Operator approach to quantum error correction

Raymond Nung-Sing Sze
Department of Applied Mathematics, The Hong Kong Polytechnic University
Hong Kong, China
(raymond.sze@inet.polyu.edu.hk)

1 Operator approach to quantum error correction

The idea of quantum error correction is developed in quantum computing to protect quantum information from errors due to decoherence and other quantum noise during transmitting information in quantum channel. During the mid 1990s, Shor [21] and Steane [22] suggested examples on how data could be redundantly encoded in the states of a quantum system, and how the redundancy could be used to protect the data. Then this research topic took flight in a short period of time by many researchers [1, 2, 3, 10, 11, 12, 20, 22] and their references, and is still under rapid development.

Mathematically, given a finite dimensional complex Hilbert space $\mathcal{H}$ (usually identified as $\mathbb{C}^n$), a quantum channel can be viewed as a trace preserving completely positive linear map $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ with the operator sum representation

$$\Phi(\rho) \mapsto \sum_{j=1}^{r} E_j \, \rho \, E_j^\dagger \quad \text{with} \quad \sum_{j=1}^{r} E_j^\dagger E_j = I, \tag{1}$$

see [4]. In the context of quantum error correction, the matrices $E_1, \ldots, E_r$ in (1) are known as the error operators associated with the channel Φ.

Example 1.1 Consider two quantum channels Φ and Ψ acting on a single qubit with operator sum representations $\Phi(\rho) = \sum_{j=1}^{2} E_j \rho E_j^\dagger$ and $\Psi(\rho) = \sum_{j=1}^{2} F_j \rho F_j^\dagger$, respectively, where

$$E_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad F_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{and} \quad F_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Notice that $F_1 = (E_1 + E_2)/\sqrt{2}$ and $F_2 = (E_1 - E_2)/\sqrt{2}$. Thus, for any $\rho \in M_2$,

$$\Psi(A) = \frac{1}{2}(E_1 + E_2)\rho(E_1 + E_2)^\dagger + \frac{1}{2}(E_1 - E_2)\rho(E_1 - E_2)^\dagger = E_1 \rho E_1^\dagger + E_2 \rho E_2^\dagger = \Phi(\rho).$$

From the above example, one can see that the sum representation for a quantum channel is *not unique*.

Theorem 1.2 *Suppose*

$$\Phi(\rho) = \sum_{j=1}^{r} E_j \rho E_j^\dagger \quad \text{and} \quad \Psi(\rho) = \sum_{k=1}^{s} F_j \rho F_j^\dagger$$

are two quantum channels. By adding zero operators, if necessary, one can assume that $r = s$. Then $\Phi = \Psi$ if and only if there exists a $r \times r$ unitary matrix $U = [u_{ij}]$ such that

$$E_i = \sum_{j=1}^{r} u_{ij} F_j \quad \text{for all} \quad i = 1, \ldots, r.$$

Proof of the theorem can be found in [20, Theorem 8.2].

1.1 Quantum error correcting code

Definition 1.3 Let $\mathcal{V}$ be a subspace of $\mathcal{H}$ and $P_\mathcal{V}$ the orthogonal projection of $\mathcal{H}$ onto $\mathcal{V}$. Then $\mathcal{V}$ is a **quantum error correcting code (QECC)** for a quantum channel Φ on $B(\mathcal{H})$ if there exists a quantum channel (trace preserving completely positive linear map) $\Psi : B(\mathcal{H}) \to B(\mathcal{H})$ such that

$$\Psi \circ \Phi(\rho) = \rho \quad \text{for all} \quad \rho \in B(\mathcal{H}) \text{ with } \rho = P_\mathcal{V} \rho P_\mathcal{V}. \tag{2}$$

Such map Ψ is called a recovery channel of Φ.

Remark 1.4 If we identify $\mathcal{H}$ with $\mathbb{C}^n$ and U is an $n \times n$ unitary matrix with columns $|u_1\rangle, \ldots, |u_n\rangle$ so that the first k states $|u_1\rangle, \ldots, |u_k\rangle$ form a basis for $\mathcal{V}$, where $k = \dim \mathcal{V}$, then the equation (2) can be restated as

$$\Psi \circ \Phi \left(U \begin{bmatrix} \tilde{\rho} & 0 \\ 0 & 0 \end{bmatrix} U^\dagger \right) = U \begin{bmatrix} \tilde{\rho} & 0 \\ 0 & 0 \end{bmatrix} U^\dagger \quad \text{for all} \quad \tilde{\rho} \in M_k.$$

Knill and Laflamme gave a necessary and sufficient condition for the existence of a quantum error correcting code; see [12].

Theorem 1.5 *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ be a quantum channel of the form (1). Suppose $\mathcal{V}$ is a subspace of $\mathcal{H}$ and $P_\mathcal{V}$ is the orthogonal projection with $\mathcal{V}$ as the range space. Then the following statements are equivalent.*

(a) *$\mathcal{V}$ is a quantum error correcting code for Φ.*

(b) *$P_\mathcal{V} E_i^\dagger E_j P_\mathcal{V} = \lambda_{ij} P_\mathcal{V}$ for some complex numbers λ_{ij} for $1 \le i, j \le r$.*

Proof of Theorem 1.5. The proof presented here is based on [20, Section 10.3].

Suppose the condition (b) holds and for notation simplicity write $P = P_\mathcal{V}$. Let $\Lambda = [\lambda_{ij}]$ and $q = \operatorname{rank} \Lambda$. Then Λ is a $r \times r$ Hermitian matrix. By Theorem 1.2, one may assume that Λ is a diagonal matrix with positive diagonal entries $\lambda_{11}, \ldots, \lambda_{qq}$ and zero elsewhere. (Exercise!)

Notice that $PE_i^\dagger E_j P = \lambda_{ij} P$ for all $1 \le i, j \le r$. By polar decomposition, there is a unitary U_k such that

$$E_k P = U_k (P E_k^\dagger E_k P)^{\frac{1}{2}} = \sqrt{\lambda_{kk}}\, U_k P.$$

Let $P_k = U_k P U_k^\dagger = E_k P U_k^\dagger / \sqrt{\lambda_{kk}}$ for $k = 1, \ldots, q$. Then for any $1 \le k, \ell \le q$,

$$P_k^\dagger P_\ell = \frac{1}{\sqrt{\lambda_{kk}\lambda_{\ell\ell}}} U_k P E_k^\dagger E_\ell P U_\ell^\dagger = \frac{\lambda_{k\ell}}{\sqrt{\lambda_{kk}\lambda_{\ell\ell}}} U_k P U_\ell^\dagger = \begin{cases} U_k P U_k^\dagger & k = \ell, \\ 0 & k \neq \ell. \end{cases}$$

Thus, the projections $P_1, \ldots, P_q$ are pairwise orthogonal. Let $P_{q+1} = I - \sum_{k=1}^q P_k$ and $U_{q+1} = I$. Notice that $P_{q+1}^2 = P_{q+1}$ and $P_{q+1}^\dagger P_j = 0$ for all $1 \le j \le q$. Now define the recovery channel $\Psi : B(\mathcal{H}) \to B(\mathcal{H})$ by

$$\Psi(\rho) = \sum_{k=1}^{q+1} U_k^\dagger P_k \rho P_k U_k.$$

Clearly, $\sum_{k=1}^{q+1} P_k U_k U_k^\dagger P_k = \sum_{k=1}^{q+1} P_k = I$ and hence Ψ is trace preserving. Now for any ρ with $\rho = P\rho P$, as $E_k P = 0$ for all $k > q$,

$$\phi(\rho) = \sum_{k=1}^{r} E_k P \rho P E_k^\dagger = \sum_{k=1}^{q} E_k P \rho P E_k^\dagger = \sum_{k=1}^{q} \lambda_{kk} P_k U_k \rho U_k^\dagger P_k,$$

and so

$$\Psi \circ \Phi(\rho) = \sum_{\ell=1}^{q+1} \sum_{k=1}^{q} \lambda_{kk} U_\ell^\dagger P_\ell P_k U_k \rho U_k^\dagger P_k P_\ell U_\ell = \sum_{k=1}^{q} \lambda_{kk} P \rho P = P\rho P = \rho.$$

Thus, $\mathcal{V}$ is a quantum error correcting code for Φ.

Conversely, suppose there is a recovery quantum channel $\Psi : B(\mathcal{H}) \to B(\mathcal{H})$ of the form $\Psi(\rho) = \sum_{k=1}^p R_k \rho R_k^\dagger$ such that $\Psi \circ \Phi(\rho) = \rho$ for all ρ with $\rho = P\rho P$. Then

$$\sum_{k=1}^{p} \sum_{j=1}^{r} R_k E_j P \rho P E_j^\dagger R_k^\dagger = P\rho P \quad \text{for all} \quad \rho \in B(\mathcal{H}).$$

By Theorem 1.2, there are scalars $c_{jk} \in \mathbb{C}$ such that

$$R_k E_j P = c_{jk} P \quad \text{for all} \quad 1 \le j \le r,\ 1 \le k \le p.$$

Notice that $\sum_{k=1}^p R_k^\dagger R_k = I$. Thus for any $1 \le i, j \le r$,

$$P E_i^\dagger E_j P = \sum_{k=1}^{p} P E_i^\dagger R_k^\dagger R_k E_j P = \sum_{k=1}^{p} \overline{c}_{ik} c_{jk} P.$$

Then the condition (b) holds. □

Remark 1.6 Several remarks on quantum error correcting code.

1. A quantum error correcting code is said to be a **degenerate code** if the $r \times r$ Hermitian matrix $\Lambda = [\lambda_{ij}]$, defined in the proof of Theorem 1.5, is singular; otherwise it is called an **non-degenerate code**.

2. Suppose U is the $n \times n$ unitary matrix given in Remark 1.4. Then condition (b) of Theorem 1.5 is equivalent to

$$U^\dagger E_i^\dagger E_j U = \begin{bmatrix} \lambda_{ij} I_k & * \\ * & * \end{bmatrix} \quad \text{for all} \quad 1 \le i, j \le r.$$

   This will lead to the discussion of joint higher rank numerical range defined in the next section.

3. The proof of Theorem 1.5 is constructive and provides a procedure for constructing a recovery channel Ψ of Φ. However, the recovery channel Ψ may be hard to implement as the construction involves projection operators.

Example 1.7 Consider the three-qubit bit-flip channel $\Phi : M_8 \to M_8$ defined by

$$\Phi(\rho) = \sum_{j=0}^{3} X_j \rho X_j^\dagger,$$

with error operators

$$X_0 = \sqrt{p_0}\, I_2 \otimes I_2 \otimes I_2, \quad X_1 = \sqrt{p_1}\, \sigma_x \otimes I_2 \otimes I_2, \quad X_2 = \sqrt{p_2}\, I_2 \otimes \sigma_x \otimes I_2, \quad \text{and} \quad X_3 = \sqrt{p_3}\, I_2 \otimes I_2 \otimes \sigma_x,$$

where $\sum_{j=0}^{3} p_j = 1$. Then $\mathcal{V} = \text{span}\{|000\rangle, |111\rangle\}$ is a QECC for Φ. The recovery channel is given by

$$\Psi(\rho) = \sum_{j=0}^{3} P X_j^\dagger \rho X_j P \rho P \rho P + (I - P)\rho(I - P) \quad \text{with} \quad P = |000\rangle\langle 000| + |111\rangle\langle 111| = E_{11} + E_{88}.$$

Exercise

1. Complete the first part of the proof in Theorem 1.5.

2. Verify that $\mathcal{V}$ is QECC for Φ in Example 1.7. Also show that Ψ is a corresponding recovery channel.

1.2 Decoherence free subspace and Noiseless subsystem

Definition 1.8 A subspace $\mathcal{V}$ of $\mathcal{H}$ is said to be a **decoherence free subspace (DFS)** for a quantum channel Φ on $B(\mathcal{H})$ if

$$\Phi(\rho) = \rho \quad \text{for all} \quad \rho \in B(\mathcal{H}) \text{ with } \rho = P_\mathcal{V} \rho P_\mathcal{V}, \tag{3}$$

where $P_\mathcal{V}$ is the orthogonal projection of $\mathcal{H}$ onto $\mathcal{V}$.

Remark 1.9 Notice that a decoherence free subspace is a QECC with identity map as the recovery channel. In general, any QECC for a quantum channel Φ is a decoherence free subspace of the channel $\Psi \circ \Phi$. Different from the quantum error correcting code, the method of decherence free subspace is a passive error correction scheme. Data is stored in a special subspace so that it will not be affected by noise. However, the disadvantage of this scheme is that such decoherence free subspace may not exist.

Definition 1.10 A subsystem $\mathcal{H}^B$ is said to be a **noiseless subsystem (NS)** for a quantum channel Φ on $B(\mathcal{H})$ if there are a co-subsystem $\mathcal{H}^A$ and a subspace $\mathcal{K}$ so that $\mathcal{H}$ has a decomposition $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ in which for any $\rho^A \in B(\mathcal{H}^A)$ and $\rho^B \in B(\mathcal{H}^B)$, there is $\sigma^A \in B(\mathcal{H}^A)$ such that

$$\Phi\left(\rho^A \otimes \rho^B\right) = \sigma^A \otimes \rho^B. \tag{4}$$

Remark 1.11 Some remarks on decoherence free subspace and noiseless subsystem.

1. Suppose U is a unitary matrix with columns $|u_1\rangle, \dots, |u_n\rangle$ so that $\{|u_1\rangle, \dots, |u_n\rangle\}$ is a basis of $\mathcal{H}$ corresponding to the decomposition $(\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ with $\dim \mathcal{H}^A = p$ and $\dim \mathcal{H}^B = k$. Then the equation (4) can be restated as follows.

   For any $\rho^A \in M_p$ and $\rho^B \in M_k$, there is a $\sigma^A \in M_p$ such that

$$\Phi\left(U \begin{bmatrix} \rho^A \otimes \rho^B & 0 \\ 0 & 0 \end{bmatrix} U^\dagger\right) = U \begin{bmatrix} \sigma^A \otimes \rho^B & 0 \\ 0 & 0 \end{bmatrix} U^\dagger.$$

2. Notice that a decoherence free subspace is indeed a special case of noiseless system, i.e., when $\dim \mathcal{H}^A = 1$. Following the same notations, the equation (3) can be restated as

$$\Phi\left(U \begin{bmatrix} \tilde{\rho} & 0 \\ 0 & 0 \end{bmatrix} U^\dagger\right) = U \begin{bmatrix} \tilde{\rho} & 0 \\ 0 & 0 \end{bmatrix} U^\dagger \quad \text{for all} \quad \tilde{\rho} \in M_k.$$

In the following, we provide a simple example for noiseless system, which is originally from [13].

Example 1.12 Consider the quantum channel $\Phi : M_4 \to M_4$ with error operators $E_1 = F_1 \otimes I_2$ and $E_2 = F_2 \otimes I_2$, where

$$F_1 = \begin{bmatrix} \sqrt{\alpha} & 0 \\ 0 & \sqrt{1-\alpha} \end{bmatrix} \quad \text{and} \quad F_2 = \begin{bmatrix} 0 & \sqrt{\alpha} \\ \sqrt{1-\alpha} & 0 \end{bmatrix},$$

for some $0 \le \alpha \le 1$. Decompose $\mathbb{C}^4 = \mathcal{H}^A \otimes \mathcal{H}^B$ with respect to the standard basis so that $\mathcal{H}^A = \mathcal{H}^B = \mathbb{C}^2$. Then for any $\rho^A \in B(\mathcal{H}^A)$ and $\rho^B \in B(\mathcal{H}^B)$,

$$\Phi(\rho^A \otimes \rho^B) = \left(F_1 \rho^A F_1^\dagger + F_2 \rho^A F_2^\dagger\right) \otimes \rho^B = \sigma^A \otimes \rho^B.$$

There are several equivalent definitions for noiseless subsystem, see the following proposition. The proof of the proposition can be found in [13].

Proposition 1.13 *Given a decomposition $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and a quantum channel Φ on $B(\mathcal{H})$. The following conditions are equivalent.*

(1) *$\mathcal{H}^B$ is a noiseless subsystem.*

(2) *For any $\rho^A \in B(\mathcal{H}^A)$ and $\rho^B \in B(\mathcal{H}^B)$, there is $\sigma^A \in B(\mathcal{H}^A)$ such that*

$$\Phi(\rho^A \otimes \rho^B) = \sigma^A \otimes \rho^B.$$

(3) *For any $\rho^B \in B(\mathcal{H}^B)$, there is $\sigma^A \in B(\mathcal{H}^A)$ such that*

$$\Phi(I_A \otimes \rho^B) = \sigma^A \otimes \rho^B.$$

(4) *For any $\rho^A \in B(\mathcal{H}^A)$ and $\rho^B \in B(\mathcal{H}^B)$,*

$$\mathrm{Tr}_A \left(P_{AB} \circ \Phi(\rho^A \otimes \rho^B) \right) = \rho^B,$$

where P_{AB} is the orthogonal projection of $\mathcal{H}$ onto $\mathcal{H}^A \otimes \mathcal{H}^B$.

To present a necessary and sufficient condition for the existence of noiseless system, we need the following notations. Fixed orthonormal bases $\{|a_1\rangle, \ldots, |a_p\rangle\}$ and $\{|b_1\rangle, \ldots, |b_k\rangle\}$ for $\mathcal{H}^A$ and $\mathcal{H}^B$, respectively. Let

$$P_{ij} = |a_i\rangle\langle a_j| \otimes I_B \quad \text{for all} \quad 1 \le i, j \le p.$$

Notice that $P_{AB} = P_{11} + \cdots + P_{pp}$ is the orthogonal projection of $\mathcal{H}$ onto $\mathcal{H}^A \otimes \mathcal{H}^B$. The following result was proved in [13].

Theorem 1.14 *Given a decomposition $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and a quantum channel Φ on $B(\mathcal{H})$. Then $\mathcal{H}^B$ is a noiseless subsystem for Φ if and only if*

$$E_s P_{AB} = P_{AB} E_s P_{AB} \quad \textit{for all} \quad 1 \le s \le r, \tag{5}$$

and there are scalars $\lambda_{i,j,s} \in \mathbb{C}$ such that

$$P_{ii} E_s P_{jj} = \lambda_{i,j,s} P_{ij} \quad \textit{for all} \quad 1 \le i, j \le p, \ 1 \le s \le r. \tag{6}$$

Remark 1.15 Let U be a unitary matrix with states $|a_1\rangle \otimes |b_1\rangle, |a_1\rangle \otimes |b_2\rangle, \ldots, |a_p\rangle \otimes |b_k\rangle$ as the first pk columns. Then equations (5) and (6) hold if and only if

$$U^\dagger E_s U = \begin{bmatrix} \Lambda^{(s)} \otimes I_B & * \\ 0 & * \end{bmatrix} \quad \text{with} \quad \Lambda^{(s)} = \left[\lambda_{i,j,s} \right] \quad \text{for all} \quad 1 \le s \le r.$$

Corollary 1.16 *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ be a quantum channel of the form (1). Then a subspace $\mathcal{V}$ of $\mathcal{H}$ is a decoherence free subspace for Φ if and only if there are scalars $\lambda_s \in \mathbb{C}$ such that*

$$E_s P_{\mathcal{V}} = \lambda_s P_{\mathcal{V}} \quad \textit{for all} \quad 1 \le s \le r.$$

Example 1.17 Consider the quantum channel $\Phi : M_4 \to M_4$ with error operators

$$E_1 = \begin{bmatrix} \sqrt{1-2\alpha} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \sqrt{1-2\alpha} \end{bmatrix} \quad \text{and} \quad E_2 = \begin{bmatrix} \sqrt{\alpha} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\alpha} \\ \sqrt{\alpha} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\alpha} \end{bmatrix}$$

for some $0 \le \alpha \le 1$. Let $U = E_{11} + E_{24} + E_{33} + E_{42}$. Then

$$U^\dagger E_1 U = \begin{bmatrix} \sqrt{1-2\alpha} & 0 \\ 0 & 1 \end{bmatrix} \otimes I_2 \quad \text{and} \quad U^\dagger E_2 U = \begin{bmatrix} \sqrt{\alpha} & 0 \\ \sqrt{\alpha} & 0 \end{bmatrix} \otimes I_2.$$

So for any $\rho^B \in M_2$,

$$\Phi\left(U(I_A \otimes \rho^B)U^\dagger\right) = U(\sigma^A \otimes \rho^B)U^\dagger \quad \text{where} \quad \sigma^A = \begin{bmatrix} 1-\alpha & \alpha \\ \alpha & 1+\alpha \end{bmatrix}.$$

Equivalently, $\mathcal{H}^B$ is a noiseless subsystem if one decompose $\mathcal{H}$ to $\mathcal{H}^A \otimes \mathcal{H}^B$, $\dim \mathcal{H}^A = \dim \mathcal{H}^B = 2$, with respect to the basis $\{|00\rangle, |11\rangle, |10\rangle, |01\rangle\}$.

Exercise Verify all the detail in Example 1.17. Also show that this channel Φ has a 2-dimensional decoherence free subspace.

1.3 QECC vs DFS

Suppose a quantum channel Φ on $B(\mathcal{H})$ has a quantum error correcting code $\mathcal{V}$. Although the subspace $\mathcal{V}$ may not necessarily be a decoherence free subspace, the behavior of Φ on $\mathcal{V}$ is indeed quite close to those on a decoherence free subspace. In fact, one can compose the quantum channel Φ with a unitary similarity transform so that the output state is a direct sum of zero operator and a tensor product of the decoded qubit state and an encoding ancilla state. The following idea was introduced in [14].

Theorem 1.18 *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{H})$ be a quantum channel of the form (1) with $n = \dim \mathcal{H}$. Suppose Φ has a k-dimensional quantum error correcting code $\mathcal{V}$ with orthogonal projection $P_{\mathcal{V}} = WW^\dagger$ with $W^\dagger W = I_k$. Then there is a unitary R and a positive definite $\sigma \in M_q$ with $q \le n/k$ such that*

$$\Phi\left(W\tilde{\rho}W^\dagger\right) = R \begin{bmatrix} \sigma \otimes \tilde{\rho} & 0 \\ 0 & 0 \end{bmatrix} R^\dagger \quad \text{for all} \quad \tilde{\rho} \in M_k.$$

In particular, if k divides n so that $B(\mathcal{H})$ can be regarded as $M_{n/k} \otimes M_k$, there is a positive semi-definite $\sigma \in M_{n/k}$ such that

$$\Phi\left(W\tilde{\rho}W^\dagger\right) = R(\sigma \otimes \tilde{\rho})R^\dagger \quad \text{for all} \quad \tilde{\rho} \in M_k,$$

and a recovery channel can be constructed as the map $\Psi : B(\mathcal{H}) \to B(\mathcal{H})$ defined by

$$\Psi(\rho) = W(\,\mathrm{Tr}_1(R^\dagger \rho R)\,)W^\dagger,$$

where Tr_1 stands for the partial trace over the encoding ancilla Hilbert space.

Proof of Theorem 1.18. Suppose the equivalent conditions in Theorem 1.5 hold. Let q be the rank of the $r \times r$ Hermitian matrix $\Lambda = [\lambda_{ij}]$. By a similar argument as in Theorem 1.5, we may assume that $PE_i^\dagger E_j P = \lambda_{ij} P$ for $1 \le i, j \le r$, where $\lambda_{ij} = 0$ for all i and j, except for $(i,j) = (1,1), (2,2), \ldots, (q,q)$.

Define $E = \begin{bmatrix} E_1 & E_2 & \cdots & E_q \end{bmatrix}$ and $\sigma = \operatorname{diag}(\lambda_{11}, \ldots, \lambda_{qq})$. Since $P = WW^\dagger$ with $W^\dagger W = I_k$, it follows that

$$W^\dagger E_i^\dagger E_j W = \lambda_{ij} I_k \qquad \text{and} \qquad (I_q \otimes W)^\dagger E^\dagger E (I_q \otimes W) = \sigma \otimes I_k.$$

Define an $n \times qk$ matrix

$$R_1 = E(I_q \otimes W)(\sigma^{-1/2} \otimes I_k).$$

Then $R_1^\dagger R_1 = I_{qk}$. Take an $n \times (n - qk)$ matrix R_2 such that $R = \begin{bmatrix} R_1 & R_2 \end{bmatrix}$ is unitary. Notice that

$$R^\dagger E(I_q \otimes W) = R^\dagger R_1 (\sigma^{1/2} \otimes I_k) = \begin{bmatrix} \sigma^{1/2} \otimes I_k \\ 0 \end{bmatrix}.$$

Now for any $\tilde\rho \in M_k$, let $\rho = W\tilde\rho W^\dagger$. Since $W^\dagger E_j^\dagger E_j W = \lambda_{jj} I_k = 0$ and hence $E_j W = 0$ for all $j > q$,

$$\Phi(\rho) = \sum_{j=1}^{r} E_j (W\tilde\rho W^\dagger) E_j^\dagger = \sum_{j=1}^{q} E_j (W\tilde\rho W^\dagger) E_j^\dagger = E(I_q \otimes (W\tilde\rho W^\dagger))E^\dagger.$$

It follows that

$$\begin{aligned} R^\dagger \Phi(\rho) R &= R^\dagger E (I_q \otimes W)(I_q \otimes \tilde\rho)(I_q \otimes W^\dagger) E^\dagger R \\ &= \begin{bmatrix} \sigma^{1/2} \otimes I_k \\ 0 \end{bmatrix} (I_q \otimes \tilde\rho) \begin{bmatrix} \sigma^{1/2} \otimes I_k & 0 \end{bmatrix} = \begin{bmatrix} \sigma \otimes \tilde\rho & 0 \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

The result follows. □

Remark 1.19 *If one extends W to a unitary matrix U, then the equation in Theorem 1.18 can be restated as*

$$\Phi\left(U \begin{bmatrix} E_{11} \otimes \tilde\rho & 0 \\ 0 & 0 \end{bmatrix} U^\dagger \right) = R \begin{bmatrix} \sigma \otimes \tilde\rho & 0 \\ 0 & 0 \end{bmatrix} R^\dagger \quad \textit{for all} \quad \tilde\rho \in M_k.$$

The two unitary matrices U and R can be regarded as different orthonormal bases of $\mathcal{H}$. Respect to these two different bases, Φ actually sends $E_{11} \otimes \tilde\rho$ to $\sigma \otimes \tilde\rho$. In some cases, U and R can be chosen to be the same unitary matrix. Then one can decompose $\mathcal{H}$ as $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and there exist a state $|a\rangle \in \mathcal{H}^A$ and $\sigma^A \in B(\mathcal{H}^A)$ such that

$$\Phi\left(|a\rangle\langle a| \otimes \rho^B \right) = \sigma^A \otimes \rho^B \quad \textit{for all} \quad \rho^B \in B(\mathcal{H}^B).$$

Example 1.20 We now revisit the same three-qubit bit-flip quantum channel in Example 1.7 to clarify Theorem 1.18. The corresponding quantum error correcting code is $\mathcal{V} = \text{span}\{|000\rangle, |111\rangle\}$ and the projection is

$$P = |000\rangle\langle 000| + |111\rangle\langle 111| = E_{11} + E_{88},$$

which is also written as $P = WW^\dagger$, where

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}^\dagger.$$

Evidently, $W^\dagger W = I_2$. A one-qubit state $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded with two encoding ancilla qubits as $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$. Let

$$\tilde{\rho} = |\psi_0\rangle\langle\psi_0| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}. \tag{7}$$

The encoded state is then

$$\rho = W\tilde{\rho}W^\dagger = \begin{bmatrix} |\alpha|^2 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha\beta^* \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & \vdots & & & \vdots & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^*\beta & 0 & 0 & 0 & 0 & 0 & 0 & |\beta|^2 \end{bmatrix}. \tag{8}$$

It is easy to verify (exercise!) that $\sigma = \text{diag}(p_0, p_1, p_2, p_3)$ and

$$R = R_1 = E_{11} + E_{27} + E_{35} + E_{44} + E_{53} + E_{66} + E_{78} + E_{82},$$

It follows that

$$R^\dagger \Phi(\rho) R = \sigma \otimes \tilde{\rho}. \tag{9}$$

Now the decoded state $\tilde{\rho}$ appears in the output with no syndrome measurements nor explicit projection. It should be pointed out that the unitary operation R is independent of the choice of nonnegative numbers p_j.

Exercise Verify the construction of D and R in Example 1.20 and show that these R and D satisfy equation (9).

1.4 Operator quantum error correction

In the paper [13], Kribs et al. introduced a more generalized approach to quantum error correction. They call this scheme the **operator quantum error correction (OQEC)**.

Definition 1.21 A subsystem $\mathcal{H}^B$ is said to be a **correctable subsystem (CS)** for a quantum channel Φ on $B(\mathcal{H})$ if there are a quantum channel Ψ on $B(\mathcal{H})$, a co-subsystem $\mathcal{H}^A$, and a subspace $\mathcal{K}$ so that $\mathcal{H}$ has a decomposition $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and for any $\rho^A \in B(\mathcal{H}^A)$ and $\rho^B \in B(\mathcal{H}^B)$, there is $\sigma^A \in B(\mathcal{H}^A)$ such that

$$\Psi \circ \Phi(\rho^A \otimes \rho^B) = \sigma^A \otimes \rho^B. \tag{10}$$

Or equivalently, Φ satisfies

$$\mathrm{Tr}_A \left(P_{AB} \circ \Psi \circ \Phi(\rho^A \otimes \rho^B)\right) = \rho^B \quad \text{for all} \quad \rho^A \in B(\mathcal{H}^A) \text{ and } \rho^B \in B(\mathcal{H}^B),$$

where P_{AB} is the orthogonal projection of $\mathcal{H}$ onto $\mathcal{H}^A \otimes \mathcal{H}^B$.

A necessary and sufficient condition for the existence of correctable system was also given in [13].

Theorem 1.22 *Given a decomposition $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and a quantum channel Φ on $B(\mathcal{H})$. Then $\mathcal{H}^B$ is a correctable subsystem for Φ if and only if there are scalars $\lambda_{i,j,s,t} \in \mathbb{C}$ such that*

$$P_{ii} E_s^\dagger E_t P_{jj} = \lambda_{i,j,s,t}\, P_{ij} \quad \textit{for all} \quad 1 \le i, j \le p,\ 1 \le s, t \le r. \tag{11}$$

Remark 1.23 Remarks on operator quantum error correction.

1. A noiseless subsystem is a correctable subsystem with identity map as the recovery channel. Also a correctable subsystem will reduce to a QECC if $\mathcal{H}^A$ has dimension 1. So this approach can be regarded as a unified formalism for all the technique mentioned in the subsections.

2. The equation (11) holds if and only if there is a unitary U such that

$$U^\dagger E_s^\dagger E_t\, U = \begin{bmatrix} \Lambda^{(s,t)} \otimes I_B & * \\ * & * \end{bmatrix} \quad \text{with} \quad \Lambda^{(s,t)} = \left[\lambda_{i,j,s,t}\right] \quad \text{for all} \quad 1 \le s, t \le r.$$

2 Joint higher rank numerical range

Motivated by Theorem 1.5, researchers study the (joint) higher rank numerical range defined as follows, see for example [5, 6, 7, 8, 16, 17, 18, 23].

Definition 2.1 *Given $A_1, \dots, A_m \in M_n$. The* **(joint) rank-k numerical range** $\Lambda_k(\mathbf{A})$ *of the matrices* $\mathbf{A} = (A_1, \dots, A_m)$ *is defined as the collection of* $(a_1, \dots, a_m) \in \mathbb{C}^{1\times m}$ *such that*

$$PA_jP = a_jP, \qquad j = 1, \dots, m,$$

for some rank-k orthogonal projection P.

Given a quantum channel $\Phi : M_n \to M_n$ with error operators $E_1, \dots, E_r$. Then Φ has a k-dimensional quantum correcting code if and only if

$$\Lambda_k(E_1^\dagger E_1, E_1^\dagger E_2, \dots, E_r^\dagger E_r) \neq \emptyset.$$

It is easy to check that $(a_1, \dots, a_m) \in \Lambda_k(A_1, \dots, A_m)$ if and only if any one of the following holds.

(i) There is a unitary $U \in M_n$ such that $U^\dagger A_j U = \begin{bmatrix} a_jI_k & * \\ * & * \end{bmatrix}$ for $j = 1, \dots, m$.

(ii) There is an $n \times k$ matrix X such that $X^\dagger X = I_k$ and $X^\dagger A_j X = a_j I_k$ for $j = 1, \dots, m$.

Note that $\Lambda_1(A_1, \dots, A_m)$ reduces to the (classical) joint numerical range of the matrices $A_1, \dots, A_m$ defined and denoted by

$$W(A_1, \dots, A_m) = \{(\langle x|A_1|x\rangle, \dots, \langle x|A_m|x\rangle) : |x\rangle \in \mathbb{C}^n, \langle x|x\rangle = 1\},$$

which is useful in the study of matrices and operators; see [9].

2.1 Single matrix case

Example 2.2 Consider the bi-unitary channel

$$\Phi(\rho) = pU_1\rho U_1^\dagger + (1-p)U_2\rho U_2^\dagger,$$

where U_1 and U_2 are unitary. Then Φ has a k-dimensional QECC if and only if

$$\Lambda_k(U_1^\dagger U_2) \neq \emptyset.$$

From the above example, it is of interest to study rank-k numerical range of a single matrix, $\Lambda_k(A)$. Here are some basis properties.

(P1) For any $a, b \in \mathbb{C}$, $\Lambda_k(aA + bI) = a\Lambda_k(A) + b$.

(P2) For any unitary $U \in M_n$, $\Lambda_k(U^\dagger AU) = \Lambda_k(A)$.

(P3) For any $n \times r$ matrix V with $r \geq k$ and $V^\dagger V = I_r$, we have $\Lambda_k(V^\dagger AV) \subseteq \Lambda_k(A)$.

(P4) Suppose $n < 2k$. The set $\Lambda_k(A)$ has at most one element.

The following results have been proved in [5, 7, 16, 18, 23].

Theorem 2.3 *Let $A \in M_n$ and $k \in \{1, \ldots, n\}$.*

(a) *If $n \geq 3k - 2$, then $\Lambda_k(A)$ is non-empty.*

(b) *If $n < 3k - 2$, there is $B \in M_n$ such that $\Lambda_k(B) = \emptyset$.*

(c) *If $A = A^\dagger$ has eigenvalues $\lambda_1(A) \geq \cdots \geq \lambda_n(A)$, then*

$$\Lambda_k(A) = [\lambda_{n-k+1}(A), \lambda_k(A)],$$

where the interval is an empty set if $\lambda_{n-k+1}(A) > \lambda_k(A)$ when $k > n/2$.

(d) *We have*

$$\Lambda_k(A) = \bigcap_{\xi \in [0, 2\pi)} \left\{ \mu \in \mathbb{C} : e^{i\xi}\mu + e^{-i\xi}\bar{\mu} \leq \lambda_k(e^{i\xi}A + e^{-i\xi}A^\dagger) \right\},$$

where $\lambda_k(H)$ denotes the k-th largest eigenvalue of the Hermitian matrix $H \in M_n$.

(e) *$\Lambda_k(A)$ is always convex.*

(f) *If $A \in M_n$ is a normal matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$, then*

$$\Lambda_k(A) = \bigcap_{1 \leq j_1 < \cdots < j_{n-k+1} \leq n} \mathrm{conv}\{\lambda_{j_1}, \ldots, \lambda_{j_{n-k+1}}\}.$$

2.2 General case

Let H_n be the space of $n \times n$ Hermitian matrices. Suppose

$$A_j = H_{2j-1} + iH_{2j} \quad \text{with} \quad H_{2j-1}, H_{2j} \in H_n \quad \text{for} \quad j = 1, \ldots, m.$$

Then $\Lambda_k(A_1, \ldots, A_m) \subseteq \mathbb{C}^m$ can be identified with $\Lambda_k(H_1, \ldots, H_{2m}) \subseteq \mathbb{R}^{2m}$. Thus, we will focus on the joint rank-k numerical ranges of Hermitian matrices in our discussion. Here are some basic properties.

Proposition 2.4 *Suppose $\mathbf{A} = (A_1, \ldots, A_m) \in H_n^m$, and $T = [t_{ij}]$ is an $m \times r$ real matrix. If $B_j = \sum_{i=1}^m t_{ij}A_i$ for $j = 1, \ldots, r$, and $\mathbf{B} = (B_1, \ldots, B_r)$, then*

$$\{(a_1, \ldots, a_m)T : (a_1, \ldots, a_m) \in \Lambda_k(\mathbf{A})\} \subseteq \Lambda_k(\mathbf{B}).$$

The inclusion becomes equality if $\{A_1, \ldots, A_m\}$ is linearly independent and

$$\mathrm{span}\,\{A_1, \ldots, A_m\} = \mathrm{span}\,\{B_1, \ldots, B_r\}.$$

In view of the above proposition, in the study of the geometric properties of $\Lambda_k(\mathbf{A})$, we may always assume that $A_1, \ldots, A_m$ are linearly independent.

Proposition 2.5 *Let* $\mathbf{A} = (A_1, \ldots, A_m) \in H_n^m$, *and let* $k < n$.

(a) *For any real vector* $\mu = (\mu_1, \ldots, \mu_m)$,

$$\Lambda_k(A_1 - \mu_1 I, \ldots, A_m - \mu_m I) = \Lambda_k(\mathbf{A}) - \mu.$$

(b) *If* $(a_1, \ldots, a_m) \in \Lambda_k(\mathbf{A})$, *then* $(a_1, \ldots, a_{m-1}) \in \Lambda_k(A_1, \ldots, A_{m-1})$.

(c) $\Lambda_{k+1}(\mathbf{A}) \subseteq \Lambda_k(\mathbf{A})$.

Proposition 2.6 *Let* $\mathbf{A} \in H_n^m$ *and* $1 < k < n$. *Then* $\Lambda_k(\mathbf{A})$ *is non-empty if*

$$n \geq (k-1)(m+1)^2.$$

If $\Lambda_k(A_1, \ldots, A_m)$ has a non-trivial convex subset, then it is more resistant to perturbation. Recall that a set $\mathcal{S} \subseteq \mathbb{R}^m$ is **star-shaped** with a star center μ_0 if for every $\mu \in \mathcal{S}$, the line segment joining μ_0 and μ lies entirely in $\mathcal{S}$.

Theorem 2.7 *Let* $\mathbf{A} = (A_1, \ldots, A_m) \in H_n^m$ *and* $k \in \{1, \ldots, n-1\}$. *If* $\Lambda_{\hat{k}}(\mathbf{A}) \neq \emptyset$ *for some* $\hat{k} \geq (m+2)k$, *then* $\Lambda_k(\mathbf{A})$ *is star-shaped and contains the convex subset* $\mathrm{conv}\Lambda_{\hat{k}}(\mathbf{A})$ *so that every element in* $\mathrm{conv}\Lambda_{\hat{k}}(\mathbf{A})$ *is a star center of* $\Lambda_k(\mathbf{A})$.

Remark 2.8 There are many open problems for joint higher rank numerical range.

1. If A_1, A_2, A_3 mutually commute and $n \geq 5$, then $\Lambda_2(A_1, A_2, A_3)$ is non-empty. For general $A_1, A_2, A_3 \in H_n$, we only know that $\Lambda_2(A_1, A_2, A_3)$ is non-empty if $n \geq 7$. How about $n = 5, 6$?
2. It would be interesting to determine the minimum n (depending on m and k) for which $\Lambda_k(A_1, \ldots, A_m)$ is non-empty, star-shaped, or convex.

Exercise

1. Prove the basis properties (P1) – (P4).
2. Suppose $A \in M_8$ is unitary with eigenvalues $1, w, \ldots, w^7$, where $w = e^{i2\pi/8}$. What are $\Lambda_2(A)$, $\Lambda_3(A)$, and $\Lambda_4(A)$? What if we replace the eigenvalue 1 by $e^{i\theta}$ for some small $\theta > 0$?
3. Suppose U is a 4×4 unitary matrix. Show that $\Lambda_2(U)$ is either a singleton set of a line segment. Hence, show that a bi-unitary quantum channel on M_4 always have a 2-dimensional QECC.
4. Prove Propositions 2.5 and 2.6.

3 Fully correlated quantum channel

A noisy quantum channel is called **fully correlated** when all the qubits constituting the codeword are subject to the same error operators. This situation happens when size of the system is much smaller than the wavelength of the external disturbance causing the error. In general, such quantum channel has error operator of the form

$$W^{\otimes n} = W \otimes \cdots \otimes W \quad \text{with unitary } W \in M_2.$$

We introduce operators

$$X_n = \otimes_{i=1}^n \sigma_x, \quad Y_n = \otimes_{i=1}^n \sigma_y \quad \text{and} \quad Z_n = \otimes_{i=1}^n \sigma_z$$

acting on the n-qubit space $\mathbb{C}^{2^n} = \otimes_{i=1}^n \mathbb{C}^2$, where $n > 2$. Consider the quantum channel of the form

$$\Phi(\rho) = p_0\rho + p_1 X_n \rho X_n^\dagger + p_2 Y_n \rho Y_n^\dagger + p_3 Z_n \rho Z_n^\dagger \qquad \text{with} \quad p_j > 0 \text{ and } \sum_{i=0}^{3} p_i = 1. \tag{12}$$

Notice that Φ has a k-dimensional quantum error correcting code if and only if $\Lambda_k(X_n, Y_n, Z_n) \neq \emptyset$. To prove this statement, recall that from Theorems 1.5, there is a QECC with dimension k if and only if $\Lambda_k(\{E_i^\dagger E_j\}_{1\leq i,j\leq r}) \neq \emptyset$. Notice that $X_n^2 = Y_n^2 = Z_n^2 = I$ and

$$X_nY_n = i^n Z_n, \quad Y_nZ_n = i^n X_n, \quad Z_nX_n = i^n Y_n,$$

the channel (12) has a k-dimensional QECC if and only if

$$\Lambda_k(X_n, Y_n, Z_n, I) \neq \emptyset.$$

By noting that $PIP = P$, we find $\Lambda_k(X_n, Y_n, Z_n) \neq \emptyset$ if and only if $\Lambda_k(X_n, Y_n, Z_n, I) \neq \emptyset$.

The following results can be found in [15].

Theorem 3.1 *Suppose $n > 2$ is odd. Then $\Lambda_{2^{n-1}}(X_n, Y_n, Z_n) \neq \emptyset$.*

With the help of Theorem 1.18, one can prove the following.

Corollary 3.2 *Suppose n is odd and $\Phi : M_{2^n} \to M_{2^n}$ is a fully correlated quantum channel given by*

$$\Phi(\rho) = p_0\rho + p_1 X_n \rho X_n^\dagger + p_2 Y_n \rho Y_n^\dagger + p_3 Z_n \rho Z_n^\dagger.$$

There exist a unitary $R \in M_{2^n}$ and a density matrix $\rho_a \in M_2$ such that

$$\Phi\left(R(|0\rangle\langle 0| \otimes \tilde{\rho})R^\dagger\right) = R\left(\rho_a \otimes \tilde{\rho}\right)R^\dagger \quad \text{for all} \quad \tilde{\rho} \in M_{2^{n-1}}.$$

So one can encode $(n-1)$-data qubit states to n-qubit codewords.

Example 3.3 When $n = 3$, the recovery unitary matrix $R \in M_8$ can be chosen as

$$\begin{aligned} R &= E_{11} + E_{42} + E_{73} + E_{64} + E_{85} + E_{56} + E_{27} + E_{38} \\ &= |000\rangle\langle 000| + |011\rangle\langle 001| + |110\rangle\langle 010| + |101\rangle\langle 011| \\ &\quad +|111\rangle\langle 100| + |100\rangle\langle 101| + |001\rangle\langle 110| + |010\rangle\langle 111|, \end{aligned}$$

which is indeed a permutation matrix. Figure 1 shows a quantum circuit of the matrix R for $n = 3$.

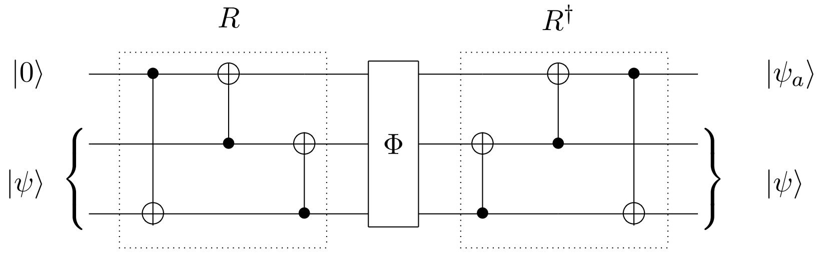

Figure 1: An encoding and recovery circuit, which encodes and recovers an arbitrary 2-qubit state $|\psi\rangle$ with a single ancilla qubit initially in the state $|0\rangle$. The quantum channel in the box represents a quantum operation with fully correlated noise given in Eq. (12). The output ancilla state is $* = 0$ (1) for error operators I and Z_3 (X_3 and Y_3) for $n = 3$.

When $n = 5$, R can be chosen as

$$\begin{aligned} R = \; & |00000\rangle\langle 00000| + |00011\rangle\langle 00001| + |00110\rangle\langle 00010| + |00101\rangle\langle 00011| + |01100\rangle\langle 00100| \\ & +|01111\rangle\langle 00101| + |01010\rangle\langle 00110| + |01001\rangle\langle 00111| + |11000\rangle\langle 01000| + |11011\rangle\langle 01001| \\ & +|11110\rangle\langle 01010| + |11101\rangle\langle 01011| + |10100\rangle\langle 01100| + |10111\rangle\langle 01101| + |10010\rangle\langle 01110| \\ & +|10001\rangle\langle 01111| + |11111\rangle\langle 10000| + |11100\rangle\langle 10001| + |11001\rangle\langle 10010| + |11010\rangle\langle 10011| \\ & +|10011\rangle\langle 10100| + |10000\rangle\langle 10101| + |10101\rangle\langle 10110| + |10110\rangle\langle 10111| + |00111\rangle\langle 11000| \\ & +|00100\rangle\langle 11001| + |00001\rangle\langle 11010| + |00010\rangle\langle 11011| + |01011\rangle\langle 11100| + |01000\rangle\langle 11101| \\ & +|01101\rangle\langle 11110| + |01110\rangle\langle 11111|. \end{aligned}$$

Figure 2 shows a quantum circuit of the matrix R for $n = 5$.

Now let us turn to the even n case.

Theorem 3.4 *Suppose $n > 2$ is even. Then $\Lambda_{2^{n-2}}(X_n, Y_n, Z_n) \neq \emptyset$ but $\Lambda_{2^{n-1}}(X_n, Y_n, Z_n) = \emptyset$.*

For even n, one can encode at most $(n-2)$-data qubit states to n-qubit codewords. Furthermore, one can show that Φ actually has a 2^{n-2}-dimensional decoherence free subspace.

Corollary 3.5 *Suppose n is even and $\Phi : M_{2^n} \to M_{2^n}$ is a fully correlated quantum channel given by*

$$\Phi(\rho) = p_0\rho + p_1 X_n \rho X_n^\dagger + p_2 Y_n \rho Y_n^\dagger + p_3 Z_n \rho Z_n^\dagger.$$

There exists a unitary $R \in M_{2^n}$ such that

$$\Phi\left(R(|00\rangle\langle 00| \otimes \tilde{\rho})R^\dagger\right) = R\left(|00\rangle\langle 00| \otimes \tilde{\rho}\right) R^\dagger \quad \textit{for all} \quad \tilde{\rho} \in M_{2^{n-2}}.$$

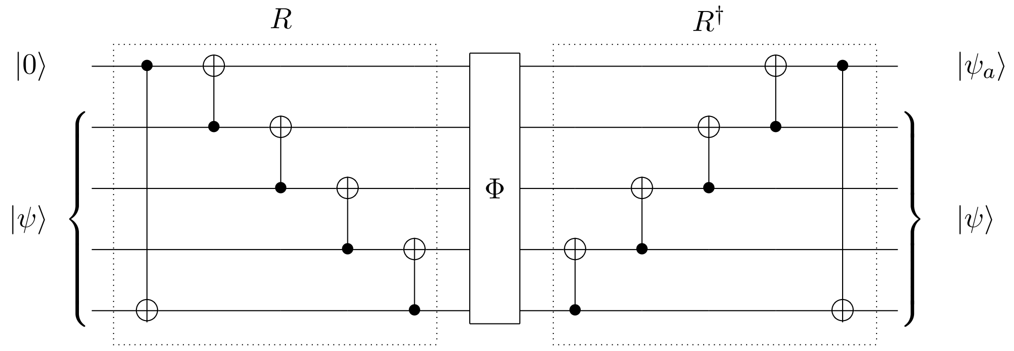

Figure 2: An encoding and recovery circuit, which encodes and recovers an arbitrary 4-qubit state $|\psi\rangle$ with a single ancilla qubit initially in the state $|0\rangle$. The quantum channel in the box represents a quantum operation with fully correlated noise given in Eq. (12). The output ancilla state is $* = 0$ (1) for error operators I and Z_5 (X_5 and Y_5) for $n = 5$.

Example 3.6 When $n = 4$, consider the vectors

$$\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle), \quad \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle),$$
$$\frac{1}{\sqrt{2}}(|0101\rangle + |1010\rangle), \quad \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle),$$

These vectors are invariant under the action of X_4, Y_4, and Z_4. Thus, the space spanned by the four vectors forms a 4-dimensional quantum error correcting code. Indeed, we find a decoherence-free encoding for 2 qubits by projecting onto this invariant subspace spanned by these basis. It should be noted that in this case, $(1, 1, 1) \in \Lambda_4(X_4, Y_4, Z_4)$. Figure 3 shows a quantum circuit of the matrix R for $n = 4$.

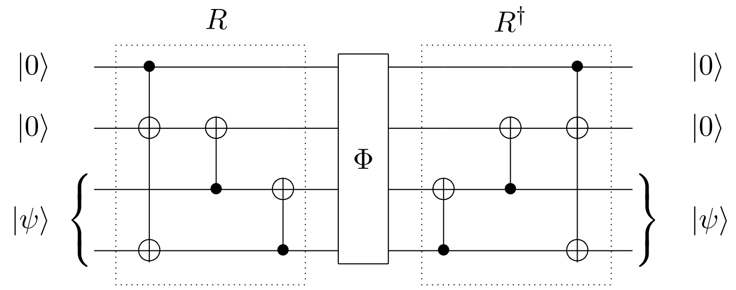

Figure 3: An encoding and recovery circuit, which encodes and recovers an arbitrary 2-qubit state ρ with two ancilla qubit initially in the state $|00\rangle\langle 00|$. The quantum channel in the box represents a quantum operation with fully correlated noise given in Eq. (12). The output ancilla state is always $|00\rangle\langle 00|$, irrespective of error operators acted in the channel.

Exercise Define

$$\mathcal{V} = \text{span}\left\{|j_1\, j_2\, \ldots\, j_n\rangle \in \mathbb{C}^{2^n} : \text{ number of } k \text{ where } j_k = 1 \text{ is even}\right\}.$$

Show that when n is odd, $\mathcal{V}$ is a 2^{n-1}-dimensional QECC for the quantum channel Φ of the form (12). Also construct a 2^{n-2}-dimensional QECC when n is even.

Acknowledgemnt

The author would like to thank Professors Jinchuan Hou and Chi-Kwong Li, the organizers of the "Summer School on Quantum Information Science", for giving me the opportunity to lecture at the summer school. Thanks are also extended to colleagues at Taiyuan University of Technology for their hospitality and support during his visit at Taiyuan, China. This work was supported in part by a HK RGC grant.

References

[1] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Mixed state entanglement and quantum error correction, Phys. Rev. A 54 (1996), 3824-3851.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inf. Th. 44 (1998), 1369.

[3] A.R. Calderbank and P.W. Shor, Good quantum error correcting codes exists, Phys. Rev. A 54 (1996), 1098-1105.

[4] M.D. Choi, Completely positive linear maps on complex matrices. Linear Algebra and Appl. 10 (1975), 285-290.

[5] M.D. Choi, M. Giesinger, J. A. Holbrook, and D.W. Kribs, Geometry of higher-rank numerical ranges, Linear and Multilinear Algebra 56 (2008), 53-64.

[6] M.D. Choi, J.A. Holbrook, D. W. Kribs, and K. Życzkowski, Higher-rank numerical ranges of unitary and normal matrices, Operators and Matrices 1 (2007), 409-426.

[7] M.D. Choi, D. W. Kribs, and K. Życzkowski, Higher-rank numerical ranges and compression problems, Linear Algebra Appl., 418 (2006), 828–839.

[8] M.D. Choi, D. W. Kribs, and K. Życzkowski, Quantum error correcting codes from the compression formalism, Rep.. Math. Phys., 58 (2006), 77–91.

[9] K.E. Gustafson and D.K.M. Rao, Numerical ranges: The field of values of linear operators and matrices, Springer, New York, 1997.

[10] J. Kempe, Approaches to quantum error correction, Séminaire Poincaré 2 (2005), 1-29.

[11] A.Y. Kitaev, A.H. Shen, and M.N. Vyalyi, Classical and quantum computation, Graduate Series in Mathematics no. 47, AMS, 2002.

[12] E. Knill and R. Laflamme, Theory of quantum error correcting codes, Phys. Rev. A 55 (1997), 900-911.

[13] D.W. Kribs, R. Laflamme, D. Poulin, M. Lesosky Operator quantum error correction, Quant. Inf. & Comp., 6 (2006), 383-399.

[14] C.K. Li, M. Nakahara, Y.T. Poon, N.S. Sze, H. Tomita Quantum error correction without measurement and an efficient recovery operation, preprint. [arVix:1102.1618]

[15] C.K. Li, M. Nakahara, Y.T. Poon, N.S. Sze, H. Tomita Efficient Quantum Error Correction for Fully Correlated Noise, Phys. Lett. A, to appear. [arVix:1104.4750]

[16] C.K. Li, Y.T. Poon, and N.S. Sze, Condition for the higher rank numerical range to be non-empty, Linear and Multilinear Algebra 57 (2009), 365-368.

[17] C.K. Li, Y.T. Poon, and N.S. Sze, Higher rank numerical ranges and low rank perturbations of quantum channels, J. Mathematical Analysis Appl. 348 (2008), 843-855.

[18] C.K. Li and N.S. Sze, Canonical forms, higher rank numerical ranges, totally isotropic subspaces, and matrix equations, Proc. Amer. Math. Soc. 136 (2008), 3013-3023

[19] M. Nakahara and T. Ohmi, Quantum Computing: From Linear Algebra to Physical Realizations, CRS Press, New York, 2008.

[20] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[21] P.W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A, 52 (1995), 2493-2496.

[22] A.M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. 77 (1996), 793-797.

[23] H. Woerdeman, The higher rank numerical range is convex, Linear and Multilinear Algebra 56 (2008), 65-67.