangle\langle 01| + 3|10\rangle\langle 10| + 4|11\rangle\langle 11|.$$

Then $\Lambda_1(\sigma) = [1, 4]$, $\Lambda_2(\sigma) = [2, 3]$, and $\Lambda_3(\sigma)$ and $\Lambda_4(\sigma)$ are empty.

(2) Consider the Pauli matrix $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Then $\Lambda_1(Z) = [-1, 1]$ and $\Lambda_2(Z)$ is empty. On $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, if we let $Z_1 = Z \otimes \mathbb{1}_2$, then $\Lambda_1(Z_1) = [-1, 1]$, $\Lambda_2(Z_1) = [-1, 1]$, and $\Lambda_3(Z_1)$ and $\Lambda_4(Z_1)$ are empty. More generally, if $Z_1 = Z \otimes \mathbb{1}_{2^{n-1}}$ acts on $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$, then $\Lambda_k(Z_1) = [-1, 1]$ for $k \leq 2^{n-1}$.

We have extended Theorem 1 in [15] partly to the case of normal operators; i.e. $\sigma \in \mathcal{B}(\mathcal{H})$ such that $\sigma\sigma^\dagger = \sigma^\dagger\sigma$. Recall that the convex hull $\operatorname{co}\Gamma$ of a subset $\Gamma \subseteq \mathbb{C}$ is given by

$$\operatorname{co}\Gamma = \left\{ t_1\lambda_1 + \cdots + t_m\lambda_m \,\middle|\, \sum_{j=1}^{m} t_j = 1,\ t_j \geq 0,\ \lambda_j \in \Gamma,\ m \geq 1 \right\}.$$

Notice that the following result applies to unitary operators. We have conjectured in [15] that the converse inclusion of Eq. (11) below holds for arbitrary normal operators σ.

THEOREM 2. *If σ is a normal operator on $\mathcal{H} = \mathbb{C}^N$, then for all $k \geq 1$, the rank-k numerical range $\Lambda_k(\sigma)$ is a subset of every convex hull $\operatorname{co}\Gamma$ where Γ is* *an* $(N+1-k)$*-point subset (counting multiplicities) of the spectrum of* σ*; that is*

$$\Lambda_k(\sigma) \subseteq \bigcap_{\Gamma} (\mathrm{co}\,\Gamma). \tag{11}$$

In the next section we shall present a solution to the error correction problem for a special class of channels. The solution depends on the analysis of higher-rank numerical ranges discussed above and specific properties of the channels. Before continuing, however, let us briefly describe a general method to find correctable codes based on this tool that may lead to more general applications. Let $\mathcal{E} = \{E_a\}$ be an arbitrary quantum channel on $\mathcal{B}(\mathcal{H})$. Then all correctable codes for $\mathcal{E}$ may be obtained by applying the following procedure:

(i) For all a, b, find scalars λ such that $PE_a^\dagger E_b P = \lambda P$ for some projection P.
(ii) For all λ from (i), find the projections P.
(iii) The set of intersections of ranges of projections P_{ab} over all distinct pairs a, b from (ii), corresponds precisely to the set of correctable codes for $\mathcal{E}$.

We emphasize that in QEC, the projections P from (ii) must be explicitly identified for practical applications in quantum computing. The idea in (iii) will be expanded upon in the discussion below. We have stated the problem in this form, because it lends itself to consideration as a “compression problem”. Of course, this process is still somewhat abstract. In particular, step (ii) will typically require taking infinitely many intersections. Nevertheless, there may be a way to avoid these infinities. Let us describe one simplification of the process. Namely, while the family of operators $E_a^\dagger E_b$, $\forall a, b$, will not be Hermitian in general, the solving of (i) and (ii) can be reduced to the Hermitian case, the case for which we have the most general information.

PROPOSITION 2. *The projection* P *is a solution to Eq.* (2) *for the family* $\{E_a^\dagger E_b : a, b\}$ *if and only if* P *is a solution to Eq.* (2) *for the family of Hermitian operators* $\{E_a^\dagger E_a, T_{ab}^+, T_{ab}^- : a, b\}$, *where*

$$T_{ab}^+ = E_a^\dagger E_b + E_b^\dagger E_a, \tag{12}$$

$$T_{ab}^- = i(E_a^\dagger E_b - E_b^\dagger E_a). \tag{13}$$

Proof: This simply follows from the fact that the operator subspace spanned by an operator A and its adjoint $A^\dagger$, is also spanned by the Hermitian operators $A + A^\dagger$ and $i(A - A^\dagger)$. □

Randomized unitary channels

The class of “randomized unitary channels” [19] form a large class of physical quantum operations. Such a channel has an operator-sum representation of the form $\mathcal{E}(\sigma) = \sum_k p_k U_k \sigma U_k^\dagger$, where the U_k are unitary and the $\{p_k\}$ determine a probability distribution. The error models $\mathcal{E} = \{U_k\}$ commonly arise in quantum error correction, quantum communication and cryptography, quantum information processing and theory, etc., and are of great physical relevance.

DEFINITION 1. A *bi-unitary channel* (BUC) is a randomized unitary channel $\mathcal{E} = \{V, W\}$ on a Hilbert space $\mathcal{H}$ with an operator-sum representation consisting of two unitaries; so

$$\mathcal{E}(\sigma) = pV\sigma V^\dagger + (1-p)W\sigma W^\dagger, \qquad \forall\sigma \in \mathcal{B}(\mathcal{H}), \tag{14}$$

for a fixed p with $0 < p < 1$.

We identify correctable qubit codes for all such channels, and we solve the error correction problem for BUCs on four-dimensional Hilbert space. The approach we use is constructive in nature and allows for an explicit identification of the correctable codes. We shall use properties of the higher-rank numerical range discussed in the previous section.

There are four non-zero equations to consider in Eq. (4) here. In terms of the matrix E, we must solve the following matrix equation for projections P and matrices $\Lambda = (\lambda_{ij})$:

$$\begin{pmatrix} pP & qrPV^\dagger WP \\ qrPW^\dagger VP & (1-p)P \end{pmatrix} = \begin{pmatrix} \lambda_{11}P & \lambda_{12}P \\ \lambda_{21}P & \lambda_{22}P \end{pmatrix}, \tag{15}$$

where we have written $q = \sqrt{p}$ and $r = \sqrt{1-p}$. For any projection P, the λ_{11} and λ_{22} equations are trivially satisfied with $\lambda_{11} = p$ and $\lambda_{22} = 1 - p$. Further, the λ_{12} equation is satisfied if and only if the λ_{21} equation is satisfied. Specifically,

$$qrPV^\dagger WP = \lambda P \quad \text{ if and only if } \quad qrPW^\dagger VP = \overline{\lambda}P. \tag{16}$$

Thus, we can reduce the entire problem to solving a single (normalized) equation of the form

$$PUP = \lambda P, \tag{17}$$

for λ and P, where U is a unitary on $\mathcal{H}$.

This can also be seen by simply noting that a code is correctable for the channel $\mathcal{E} = \{V, W\}$ precisely when it is correctable for $\mathcal{E}' = \{\mathbb{1}, V^\dagger W\}$. In fact, for ease of presentation, when it is convenient we shall assume the channel $\mathcal{E}$ has the latter form; i.e. there is a unitary U on $\mathcal{H}$ such that

$$\mathcal{E}(\sigma) = p\sigma + (1-p)U\sigma U^\dagger, \qquad \forall\sigma \in \mathcal{B}(\mathcal{H}). \tag{18}$$

Thus, in the case that $\mathcal{H} = \mathbb{C}^4$, we must solve Eq. (17) for an arbitrary 4×4 unitary U. This follows from the next result.

THEOREM 3. *Let U be a unitary on $\mathcal{H} = \mathbb{C}^4$. Then we have the following characterizations of the numerical ranges for U:*

(i) *$\Lambda_1(U) = W(U)$ is the subset of the unit disk in $\mathbb{C}$ given by the convex hull of the eigenvalues for U.*

(ii) *$\Lambda_2(U)$ is non-empty and given as follows. Let $z_k = e^{i\theta_k}$, with $\theta_k \in [0, 2\pi)$ for $k = 1, 2, 3, 4$, be the eigenvalues for U, ordered so that $0 \leq \theta_1 \leq \theta_2 \leq \theta_3 \leq \theta_4 < 2\pi$.*

(a) *If the spectrum of U is non-degenerate, so $\theta_k \neq \theta_j$ $\forall k \neq j$, then $\Lambda_2(U) = \{\lambda\}$, where λ is the intersection point in $\mathbb{C}$ of the line ℓ_{13} through z_1 and z_3, with the line ℓ_{24} through z_2 and z_4.*

(b) *If U has three distinct eigenvalues, say $\theta_j = \theta_k$ for some pair $j \neq k$ but $\theta_j \neq \theta_l$ otherwise, then $\Lambda_2(U) = \{z_j\}$.*

(c) *If U has two distinct eigenvalues, each of multiplicity two, say z and w, then $\Lambda_2(U)$ consists of the line segment $L = [z, w]$ joining z and w.*

(d) *If U has two distinct eigenvalues, one $\lambda = z$ with multiplicity three and the other with multiplicity one, then $\Lambda_2(U) = \{z\}$.*

(e) *If U has a single eigenvalue $\lambda = z$, then U is the scalar operator $U = z\mathbb{1}_4$ and $\Lambda_2(U) = \{z\}$.*

(iii) *$\Lambda_3(U)$ is non-empty if and only if $\Lambda_3(U) = \{\lambda_0\}$ is a singleton set and λ_0 is an eigenvalue for U of geometric multiplicity at least three,*

$$\dim(\ker(U - \lambda_0\mathbb{1})) \geq 3. \tag{19}$$

(iv) *$\Lambda_4(U)$ is non-empty if and only if U is a scalar multiple of the identity operator.*

Proof: The structure of the standard numerical range $\Lambda_1(U) = W(U)$ follows from well-known matrix analysis theory [18], and the structures of $\Lambda_k(U)$, $k = 3, 4$, follow from Proposition 1 and Theorem 2. The case of interest is that of (ii).

To see (ii), notice that Theorem 2 can be applied to show that $\Lambda_2(U)$ is contained in the claimed set for each of the subcases. (See Fig. 2 for a depiction of the four non-trivial cases (a), (b), (c), and (d).) For the converse inclusion in each case, we offer a constructive proof of the required rank-2 projections.

To verify case (a), it suffices to show that the intersection point λ of ℓ_{13} and ℓ_{24} belongs to $\Lambda_2(U)$. First solve the following equations,

$$\begin{cases} \lambda = az_1 + bz_3, \\ \lambda = cz_2 + dz_4 \end{cases} \tag{20}$$

for nonnegative scalars $a, b, c, d \geq 0$ such that $a+b = 1$ and $c+d = 1$. For instance, a and $b = 1 - a$ may be obtained via the equation

$$a = \cos^2\theta_a = \frac{\lambda - z_1}{z_1 - z_3}, \tag{21}$$

for some angle θ_a. Then define an orthonormal pair of vectors $\{|\phi_1\rangle, |\phi_2\rangle\}$ by

$$\begin{cases} |\phi_1\rangle = \cos\theta_a|\psi_1\rangle + \sin\theta_a|\psi_3\rangle, \\ |\phi_2\rangle = \cos\theta_c|\psi_2\rangle + \sin\theta_c|\psi_4\rangle. \end{cases} \tag{22}$$

Then we define a rank-2 projection

$$P = |\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2|. \tag{23}$$

Observe that

$$\langle U\phi_1|\phi_1\rangle = \cos\theta_a z_1\langle\psi_1|\phi_1\rangle + \sin\theta_a z_3\langle\psi_3|\phi_1\rangle \tag{24}$$

$$= az_1 + bz_3 = \lambda. \tag{25}$$

Similarly, we have $\langle U\phi_2|\phi_2\rangle = \lambda$. Further, we also have

$$\langle U\phi_1|\phi_2\rangle = 0 = \langle U\phi_2|\phi_1\rangle. \tag{26}$$

It follows that $PUP = \lambda P$, and hence λ belongs to $\Lambda_2(U)$ as claimed. This verifies case (a).

In case (b), the rank-2 projection $P = |\psi_j\rangle\langle\psi_j| + |\psi_k\rangle\langle\psi_k|$ can be seen to satisfy $PUP = z_j P$. For case (d), without loss of generality assume $z_1 = z_2 = z_3 = z \neq z_4$. Then $P = \sum_{j=1}^{3} |\psi_j\rangle\langle\psi_j|$ satisfies $PUP = zP$. This verifies both case (b) and (d).

Finally, for case (c), we have say $z_1 = z_2 = z$ and $z_3 = z_4 = w$. Let λ belong to the line segment $\ell = [w, z]$, and, as above, solve the following equations for a, b, c, d;

$$\begin{cases} \lambda = az_1 + bz_3 = az + bw, \\ \lambda = cz_2 + dz_4 = cz + dw. \end{cases} \tag{27}$$

Then define $\{|\phi_1\rangle, |\phi_2\rangle\}$ precisely as in Eqs. (21 and 22). With $P = |\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2|$, we have $PUP = \lambda P$. Thus, $\Lambda_2(U)$ coincides with $L = [w, z]$ in this case, and the result follows. □

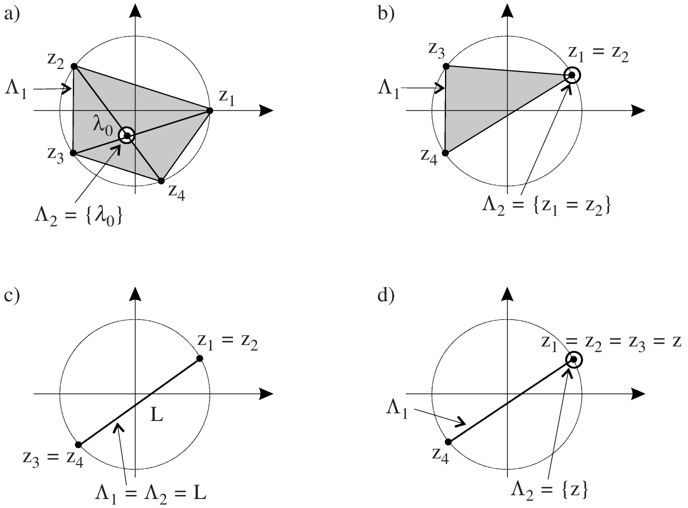

Fig. 2. Numerical ranges Λ_1 and Λ_2 of a unitary operator $U \in U(4)$ and the structure of the spectrum of U: a) generic case; b) double degeneracy; c) both eigenvalues doubly degenerated; d) triple degeneracy.

The construction of rank-2 projections used in the previous proof is typical in a certain sense. Ostensibly this follows because, as proved above, these sets have no topological interior. They are either finite discrete sets, or line segments. We shall provide full details on this point in the next section. (In fact, this result together with the discussion of the subsequent section can be easily adjusted to verify the higher-rank numerical range conjecture from [15] for arbitrary normal operators on 4-dimensional Hilbert space.) Of course, a further extension of Theorem 3 to the case of arbitrary $\Lambda_k(U)$ would greatly benefit from either the verification of the conjecture, or, at the least, more substantive information on these sets for arbitrary unitary operators.

We can establish the following as a consequence of the previous proof.

THEOREM 4. *Let $\mathcal{E} = \{V, W\}$ be a BUC on a Hilbert space $\mathcal{H}$ with* $\dim \mathcal{H} \geq 4$. *Then there are 2-dimensional code subspaces $\mathcal{C}$ of $\mathcal{H}$ such that $\mathcal{C}$ is correctable for $\mathcal{E}$.*

Proof: As in Eq. (18), we may assume the channel is of the form $\mathcal{E} = \{\mathbb{1}, U\}$. Thus, the theorem will be proved if we can show that $\Lambda_2(U)$ is non-empty for an arbitrary unitary operator U.

In the case $\mathcal{H} = \mathbb{C}^4$, this result follows directly from case (ii) of Theorem 3. Indeed, observe that $\Lambda_2(U)$ is shown to be non-empty in each of the subcases of (ii). The analysis of this case may be adapted to the case of arbitrary $\mathcal{H}$. To see this, note first that if there is degeneracy in the spectrum of U, say the eigenvalue $\lambda = z_j$ has multiplicity at least two, then we can simply choose a rank-2 sub-projection of the eigen-projection for z_j to show that $\Lambda_2(U)$ is non-empty in this case.

On the other hand, if there is no degeneracy in the spectrum of U, then we may find four distinct eigenvalues for U lying on the unit circle, $z_j = e^{i\theta_j}$, $j = 1, 2, 3, 4$, ordered so that $0 \leq \theta_1 < \theta_2 < \theta_3 < \theta_4 < 2\pi$. As in the previous proof, we can now use the constructive "eigenvalue pairing" approach to show that the intersection point of the line through z_1 and z_3, with the line through z_2 and z_4, belongs to the set $\Lambda_2(U)$. This completes the proof. □

Let us note that Theorem 3 can also be used in a negative fashion. For instance, consider the class of two-qubit randomized unitary channels with at least three distinct unitary error operators. We can conclude from Theorem 3 that the set of such channels for which there exist correctable codes forms a set of measure zero within the set of all such channels. (Contrast this with the case of BUCs in Theorem 4.) Indeed, if $\mathcal{E} = \{\mathbb{1}, U, V\}$ is a two-qubit channel with $U \neq V$, and neither equal to a scalar multiple of $\mathbb{1}$, then there are three pertinent equations to solve of the form given in Eq. (17); namely, for the unitaries U, V, and $U^\dagger V$. But we know that in the generic non-degenerate case, the set Λ_2 will be a singleton, and that there will almost never be a projection of rank at least two that simultaneously solves Eq. (17) for all three operators.

Correctable codes for the two-qubit case

We first discuss a simple example to illustrate the connection with the stabilizer formalism. Let $\mathcal{E} = \{\mathbb{1}_4, ZZ\}$ be the error model on $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ for a channel that leaves states alone with some probability, and applies the Pauli phase flip operator $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ on each qubit with another probability. We have chosen this particular example to simplify the presentation, but a similar analysis applies to any of the two-qubit Pauli-error models.

The stabilizer formalism applied to the error model $\mathcal{E} = \{\mathbb{1}_4, ZZ\}$ obtains codes by considering the joint eigenspace structure for the error operators $\{\mathbb{1}_4, ZZ\}$, and hence just $ZZ = Z \otimes Z$ in this case. Through this approach one can find the rank-2 projections

$$P_1 = |00\rangle\langle 00| + |11\rangle\langle 11|, \tag{28}$$

$$P_{-1} = |01\rangle\langle 01| + |10\rangle\langle 10|, \tag{29}$$

as correctable codes for $\mathcal{E} = \{\mathbb{1}_4, ZZ\}$. Indeed, Eq. (2) is satisfied since $P_{\pm 1} ZZ P_{\pm 1} = ZZ P_{\pm 1} = \pm P_{\pm 1}$.

On the other hand, the higher-rank numerical range approach captures these projections, and more. Specifically, as ZZ is Hermitian, Theorem 1 can be applied to obtain $\Lambda_2(ZZ) = [-1, 1]$. Thus, there is a family of rank-2 projections, each of which yields a correctable qubit code for $\mathcal{E} = \{\mathbb{1}_4, ZZ\}$, for every element $\lambda \in [-1, 1]$. For instance, given $a, b, c, d \geq 0$ such that $a + b = 1 = c + d$, we can define

$$|\psi_1\rangle = \sqrt{a}|00\rangle + \sqrt{b}|01\rangle, \tag{30}$$

$$|\psi_2\rangle = \sqrt{c}|11\rangle + \sqrt{d}|10\rangle, \tag{31}$$

and define $P = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|$. Then $PZZP = \lambda P$ (though note it is not true in general that $PZZP = ZZP$), and it follows that $P\mathcal{H} = \mathrm{span}\{|\psi_1\rangle, |\psi_2\rangle\}$ is correctable for $\mathcal{E} = \{\mathbb{1}_4, ZZ\}$. Notice that P_1 is captured by $b = d = 0$ and P_{-1} by $a = c = 0$. However, the cases $a \neq b$ and $c \neq d$ are not obtained as stabilizers of two-qubit Pauli-error models.

REMARK 1. There are more projections that yield correctable codes for $\mathcal{E}$, and we shall indicate this in the context of the next example. We first wish to emphasize a basic point exposed by this example. The operator equation $PAP = \lambda P$ does not necessarily imply $AP = \lambda P$; i.e., if the compression of an operator A by a projection P is a scalar multiple of P, then not necessarily is the restriction of A also a scalar multiple of P. In terms of the block matrix decomposition of A with respect to $\mathcal{H} = P\mathcal{H} \oplus P^{\perp}\mathcal{H}$, these two statements can be phrased visually as follows:

$$PAP = \lambda P \quad \text{if and only if} \quad A = \begin{pmatrix} \lambda \mathbb{1}_P & * \\ * & * \end{pmatrix} \tag{32}$$

$$AP = \lambda P \quad \text{if and only if} \quad A = \begin{pmatrix} \lambda \mathbb{1}_P & * \\ 0 & * \end{pmatrix}. \tag{33}$$

It is evident that Eq. (32) allows for more possibilities.

To be more precise, given an error model $\mathcal{E} = \{E_a\}$, one way to seek correctable codes for $\mathcal{E}$ is to consider the joint eigenspaces for the operators E_a (as is done in the stabilizer formalism applied for Pauli errors); i.e. projections P such that $E_a P = \lambda_a P$ for some scalar λ_a, for all a. (Recall also that by Proposition 2, the E_a may be assumed to be Hermitian.) Then necessarily Eq. (2) is satisfied for all a, b. However, $PE_a^\dagger E_b P = \lambda_{ab} P$ does not in general imply that P is a joint eigen-projection for E_a and E_b. Thus, the previous example, and those that follow, are illustrative of a more general phenomena. Namely, to capture all possible correctable codes, we need to consider "compressions" of operators instead of restricting ourselves to "restrictions".

Let us discuss, in more detail than the previous example, the correctable code structure for the Pauli-error model given by $\mathcal{E} = \{\mathbb{1}_4, Z_1\}$ on $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, where

$$Z_1 = Z \otimes \mathbb{1}_2 = |00\rangle\langle 00| + |01\rangle\langle 01| - |10\rangle\langle 10| - |11\rangle\langle 11|.$$

Here the structure of $\Lambda_2(Z_1) = [-1, 1]$ determines the code structure for $\mathcal{E}$. Let us consider the case $\lambda = 0 \in \Lambda_2(Z_1)$. Let P_+ (respectively P_-) be the projection onto the eigenspace $\mathcal{V}_+ = \operatorname{span}\{|00\rangle, |01\rangle\}$ (respectively $\mathcal{V}_- = \operatorname{span}\{|10\rangle, |11\rangle\}$). Then a typical rank-2 code for $\mathcal{E}$ is given as follows. Let $\{|\psi_\pm\rangle, |\phi_\pm\rangle\}$ be an orthonormal pair of vectors in $\mathcal{V}_\pm$. Define

$$\mathcal{C} = \operatorname{span}\{|\psi_+\rangle + |\psi_-\rangle, |\phi_+\rangle + |\phi_-\rangle\}. \tag{34}$$

One can verify that $PZ_1P = 0 = 0P$. For instance, if $|\psi\rangle = |\psi_+\rangle + |\psi_-\rangle$, then

$$\langle Z_1\psi|\psi\rangle = \langle\psi_+|\psi_+\rangle - \langle\psi_-|\psi_-\rangle = 0. \tag{35}$$

On the other hand, suppose $\mathcal{C}$ is a two-dimensional subspace, with projection P, such that $PZ_1P = 0$. Then it follows that $\mathcal{C} = P\mathcal{H} = P_+P\mathcal{H} \oplus P_-P\mathcal{H}$, and that each of the subspaces $P_\pm P\mathcal{H}$ is two-dimensional. Hence, as two-dimensional subspaces of $\mathcal{V}_\pm$, we have $P_\pm P\mathcal{H} = \mathcal{V}_\pm$. Thus, $\mathcal{C}$ necessarily has the form given in Eq. (34). (See [15] for a more complete discussion on this point in the arbitrary Hermitian case.)

We finish by characterizing the correctable codes for a generic BUC on two-qubit Hilbert space. As above, for error correction purposes, we may assume such a channel has the form $\mathcal{E} = \{\mathbb{1}_4, U\}$, where U is a unitary on $\mathcal{H} = \mathbb{C}^4$. In the generic case, the spectrum of U will be non-degenerate, and so we can assume the eigenvalues for U are four distinct complex numbers $\{z_1, z_2, z_3, z_4\}$, ordered so that $0 \leq \arg z_1 < \ldots < \arg z_4 < 2\pi$. Let $|\psi_j\rangle$ be corresponding eigenvectors; $U|\psi_j\rangle = z_j|\psi_j\rangle$.

By Theorem 3, the correctable qubit codes for $\mathcal{E}$ correspond to the projections P that satisfy Eq. (17) for the unique λ that belongs to $\Lambda_2(U)$. Without loss of generality, we shall assume $\lambda = 0$. (The reader will notice that the following argument applies to normal operators. Hence, if $\Lambda_2(U) = \{\lambda\}$, then we could replace U by the normal operator $U - \lambda \mathbb{1}_4$.)

Given that $\Lambda_2(U) = \{0\}$, we claim that

$$P = |\xi_1\rangle\langle\xi_1| + |\xi_2\rangle\langle\xi_2| \tag{36}$$

is a rank-2 projection such that

$$PUP = 0 \tag{37}$$

if and only if there are angles $\alpha_k, \beta_k, \gamma_k, \theta_{kj}$, for $k = 1, 2$ and $j = 2, 3, 4$, such that

$$|\xi_k\rangle = a_k|\psi_1\rangle + b_k|\psi_2\rangle + c_k|\psi_3\rangle + d_k|\psi_4\rangle, \tag{38}$$

where

$$\begin{cases} a_k = \cos\alpha_k \cos\beta_k, \\ b_k = e^{i\theta_{k2}} \sin\alpha_k \cos\gamma_k, \\ c_k = e^{i\theta_{k3}} \cos\alpha_k \sin\beta_k, \\ d_k = e^{i\theta_{k4}} \sin\alpha_k \sin\gamma_k, \end{cases} \tag{39}$$

and the following equations are satisfied:

$$\begin{cases} \cos^2\beta_k z_1 + \sin^2\beta_k z_3 = 0, \\ \cos^2\gamma_k z_2 + \sin^2\gamma_k z_4 = 0, \end{cases} \tag{40}$$

and

$$\begin{cases} a_1 a_2 z_1 + b_1 \overline{b_2} z_2 + c_1 \overline{c_2} z_3 + d_1 \overline{d_2} z_4 = 0, \\ a_1 a_2 z_1 + \overline{b_1} b_2 z_2 + \overline{c_1} c_2 z_3 + \overline{d_1} d_2 z_4 = 0. \end{cases} \tag{41}$$

To verify the sufficiency of these constraints for Eq. (37), it must be shown that $\langle U\xi_k|\xi_l\rangle = 0$ for $k, l = 1, 2$ when ξ_1 and ξ_2 are defined as in Eq. (38) and the subsequent equations. This follows from Eqs. (40) and (41), and we leave this computation to the interested reader. Note the special case of this construction in which the vectors are obtained from the eigenvalue-pairing construction as in Eq. (22). (In that case, Eq. (41) is trivially satisfied.)

On the other hand, for necessity, suppose P and ξ_1, ξ_2 are given as in Eq. (36) and Eq. (38), and that $PUP = 0$. Then Eq. (41) comes as a direct consequence of the identity $\langle U\xi_1|\xi_2\rangle = 0 = \langle U\xi_2|\xi_1\rangle$. Further, for $k = 1, 2$ we have

$$0 = \langle U\xi_k|\xi_k\rangle \tag{42}$$

$$= |a_k|^2 z_1 + |b_k|^2 z_2 + |c_k|^2 z_3 + |d_k|^2 z_4. \tag{43}$$

In particular, this implies that

$$|a_k|^2 z_1 + |c_k|^2 z_3 = -|b_k|^2 z_2 - |d_k|^2 z_4 = 0, \tag{44}$$

as this equation describes the intersection point ($\lambda = 0$) of the line through z_1, z_3 with the line through z_2, z_4. This yields Eq. (40), and for succinctness we shall leave the verification of the specific form of the scalars a_k, b_k, c_k, d_k given by Eq. (39) to the reader.

Let us briefly summarize how one can find all correctable codes for any given bi-unitary channel $\mathcal{E} = \{V, W\}$ on $\mathcal{H} = \mathbb{C}^4$:

(i) Compute the set of compression-values $\Lambda_2(V^\dagger W)$ via Theorem 3.
(ii) For each compression-value λ from (i), the family of projections P that satisfy $PV^\dagger WP = \lambda P$ may be obtained as in the discussion of this section.
(iii) The subspaces corresponding to ranges of projections from (ii) are precisely the correctable codes for $\mathcal{E} = \{V, W\}$.

Conclusion

We have solved the fundamental error correction problem in quantum computing for bi-unitary channels on two-qubit Hilbert space. This was accomplished through an application of a new tool—the “higher-rank numerical range”—that has been recently developed to solve algebraic compression problems. We have shown that, in the case of Pauli-error models, this approach captures codes not obtained through the stabilizer formalism for Pauli matrices. We also discussed further applications to more general quantum channels on larger Hilbert spaces. As an example, we constructed qubit codes for bi-unitary channels on arbitrary Hilbert spaces. (Compression error correcting codes for bi-unitary channels on arbitrary Hilbert spaces will be analyzed in a forthcoming article [23].) We also discussed how this approach can be used to establish negative results.

To apply the information we have derived for the higher-rank numerical ranges in the Hermitian case more generally, a better understanding of the intersections of projections in Eq. (2) is required. As another avenue to more general applications, a complete understanding of the higher-rank numerical range for the case of normal operators, or even unitary operators, could help in special cases such as the class of randomized unitary channels. We have not considered possible implications of the higher-rank numerical ranges to problems in the new protocol for error correction called “operator quantum error correction” [20, 21]. In this scheme, a characterization of correction has been obtained [21, 22] that generalizes Eq. (2), and it may be possible to apply these tools to that more general setting.

Acknowledgements

We would like to thank Daniel Gottesman and Raymond Laflamme for helpful discussions. We are also grateful to other colleagues at IQC, PI, and UofG for stimulating conversations. M.D.C. and D.W.K. were partially supported by NSERC. K. Ż. is thankful to Perimeter Institute for creating optimal working conditions in Waterloo and acknowledges a partial support by the grant number PBZ-MIN-008/P03/2003 of Polish Ministry of Science and Information Technology.

REFERENCES

[1] P. W. Shor: *Phys. Rev. A* **52** (1995), R2493.
[2] A. M. Steane: *Phys. Rev. Lett.* **77** (1996), 793.
[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters: *Phys. Rev. A* **54** (1996), 3824.
[4] E. Knill and R. Laflamme: *Phys. Rev. A* **55** (1997), 900.
[5] D. Gottesman: *Phys. Rev. A* **54** (1996), 1862.
[6] D. Gottesman: Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997).
[7] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane: *Phys. Rev. Lett.* **78** (1997), 405.
[8] E. M. Rains, R. H. Hardin, P. W. Shor and N. J. A. Sloane: *Phys. Rev. Lett.* **79** (1997), 953.
[9] D. Aharonov and M. Ben-Or: arxiv.org/quant-ph/9906129.
[10] E. M. Rains: *IEEE Trans. Inf. Theory* **45** (1999, 2361).
[11] M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
[12] A. Klappenecker and M. Roetteler: *IEEE Trans. Inf. Theory*, **48** (2002), 2392.
[13] H. Pollatsek and M. B. Ruskai: *Lin. Alg. Appl.* **392** (2004), 255.
[14] D. Gottesman: *arxiv.org/quant-ph/0507174*.
[15] M. D. Choi, D. W. Kribs and K. Życzkowski: *Lin. Alg. Appl.*, to appear.
[16] M. D. Choi, *Lin. Alg. Appl.* **10** (1975), 285–290.
[17] K. Kraus, *Ann. Physics* **64** (1971), 311–335.
[18] P. Halmos: *Measure Theory*, D. Van Nostrand Company, Ltd., Toronto 1967.
[19] R. Alicki and K. Lendi: *Quantum Dynamical Semigroups and Applications*, Lecture Notes in Physics, Vol. 286, Springer, Berlin 1987.
[20] D. W. Kribs, R. Laflamme and D. Poulin: *Phys. Rev. Lett.* **94** (2005), 180501.
[21] D. W. Kribs, R. Laflamme, D. Poulin and M. Lesosky: *Quant. Inf. Comp.* **6** (2006), 382–399.
[22] M. A. Nielsen and D. Poulin: arxiv.org/quant-ph/0506069.
[23] M. D. Choi, J. A. Holbrook, D. W. Kribs and K. Życzkowski: in preparation.