Zero-error subspaces of quantum channels

Samuel L Braunstein[1], David W Kribs[2], and Manas K Patra[1]

[1]Department of Computer Science, University of York, York YO10 4HZ, UK
[2]IQC, University of Waterloo and Department of Mathematics, University of Guelph, Guelph, Ontario, Canada

***Abstract*—This work deals with zero-error subspaces of quantum channels and their intimate connection with quantum *and* classical codes. We give operator algebraic characterizations of such subspaces and give some upper and lower bounds on their maximum dimension. Classical and quantum codes and (quantum) noiseless subsystems may be considered as special cases of zero-error subspaces. We explore several consequences of this fact.**

I. Introduction

Communication or computing components such as channels, registers and gates are affected by noise. In classical and quantum information theory the effect of noise is most conveniently modeled as a stochastic process. More precisely, it is represented as a stochastic map. In classical communication models the map is a stochastic matrix in the usual sense [PB10]. In quantum systems it is a completely positive map. Thus we consider a two-terminal quantum channel C as a *completely positive* (**CP**) map $\Phi_C : \mathcal{A} \to \mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are C^* algebras. For most of the work the algebras will be assumed to be finite dimensional. Then, $\mathcal{A}$ and $\mathcal{B}$ are subalgebras of $B(H_1)$ and $B(H_2)$ closed under hermitian conjugation for some finite-dimensional Hilbert spaces H_1 and H_2. Here $B(H)$ denotes the algebra of (bounded) operators on a Hilbert space H. Let the $\dim(H_1) = n$ and $\dim(H_2) = m$. Assume that $\mathcal{A} = B(H_1)$ and $\mathcal{B} = B(H_2)$. Then Choi's theorem asserts that there exist $k \leqslant mn$ operators $E_i : H_1 \to H_2$ such that

$$\Phi_C(A) = \sum_{i=1}^{k} E_i A {E_i}^\dagger, \quad A \in \mathcal{A} \tag{1}$$

We write $\Phi_C = \{E_i\}$ with the understanding the action of Φ_C is given by the above formula. Let us suppose that the quantum source generates orthogonal states in H_1. By a state we mean in general a density matrix, a positive operator with trace 1 and orthogonality is with respect to the trace norm on $B(H_1)$. The output states will not be orthogonal in general. Since non-orthogonality implies that the states cannot be distinguished unambiguously we have to devise strategies for minimizing the probability of error. The most well-studied and perhaps effective strategy in both classical and quantum domain is error correction. Another strategy is to confine to error-free subspaces. These two approaches can be combined in the so-called operator error correction theory [KLPL06].

II. Zero-error Subspaces

For purposes of communication rather than computation a somewhat more general approach may be considered. It is called the zero-error communication theory and was first analyzed for classical channels by Shannon [Sha56]. The basic idea is to seek subsets or subspaces with a distinguished orthogonal basis (in the quantum case) on which the channel acts as a "lossless" channel (see [PB10] for an algebraic characterization). Equivalently, we look for sets of orthogonal states $\{\rho_1, \ldots, \rho_k\}$ such that if $i \neq j$ then

$$\langle \Phi_C(\rho_i), \Phi_C(\rho_k) \rangle \equiv \mathtt{Tr}(\Phi_C(\rho_i)\Phi_C(\rho_k)) = 0, \ i \neq k$$

Now if the positive operators ρ_i are expressed in their respective eigenbasis

$$\rho_i = \sum_{j=1}^{l} p_j^i \, |\alpha_j^i\rangle\langle\alpha_j^i| \,, \ \rho_k = \sum_{j=1}^{m} p_j^k \, |\alpha_j^k\rangle\langle\alpha_j^k| \,,$$
$$p_j^i, p_j^k > 0 \text{ and } \sum_j p_j^i = \sum_j p_j^k = 1$$

Then a simple application of (1) yields that $\langle \Phi_C(\rho_i), \Phi_C(\rho_j) \rangle = 0$ if and only if

$$\left\langle \alpha_p^i \middle| {E_r}^\dagger E_s \middle| \alpha_q^k \right\rangle = 0, \quad i \neq k \text{ and } 1 \leqslant r, s \leqslant a \tag{2}$$

If ρ_i and ρ_j are projections (pure states) then $l = m = 1$. We are therefore led to consider orthogonal sets[1] $\{\beta_1, \ldots \beta_k\}$[2] of vectors such that

$$\left\langle \beta_i \middle| F \middle| \beta_j \right\rangle = 0, \quad i \neq j \text{ and}$$
$$F \in \mathcal{S}_C \equiv \text{span}\{{E_r}^\dagger E_s, \ 1 \leqslant r, s \leqslant a\} \subset B(H_1)$$

Note that the space $\mathcal{S}_C$ is self-adjoint in the sense that if $F \in \mathcal{S}_C$ then $F^\dagger \in \mathcal{S}_C$. If the channel map Φ_C is *unital* (maps identity to identity or equivalently, preserves trace), then $I_n \in \mathcal{S}$. Hence $\mathcal{S}_C$ is an *operator system*[Pau03]. Even when the channel map is not unital we adjoin the unit. This does not affect the definition of zero-error subspace. Given an operator system $\mathcal{S}$ we call two vectors α and β, $\mathcal{S}$-orthogonal if $\langle\alpha|F|\beta\rangle = 0$ for all $F \in \mathcal{S}$. In the light of the preceding discussion any set $Q \subset H_1$ consisting of pairwise $\mathcal{S}_C$-orthogonal vectors are mapped to mutually orthogonal states. Since $I_n \in \mathcal{S}_C$ the vectors in Q are orthogonal in the usual sense and the cardinality of Q must be $\leqslant n$. The subspace spanned by Q is called a zero-error subspace (see [DSW10] and the references there for more on zero-error subspaces and capacity). We emphasize that zero-error subspaces are subspaces with a distinguished S_C-orthogonal basis. We consider subspaces to make the connection with quantum codes

[1]We will not bother about normalization since that can always be done.
[2]We suppress Dirac notation of bras and kets for convenience. However we continue to use them in inner products.

978-1-4577-0595-3/11/$26.00 ©2011 IEEE

(which are subspaces) and noiseless subspaces. Further, our main characterization result (Theorem 1) requires the notion of subspaces. Hence it is natural to seek zero-error subspaces with maximum dimension. This maximal dimension will be called the zero-error rank z_C of C (z_C is called independence number [DSW10] but we will be defining a different kind of independence). Our next task is to give characterization of zero-error subspaces in terms of the operator system $\mathcal{S}_C$. We first define some concepts well-known to operator theorists.

Let H be Hilbert space of dimension n. Let S be a subspace of $\mathcal{B}(H)$. Then S is called transitive if for any non-zero $\alpha \in H$ we have

$$S\alpha \equiv \{F\alpha : F \in S\} = H \tag{3}$$

Clearly any $S\alpha$ is a subspace of H. Let $M_k = M_k(\mathbb{C})$ denote the space of $k \times k$ complex matrices. Then $M_k \otimes S \equiv M_k(S)$ is the space of order k matrices whose entries are elements of S. It acts on $\bigoplus^k H = H \oplus H \oplus \cdots \oplus H$, the direct sum of k copies of H. A set of (non-zero) vectors $\alpha_1, \ldots, \alpha_k \in H$ are called S-independent if there is no relation

$$\alpha_i = \sum_{j \neq i} A_{ij}\alpha_j,\ A_{ij} \in S$$

If the identity operator belongs to S then S-independence implies linear independence. Define S to be weak k-transitive if for any set of S-independent vectors $\alpha_1, \ldots, \alpha_k \in H$ we have

$$M_k(S) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = H^{\oplus k} \tag{4}$$

Here we write elements of $H^{\oplus k}$ as columns with entries from H. We note that our definition of (weak) k-transitivity is weaker than that of [Azo86], [DMR08] in the sense that the latter implies former. Of course, the two definitions coincide when $k = 1$. We need the weaker transitivity because we demand stronger form of orthogonality. Since no $r > n$ vectors can be independent in H, S is vacuously weak r-transitive. So when we talk of k-transitivity we implicitly assume $k \leqslant n$. We also drop the adjective weak since this is the only kind we will be dealing with.

Lemma 1. *For $0 < k < n$, k-transitivity implies $(k+1)$-transitivity.*

Proof: Let $\alpha_1, \ldots, \alpha_{k+1} \in H$ be S-independent and $\beta_1, \ldots, \beta_{k+1}$ be arbitrary vectors in H. There is matrix A_1 in $M_k(S)$ such that $A_1 \begin{pmatrix} \alpha_1 & \ldots & \alpha_k \end{pmatrix}^T = \begin{pmatrix} \beta_1 & \ldots & \beta_k \end{pmatrix}^T$ where the superscript T denotes transpose. Similarly there is $A_2 \in M_k(S)$ such that $A_1 \begin{pmatrix} \alpha_2 & \ldots & \alpha_{k+1} \end{pmatrix}^T = \begin{pmatrix} 0 & \ldots & 0 & |\beta_{k+1}\rangle \end{pmatrix}^T$. Let

$$A = \begin{pmatrix} & & 0 \\ & A_1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & A_2 & \\ 0 & & \end{pmatrix}$$

It is clear that $A \begin{pmatrix} \alpha_1 & \ldots & \alpha_{k+1} \end{pmatrix}^T = \begin{pmatrix} |\beta_1\rangle & \ldots & |\beta_{k+1}\rangle \end{pmatrix}^T$. S is $(k+1)$-transitive. ∎

Note that for the k-transitivity as defined in [Azo86], [DMR08] the implication in the lemma is reversed. For a subspace $S \subset \mathcal{B}(H)$ we call the smallest positive integer k for which S is (weak) k-transitive its transitivity number. For a quantum channel C and associated operator system $\mathcal{S}_C$ the transitivity number of the latter will be denoted by t_C.

Lemma 2. *For any quantum channel $z_C \leqslant t_C$.*

Proof: Let $t_C = k$. We have to show that we cannot have more than k $\mathcal{S}_C$-orthogonal vectors in H. Suppose $\alpha_1, \ldots, \alpha_{k+1} \in H$ are mutually $\mathcal{S}_C$-orthogonal. Then these vectors must be S-independent. For if, say, $\alpha_{k+1} = F_1\alpha_1 + \cdots + F_k\alpha_k,\ F_i \in \mathcal{S}_C$ then taking the scalar product of both sides with α_{k+1}, $\mathcal{S}_C$-orthogonality implies that $\alpha_{k+1} = 0$. But as $\mathcal{S}_C$ is k-transitive there is some $A \in M_k(\mathcal{S}_C)$ such that $A \begin{pmatrix} \alpha_1 & \ldots & \alpha_k \end{pmatrix}^T = \begin{pmatrix} \alpha_{k+1} & 0 & \ldots & 0 \end{pmatrix}^T$ implying S-*dependence*. Hence we cannot have more than k non-zero $\mathcal{S}_C$-orthogonal vectors. ∎

We have an upper bound on the zero-error rank of a channel. Note that we can define t_C as the cardinality of the largest $\mathcal{S}_C$-independent set. The above inequality can be strict. Before giving a lower bound we state a simple but useful lemma.

Lemma 3. *Let $\mathcal{S}$ be an operator system on a finite-dimensional space H. If $K \subset H$ is an $\mathcal{S}$ invariant subspace then its orthogonal complement $K^\perp$ is also $\mathcal{S}$ invariant.*

From the definition of z_C it is at least 1. It is also easy to state the condition for C to have at least two non-zero $\mathcal{S}_C$-orthogonal vectors. We reserve the symbol $\subset$ for proper subsets. If there is possibility of equality we will use $\subseteq$. For a set X we use $|X|$ to denote its cardinality. The following lemma is straightforward.

Lemma 4. *$z_C \geqslant 2$ if and only if $\mathcal{S}$ is not transitive.*

For an operator system $\mathcal{S}$ we define $\mathcal{S}^2$ to be the linear span of products of elements of $\mathcal{S}$. Since the identity belongs to $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{S}^2$ and the latter is also an operator system. We can similarly define the sequence of operator systems

$$\mathcal{S} \subseteq \mathcal{S}^2 \subseteq \cdots \subseteq \mathcal{S}^k \subseteq \cdots$$

Since the dimension is finite the sequence must end for some $k \leqslant n^2$, that is $\mathcal{S}^k = \mathcal{S}^{k+1} = \cdots$. Then $\mathcal{S}^k$ is a self-adjoint subalgebra of $\mathcal{B}(H)$. We now give a *lower bound* for z_C. For $\alpha \in H$ define the sequence of subspaces

$$\mathcal{S}[\alpha] = \{\mathcal{S}\alpha, \mathcal{S}^2\alpha, \ldots, \mathcal{S}^k\alpha, \ldots, \} \tag{5}$$

We consider only the distinct sets $\mathcal{S}^k\alpha$ in $\mathcal{S}[\alpha]$ of course. Then $|\mathcal{S}[\alpha]| \leqslant n^2$.

Lemma 5. *For a quantum channel C and the associated operator system $\mathcal{S}$*

$$\lfloor \max_\alpha |\mathcal{S}[\alpha]|/2 + 1 \rfloor \leqslant z_C$$

Proof: Let α be a vector for which $\mathcal{S}[\alpha] = m$ is maximum. Then we must have

$$\{\alpha\} \subset \mathcal{S}\alpha \subset \mathcal{S}^2\alpha \subset \ldots \subset \mathcal{S}^m\alpha$$

By our convention each is a proper subset. The last term in the series must satisfy $\mathcal{S}^m\alpha = \mathcal{S}^{m+1}\alpha$ or $S^m\alpha = H$. Put $\mathcal{S}^0\alpha = \{\alpha\}$. Let $0 \leqslant k < m$ be an integer. Then there exist $\beta_k \in \mathcal{S}^{k+1}\alpha - \mathcal{S}^k\alpha$. Let $\beta_k = \alpha_k + \gamma_{k+1}$ where $\alpha_k \in \mathcal{S}^k\alpha$ and $\gamma_{k+1} \in (\mathcal{S}^k\alpha)^\perp$. Then, $\gamma_{k+1} = \beta_k - \alpha_k \in \mathcal{S}^{k+1}\alpha$. Let $\gamma_0 = \alpha$. Then $\gamma_0, \gamma_2, \gamma_4, \ldots, \gamma_{2[m/2]}$ is $\mathcal{S}$-orthogonal. ∎

Call the number m above the cyclic number of the operator system acting on H. Suppose H has a decomposition

$$H = H_1 \oplus H_2 \oplus \cdots H_k$$

with $\mathcal{S}$-invariant subspaces H_i. Let m_i be cyclic number of $\mathcal{S}$ acting on H_i. Then

$$\sum_i \lfloor m_i/2 \rfloor + k \leqslant z_C \tag{6}$$

We now analyze the structure of $\mathcal{S}$-orthogonal sets. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be an $\mathcal{S}$-orthogonal set. For $1 \leqslant i \leqslant k$ let

$$T_i = (\mathcal{S}\alpha_1 \oplus \mathcal{S}\alpha_2 \oplus \cdots \oplus \mathcal{S}\alpha_k)^\perp$$

where the sum on the right does *not* contain $\mathcal{S}\alpha_i$. Further, let

$$N = \left(\bigoplus_{i=1}^{k} \mathcal{S}\alpha_i\right)^\perp$$

Define subspaces

$$M_i = \{\gamma \in \mathcal{S}\alpha_i \cap T_i : \mathcal{S}\gamma \subset \mathcal{S}\alpha_i \oplus N\}$$

Since $\alpha_i \in M_i$ they are nonempty. Moreover for any $\gamma_i \in M_i$, $\gamma_j \in M_j$ and $F \in \mathcal{S}$ we have

$$\langle\gamma_i|F|\gamma_j\rangle = 0,\ i \neq j$$

This follows from the definition of M_i and the fact that $\{\alpha_i\}$ is an $\mathcal{S}$-orthogonal set. We can now state the basic structure theorem of $\mathcal{S}$-orthogonal sets. In the following by a projection P we mean a hermitian idempotent: $P^\dagger = P$ and $P^2 = P$.

Theorem 1. *Suppose a quantum channel C has an associated operator system $\mathcal{S}$. Let $A = \{\alpha_1, \ldots, \alpha_k\}$ be a set of mutually orthogonal vectors. Then A is $\mathcal{S}$-orthogonal if and only if the following condition holds. There exist mutually orthogonal subspaces $M_1, \ldots, M_k$ of H such that*

$$\alpha_i \in M_i \text{ and } \mathcal{S}M_i \subset M_i \oplus M^\perp \text{ where } M = \bigoplus_i M_i \tag{7}$$

Conversely, let P a projection and set $K = PH$. Consider the operator system

$$\mathcal{S}_P = P\mathcal{S}P \equiv \{PFP : F \in \mathcal{S}\}$$

in $B(K)$. Let $\mathscr{A}(\mathcal{S}_P)$ be the subalgebra of $B(K)$ generated by $\mathcal{S}_P$. Let $C(\mathscr{A}(\mathcal{S}_P))$ denote the commutant (operators in $B(K)$ that commute with all $X \in \mathscr{A}(\mathcal{S}_P)$) of the algebra $\mathscr{A}(\mathcal{S}_P)$. Then $\dim(C(\mathscr{A}(\mathcal{S}_P))) \leqslant z_C$ and equality holds if and only if either of the following equivalent (hence both) conditions hold.

1) $\dim(C(\mathscr{A}(\mathcal{S}_P)))$ *is maximal.*
2) $\mathcal{S}K = H$, $\mathcal{S}_P$ *acts transitively on each invariant and irreducible subspace of* $\mathscr{A}(\mathcal{S}_P)$ and

$$z_C = (\dim(C(\mathscr{A}(P\mathcal{S}P)))$$

Hence

$$z_C = \max(\dim(C(\mathscr{A}(P\mathcal{S}P))))$$

where the maximum is taken over all projections P on H and $P\mathcal{S}P$ is considered as an operator system on $\mathcal{B}(PH)$.

Proof: Suppose A is an $\mathcal{S}$-orthogonal set. The discussion preceding the theorem gives the required sets M_i. Let $\gamma_i \in M_i$ and $F \in \mathcal{S}$. Then $\langle\gamma_i|F|\gamma_j\rangle = 0$ for any $\gamma_j \in M_j$, $j \neq i$ implies that $F\gamma_i \in \mathcal{S}M_i \oplus M^\perp$. The converse is obvious. In fact, any any set $\{\gamma_1, \ldots, \gamma_k\}$ with $\gamma_i \in M_i$ is an $\mathcal{S}$-orthogonal set.

Next observe that for any projection P the space $P\mathcal{S}P$ contains hermitian conjugates of its elements. It is an operator system on the subspace $K = PH$ and the corresponding algebra generated $B_P = \mathscr{A}(P\mathcal{S}P)$ is a C^* subalgebra of $B(K)$. This implies that B_P is semisimple [Dav96] and the representation space K is completely reducible. We can see this directly as follows. Since ${B_P}^\dagger = B_P$ if X is a B_P invariant subspace $X^\perp$, the orthogonal complement of X in T is also B_P invariant. Start with an invariant subspace X_1 of smallest dimension. It must be irreducible. Then $K = K_1 \oplus K_1^\perp$. Repeat this process with $M_1^\perp$. We conclude that

$$K = K_1 \oplus K_2 \oplus \cdots \oplus K_r$$

for some positive integer r such that K_i are irreducible invariant subspaces. They are also orthogonal. Hence these subspaces correspond precisely to the subspaces M_j in (7). Choosing non-zero vectors $\alpha_i \in K_i$ we get an $\mathcal{S}$-orthogonal set. Moreover, the projections P_i onto the subspace K_i commute with the whole algebra. Since K_i are irreducible these generate the commutant (Schur lemma). Next, suppose that for a projection P the dimension of $C(\mathscr{A}(\mathcal{S}_P))$ is maximal and assume the decomposition into irreducible invariant subspaces as above. If $\mathcal{S}K \subset H$ then pick a nonzero vector $\beta \in (\mathcal{S}K)^\perp$. Then $\mathcal{S}\beta \cap K = 0$. Let $K' = K \oplus \mathbb{C}\beta$ and P' the projection onto K'. Since $P_iP' = P_iP = P_i$ we have $\dim(C(\mathscr{A}(P'\mathcal{S}P'))) \geqslant \dim(C(\mathscr{A}(\mathcal{S}_P))) + 1$. This contradicts maximality. To prove the second condition assume $\mathcal{S}_P$ is not transitive on K_1 (no loss of generality). There exist $\gamma \in K_1$ such that $\mathcal{S}_P\gamma \subset K_1$ choose γ' from the orthogonal complement of $\mathcal{S}_P\gamma$ in K_1. Pick arbitrary nonzero vectors $\alpha_i \in K_i$, $i = 2, \ldots, r$. Then $D = \{\gamma, \gamma', \alpha_2, \alpha_3, \ldots, \alpha_k\}$ is an $\mathcal{S}$-orthogonal set. We can now construct a new set of K_i corresponding to D along with new projection P' such that $\dim(C(\mathscr{A}(P'\mathcal{S}P'))) > \dim(C(\mathscr{A}(P\mathcal{S}P)))$, contradicting maximality. It follows that for any such P $\dim(C(\mathscr{A}(P\mathcal{S}P))) = z_C$. ∎

Corollary 1. *Suppose the error generators $\{E_i\}, {E_i}^\dagger\}$ form a group $\mathcal{G}$. Then the underlying Hilbert space H carries a completely reducible representation of $\mathcal{G}$. Let k be the number of irreducible components. Then $z_C = k$.*

Proof: Let P be a projection as in the theorem and $M = PH$. Let

$$H = H_1 \oplus H_2 \oplus \cdots \oplus H_k \tag{8}$$

be the decomposition of H into irreducible $\mathcal{G}$ invariant subspaces. Such a decomposition exists since $\mathcal{G}$ is finite group. We

will actually show this next proving a bit more. By assumption $E_i \in \mathcal{G}$ implies ${E_i}^\dagger \in \mathcal{G}$. Let $K \subset H$ be a $\mathcal{G}$ invariant subspace and $K^\perp$ its orthogonal complement. For $\alpha \in K$ and $\beta \in K^\perp$ we have

$$\langle \alpha | E_i | \beta \rangle = \overline{\langle \beta | {E_i}^\dagger | \alpha \rangle} = 0$$

Hence, $K^\perp$ is also $\mathcal{G}$ invariant. Since H is finite dimensional we conclude by induction that the decomposition (8) exists and the irreducible subspaces are mutually *orthogonal.* Then

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k \text{ where } M_i = M \cap H_i$$

Since H_i are $\mathcal{G}$-invariant subspaces they are invariant under the group algebra generated by $\{E_i\}, {E_i}^\dagger\}$.This is identical to the operator system (now algebra) $\mathcal{S}$. Then irreducibility of H_i implies that it is $\mathcal{S}$-transitive. Hence, by Lemma 4 there cannot be two $\mathcal{S}$-orthogonal vectors in M_i and the proof is complete. ∎

Note that we cannot take it for granted that for an arbitrary finite group the operators representing it are unitary with respect to *any* given scalar product in the representation space. Further, note that if H is an irreducible representation space then we have $z_C = 1$. That is why representation on higher-dimensional product space, that is coding, is necessary.

A. Examples

Let $H = \bigotimes^n \mathbb{C}^d$, the n "qudit" space of dimension $N = d^n$. We consider arbitrary k-qudit errors. Then a basis for the error operators is

$$E_{i_1 i_2 \cdots i_k} = A_1 \otimes A_2 \otimes \cdots \otimes A_n \tag{9}$$

where $A_j \in \mathcal{B}$, $\mathcal{B}$ any basis of a subspace of $M_d(\mathbb{C})$, if $j \in \{i_1, i_2 \ldots, i_k\}$ otherwise $A_j = I_d$ (unit matrix of order d). First, suppose that $d = 2$ (qubits) and $\mathcal{B} = \{X, I_2\}$ where X is the bit-flip let $k = 1$. This is the classical case of one-bit error. It is an elementary fact that we need at least 3 bits to correct these errors and in that case any code has two words. A bit of algebra shows however that $z_C = 3$ for $n = 3$. However, if $\mathcal{B} = M_2(\mathbb{C})$ then $z_C = 2$. One can similarly show for $n = 4, 5$ (after some tedious calculation) that for arbitrary single qubit errors $z_C = A(n, 3)$. Here $A(n, j)$ denotes the number of *classical binary* code words of length n and Hamming distance at least j [MS77]. We generalize this to the following.

Conjecture. *Let $H = \bigotimes^n \mathbb{C}^d$ and the error operators for the channel C are given by* (9) *where A_j constitute a basis of $M_d(\mathbb{C})$. Then*

$$z_C = A_d(n, 2k + 1)$$

It is easy to see that $A_d(n, 2k + 1) \leqslant z_C$. We also suspect that in this case $z_C = t_C$. The proof of these facts is rather involved even in the case $d = 2$ and $n = 5$. Note however that classical lower bounds on $A_d(n, 2k + 1) \leqslant z_C$ like Gilbert-Varshamov bound [MS77] can be derived from Theorem 1—we simply have to find the appropriate projections and the dimension of the commutants of the corresponding algebra.

III. Quantum error correction

In this section we investigate error *correction* capabilities of quantum channels. The zero-error subspaces provide us with sets of orthogonal vectors which can be distinguished after passage through the channel. In order to *recover* the original states we have to apply correcting operations. We seek conditions under which this is possible. Let us first rephrase the condition in equation (7) of Theorem 1. Using the notation of the theorem let $M \subset H$ be a subspace and P the associated orthogonal projection. Then M contains a zero-error subspace of a quantum channel C if and only if there are orthogonal projection operators P_i ($P_i P_j = \delta_{ij} P_i$) such that

$$P = \bigoplus_{i=1}^{k} P_i \text{ and } PSP = \sum_{i=1}^{k} P_i S P_i \tag{10}$$

For error correction we need to reconstruct the original state from the channel output. First we select a set of orthogonal vectors as our input alphabet. This is equivalent to taking P_i as one-dimensional projections. We simply choose a non-zero vector from each $M_i = P_i H$. We assume below that each P_i is a one-dimensional projection. Then PH is a zero-error subspace and equation (10) is equivalent to

$$P {E_i}^\dagger E_j P = \sum_k c_{ij}^k P_k \tag{11}$$

where for fixed k, c_{ij}^k is a hermitian matrix. This implies $P_a E_i E_j P_b = 0$ for $a \neq b$. By definition a subspace $N \subset H$ is a quantum code if the channel map Φ_C is invertible on $\mathcal{B}(N)$. A necessary and sufficient condition (the Knill-Laflamme condition) for N to be a code is that for the projection P_N on N

$$P_N {E_i}^\dagger E_j P_N = s_{ij} P_N \tag{12}$$

where s_{ij} is a hermitian matrix [NC01]. Comparing this with equation (11) we get the following.

Proposition 1. *A zero-error subspace M of dimension k with projection P admits a quantum code of dimension k if and only if the decomposition $P = \oplus_i P_i$ in equation* (11) *has the property that the coefficients c_{ij}^k are independent of k.*

Even in the case where the zero-error subspace is *not* a quantum code we may find a maximal subspace $N \subset M$ that *is* a code. We simply take the direct sum of a maximal number of projection operators P_i that satisfy the condition in the theorem. We illustrate this method by building the Shor code [Sho95]. The goal is to encode logical qubits in a larger space using multiple qubits. We assume the independent error model so that the each qubit is affected independently. This implies that the error operators act as tensor product of single qubit errors. We want to correct arbitrary errors. So the single qubit error operators actually generate M_2, the set of 2×2 matrices, as a complex vector space. Let us look at the problem from a more general perspective. Consider the operator system $S \subset M_d$ acting on a d-dimensional Hilbert space H_d. Consider the operators

$$E_k^i = I_d \otimes \cdots \otimes I_d \otimes A_k \otimes I_d \otimes \cdots \otimes I_d \ (r \text{ factors})$$

where the ith factor A_k constitute a basis of M_d and I_d the identity matrix of order d. The operators E_k^i act on $\otimes^r H_d$ as single "qudit" errors. Then the operator system S is generated by

$$E_{kl}^{ij} = I_d \otimes \cdots \otimes I_d \otimes A_k \otimes \cdots \otimes A_l{}^\dagger \otimes \cdots \otimes I_d$$

where the generators A_k and $A_l{}^\dagger$ are in the ith and jth place respectively. We allow the possibility $i = j$. Suppose $r = 2$. Suppose the generators A_k generate the full matrix algebra M_d. Then, the operators $A_k \otimes A_l{}^\dagger$ generate M_{d^2} and the transitivity of the latter implies that there are no non-trivial zero-error subspaces. So the minimum number of factors in the tensor product space required to have non-trivial zero-error subspace for single qudit errors is 3. Let $\{\alpha_i\}$ be a basis for H_d and consider the vectors

$$\Psi_i \equiv \alpha_i \otimes \alpha_i \otimes \alpha_i,\ i = 1, \ldots, d$$

The vectors $\{\Psi_i\}$ span a zero-error subspace for single qudit errors (Ψ_i and Ψ_j are S-orthogonal for $i \neq j$). There are many such collection of product vectors which are mutually S-orthogonal but they all have cardinality d. Now the condition on theorem 1 implies that for a quantum code we must have

$$\left\langle \Psi_i \middle| E_{rs}^{kl} \middle| \Phi_i \right\rangle = \left\langle \Psi_j \middle| E_{rs}^{kl} \middle| \Psi_j \right\rangle \ \forall i, j \tag{13}$$

suppose now that the space H_d itself is a product space, specifically, n-qubit space (dimension 2^n). Then reasoning as above for *single* qubit errors now we see that to satisfy (13) n must be greater than 2. For example, the orthogonal vectors

$$|000\rangle + e^{ic} |111\rangle \text{ and } |000\rangle - e^{ic} |111\rangle$$

where c is real number, satisfy the condition. Setting $c = 0$ gives the Shor code. In general, given $\mathcal{S}$-orthogonal states we can generate quantum codes by taking tensor products in the independent and bounded error models.

A. Noiseless subsystems

Informally, a noiseless subsystem is segment of $\mathcal{B}(H)$ that is unaffected by the operator Φ_C. More precisely, if there is some decomposition of the system Hilbert space $H = H_A \otimes H_B \oplus K$ such that for operators of the form $T_A \otimes T_B \in \mathcal{B}(H_A) \otimes \mathcal{B}(H_B)$ we have

$$\Phi_C(T_A \otimes T_B) = T'_A \otimes T_B,\ T'_A \in \mathcal{B}(H_A) \tag{14}$$

then we call B a noiseless subsystem. A necessary and sufficient condition for the existence of a such a subsystem is that the subspace $H_1 = H_A \otimes H_B$ be an invariant subspace of the algebra $\mathcal{A}$ generated by the error operators E_a and $E_a{}^\dagger$ is a subalgebra of $\mathcal{B}(H_A) \otimes I_B$ (when restricted to H_1). We say that B is a noiseless subsystem. It is easy to see that H_1 is a zero-error subspace. In general we have the following.

Theorem 2. *Let $\mathcal{E} = \{E_a, I : a = 1, 2, \ldots, \}$, be the set consisting of the error operators and the identity. Let S be the operator system generated by $\{FF^\dagger : F, G \in \mathcal{E}\}$. Then the system Hilbert space H has a noiseless subsystem if and only if the following hold. There is an S-invariant subspace $H_1 = H_A \otimes H_B$ and a basis $\{\beta_1, \ldots, \beta_k\}$ of H_B such that for any $\alpha_1, \ldots, \alpha_k \in H_A$ the vectors $\alpha_i \otimes \beta_i$ are S-orthogonal.*

Proof: The necessity part follows from the fact that $E_a|_{\mathcal{A}} \in \mathcal{B}(H_A) \otimes I_B$. Now suppose that the condition stated in theorem holds for some basis $\{\beta_1, \ldots, \beta_k\}$ of H_B. Let $\{\alpha_i : i = 1, \ldots, r\}$ be a basis for H_A. By hypothesis $\{\alpha_1 \otimes \beta_1, \ldots, \alpha_1 \otimes \beta_k\}$ is an S-orthogonal set. The generators $E_a \in S$. The invariance of H_1 for S then implies

$$E_a(\alpha_1 \otimes \beta_i) = \sum c_{jl}^{a1i} \alpha_j \otimes \beta_l = \sum \gamma_l^a \otimes \beta_l,\ \gamma_l^a = \sum_m c_{ml}^{a1i} \alpha_m$$

$\left\langle \alpha_1 \otimes \beta_j \middle| E_a \middle| \alpha_1 \otimes \beta_i \right\rangle = 0$ for $i \neq j$ by S-orthogonality. This implies that that coefficients $c_{1j}^{a1i} = 0$ for all $j \neq i$. Now let $2 \leqslant m \leqslant r$ be an integer. The set of vectors $\{\alpha_m \otimes \beta_j : j \neq i \text{ and } 1 \leqslant j \leqslant k\}$ is an S-orthogonal set. Arguing as above we conclude that $c_{mj}^{a1i} = 0$ for all m and all $j \neq i$. Hence $E_a(\alpha_1 \otimes \beta_i) = \gamma_1 \otimes \beta_i$. Replacing the index 1 by any other in the appropriate range we infer that

$$E_a(\alpha_m \otimes \beta_i) = \gamma_m^a \otimes \beta_i = \phi(E_a)\alpha_m \otimes \beta_i$$

where $\phi(E_a) \in \mathcal{B}(H_A)$. We conclude that $E_a|_{H_1} \in \mathcal{B}(H_A) \otimes I_B$. From the discussion preceding the theorem B is a noiseless subsystem. ∎

Although in the theorem we required the apparently weaker condition of S-orthogonality with respect to a *single* basis $\{\beta_i\}$ in the space H_B it is then true for any basis. This provides us with a method for searching for noiseless subsystems within zero-error subspaces.

The zero-error subspaces of a quantum or classical channel is a fascinating concept. One can then define an asymptotic quantities like the zero-error capacity and entanglement assisted capacity [DSW10]. In this work we focused on the subspaces themselves and their close connections with quantum and classical coding theory. This connection is most clearly expressed through operator theoretic concepts.

REFERENCES

[Azo86] E. A. Azoff. On finite rank operators and preannihilators. *Mem. Amer. Math. Soc.*, 64(357), 1986.

[Dav96] K. R. Davidson. *C*-Algebras by example*. AMS, 1996.

[DMR08] K. R. Davidson, L. E. Marcoux, and H. Radjavi. Transitive spaces of operators. *Integr. equ. oper. theory*, 61:187, 2008.

[DSW10] R. Duan, S. Severini, and A. Winter. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz ϑ function. arXiv:1002.2514v2 [quant-ph], 2010.

[KLPL06] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator quantum error correction. *Quant. Inf. and Comp*, 6:383–399, 2006.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland, 1977.

[NC01] M. A. Nielsen and I. L. Chuang. *Quantum computation and information*. CUP, 2001.

[Pau03] V. Paulsen. *Completely bounded maps and operator algebras*. CUP, 2003.

[PB10] M. K. Patra and S. L. Braunstein. An algebraic approach to information theory. In *IEEE Int. Symp. Inf. Th. (ISIT 2010)*, pages 2708 – 2712, 2010.

[Sha56] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Trans. Inform. Theory*, IT-2(3):8–19, 1956.

[Sho95] P. W. Shor. Sceme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493, 1995.