Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 400 (2005) 147–167
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

A quantum computing primer for operator theorists

David W. Kribs*

Department of Mathematics and Statistics, University of Guelph, Guelph, ON, Canada N1G 2W1
Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada N2L 3G1
Perimeter Institute for Theoretical Physics, 35 King St. North, Waterloo, ON, Canada N2J 2W9

Received 27 April 2004; accepted 10 November 2004
Available online 21 December 2004
Submitted by R. Bhatia

Abstract

This is an exposition of some of the aspects of quantum computation and quantum information that have connections with operator theory. After a brief introduction, we discuss quantum algorithms. We outline basic properties of quantum channels, or equivalently, completely positive trace preserving maps. The main theorems for quantum error detection and correction are presented and we conclude with a description of a particular passive method of quantum error correction.

AMS classification: 47L90; 47N50; 81P68

Keywords: Quantum computation; Quantum information; Quantum algorithms; Completely positive maps; Quantum channels; Quantum error correction; Noiseless subsystems

1. Introduction

The study of the underlying mathematics for quantum computation and quantum information is quickly becoming an interesting area of research [61]. While these

* Address: Department of Mathematics and Statistics, University of Guelph, Guelph, ON, Canada N1G 2W1.
E-mail address: dkribs@uoguelph.ca

0024-3795/$ - see front matter
doi:10.1016/j.laa.2004.11.010

fields promise far reaching applications [12,24,41,60], there are still many theoretical and experimental issues that must be overcome, and many involve deep mathematical problems. The main goal of this paper is to provide a primer on some of the basic aspects of quantum computing for researchers with interests in operator theory or operator algebras. However, we note that the only prerequisite for reading this article is a strong background in linear algebra.

This work should not be regarded as an extensive introduction to the subject. Indeed, the reader with knowledge of quantum computing will surely have complaints about the selection of material presented. Moreover, we do not consider here the increasingly diverse fields of mathematics for which there are connections with quantum computing (algebraic geometry, Fourier analysis, group theory, number theory, operator algebras, etc.). Rather, our intention is to give a brief introduction and prove some specific results with the hope that this paper will help stimulate interest within the operator community.

The paper is organized as follows. The next section (Section 2) contains a discussion of the basic notions, notation and nomenclature used in quantum computing. In Section 3 we give a brief introduction to quantum algorithms by describing some elementary examples and presenting a simple algorithm (Deutsch's algorithm [19,20]) that demonstrates the power of quantum computation. In Section 4 we outline the mathematical formalism for the evolution of information inside quantum systems. This is provided by quantum channels, which are represented by completely positive trace preserving maps [15,27,51,52,62,63]. The penultimate section (Section 5) includes a discussion of quantum error correction methods. We present the fundamental theorems for quantum error detection and correction in the 'standard model' [28,47,64]. In the final section (Section 6) we describe a specific method of quantum error prevention [23,26, 32,47,48,57,82] called the 'noiseless subsystem via noise commutant' method. Finally, we have included a large collection of references as an attempt to give the interested reader an entrance point into the quantum information literature.

2. Quantum computing basics

Let $\mathscr{H}$ be a (complex) Hilbert space. We shall use the Dirac notation for vectors and vector duals in $\mathscr{H}$: A typical vector in $\mathscr{H}$ will be written as a 'ket' $|\psi\rangle$, and the linear functional on $\mathscr{H}$ determined by this vector is written as the 'bra' $\langle\psi|$. Notice that the products of a bra and a ket yield the inner product, $\langle\psi_1||\psi_2\rangle$, and a rank one operator, $|\psi_2\rangle\langle\psi_1|$. In particular, given $|\psi\rangle \in \mathscr{H}$, the rank one projection of $\mathscr{H}$ onto the subspace $\{\lambda|\psi\rangle : \lambda \in \mathbb{C}\}$ is written $|\psi\rangle\langle\psi|$. Further let $\mathscr{B}(\mathscr{H})$ be the collection of operators which act on $\mathscr{H}$. We will use the physics convention $U^\dagger$ for the adjoint of an operator U.

The study of operators on Hilbert space is central to the theory of quantum mechanics. For instance, consider the following formulation of the *postulates of quantum mechanics* [16,61,77]:

(i) To every closed quantum system there is an associated Hilbert space $\mathscr{H}$. The state of the system at any given time is described by a unit vector $|\psi\rangle$ in $\mathscr{H}$, or equivalently by a rank one projection $|\psi\rangle\langle\psi|$. When the state of the system is not completely known, it is represented by a *density operator* ρ on $\mathscr{H}$, which is a positive operator with trace equal to one. (This is the quantum analogue of a probability distribution.)

(ii) The notion of *evolution* in a closed quantum system is described by unitary transformations. That is, there is a unitary operator U on the system Hilbert space such that the corresponding evolution is described by the conjugation map $\rho \mapsto U\rho U^\dagger$.

(iii) A *measurement* of a quantum system on $\mathscr{H}$ is described by a set of operators M_k, $1 \leqslant k \leqslant r$, such that

$$\sum_{k=1}^{r} M_k^\dagger M_k = \mathbb{1}.$$

The measurement is *projective* if each of the M_k is a projection, and thus the M_k have mutually orthogonal ranges. (A 'classical measurement' arises when all the projections are rank one.) The index k refers to the possible measurement outcomes in an experiment. If the state of the system is $|\psi\rangle$ before the experiment, then the probability that event k occurs is given by $p(k) \equiv \langle\psi|M_k^\dagger M_k|\psi\rangle$. Notice that $\{p(k)\}$ determines a probability distribution.

(iv) Given Hilbert spaces $\mathscr{H}_1, \ldots, \mathscr{H}_m$ associated with m quantum systems, there is a *composite quantum system* on the Hilbert space $\mathscr{H}_1 \otimes \cdots \otimes \mathscr{H}_m$. In particular, if the states of the individual systems are $|\psi_i\rangle$, then the state of the composite system is given by $|\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle$.

The Hilbert spaces of interest in quantum information theory are of dimension $N = d^n$ for some positive integers $n \geqslant 1$ and $d \geqslant 2$. (It is generally thought that extensions to infinite dimensional space will be necessary in the future, but the current focus is mainly on finite dimensional aspects.) For brevity we shall focus on the $d = 2$ cases. Thus we let $\mathscr{H}_N$ be the Hilbert space of dimension 2^n given by the n-fold tensor product $\mathscr{H}_N = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$. We will drop reference to N when convenient. Let $\{|0\rangle, |1\rangle\}$ be a fixed orthonormal basis for 2-dimensional Hilbert space $\mathscr{H}_2 = \mathbb{C}^2$. These vectors will correspond to the classical base states in a given two level quantum system; such as the ground and excited states of an electron in an atom, 'spin-up' and 'spin-down' of an electron, two polarizations of a photon of light, etc. We shall make use of the abbreviated form from quantum mechanics for the associated standard orthonormal basis for $\mathscr{H}_{2^n} = (\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}$. For instance, the basis for $\mathscr{H}_4$ is given by $\{|ij\rangle : i, j \in \mathbb{Z}_2\}$, where $|ij\rangle$ is the vector tensor product $|ij\rangle \equiv |i\rangle|j\rangle \equiv |i\rangle \otimes |j\rangle$.

A quantum bit of information, or a 'qubit', is given by a unit vector $|\psi\rangle = a|0\rangle + b|1\rangle$ in $\mathscr{H}_2$. The cases $a = 0$ or $b = 0$ correspond to the classical states, and otherwise $|\psi\rangle$ is said to be in a *superposition* of the states $|0\rangle$ and $|1\rangle$. A 'qudit' is a unit vector in $\mathbb{C}^d$. A vector state $|\psi\rangle$ in $\mathscr{H}_N$ is said to be *entangled* if it cannot be

written as a tensor product of states from its component systems, so that $|\psi\rangle$ does not decompose as $|\psi\rangle = |\phi_1\rangle|\phi_2\rangle$ for some vectors $|\phi_i\rangle$, $i = 1, 2$. As an example, consider $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ in $\mathscr{H}_4$, this is a vector from the so-called 'EPR pairs' or 'Bell states'. Roughly speaking, the notion of *decoherence* in a quantum system corresponds to the vanishing of off-diagonal entries in matrices associated with the system as it evolves.

A number of specific unitary matrices arise in the discussions below. The *Pauli matrices* are given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $\mathbb{1}_2$ be the 2×2 identity matrix. We regard these as matrix representations for operators acting on the given basis for $\mathscr{H}_2$. In the n-qubit case (so $N = 2^n$) we may consider all 'single qubit unitary gates' determined by the Pauli matrices. This is the set of all unitaries $\{X_k, Y_k, Z_k : 1 \leqslant k \leqslant n\}$ where $X_1 = X \otimes \mathbb{1}_2^{\otimes(n-1)}$, $X_2 = \mathbb{1}_2 \otimes X \otimes \mathbb{1}_2^{\otimes(n-2)}$, etc. Further let U_{CN} be the 'controlled-NOT gate' on $\mathscr{H}_4$. This is the unitary which acts on $\mathscr{H}_4$ by $U_{CN} : |i\rangle|j\rangle \mapsto |i\rangle|(i + j) \bmod 2\rangle$. The CNOT gate has natural extensions $\{U_{CN}^{(k,l)} : 1 \leqslant k \neq l \leqslant n\}$ to unitary gates on $\mathscr{H}_N$, where the kth and lth tensor slots act, respectively, as the control and target qubits. For instance, with this notation $U_{CN} = U_{CN}^{(1,2)}$. Note that $U_{CN}^{(k,l)}$ only acts on the kth and lth qubits in $\mathscr{H}_N = (\mathbb{C}^2)^{\otimes n}$. The set $\{X_k, Y_k, Z_k, U_{CN}^{(k,l)} : 1 \leqslant k \neq l \leqslant n\}$ forms a set of universal quantum gates for $\mathscr{H}_N$, meaning that this set generates the set of $N \times N$ unitary matrices $\mathscr{U}(N)$ as a group (up to complex phases). We shall also make use of the *Hadamard gate*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and the spin-$\frac{1}{2}$ Pauli matrices $\sigma_k = 1/2K$ for $k = x, y, z$.

3. Quantum algorithms

Simply put, a *quantum algorithm* consists of an ensemble of initial states ρ which evolves under a unitary matrix U to a final density matrix $U\rho U^\dagger$. The famous factoring algorithm of Shor [67,70] and search algorithm of Grover [31] have received tremendous attention over the last decade. As a proper treatment of these algorithms is beyond the scope of this article, in this note we shall present the Deutsch algorithm [19] (and its generalization, the Deutsch–Josza algorithm [20]) since it is easily accessible and gives a good illustration of the power of quantum computation. In doing so, we shall give a description of two fundamental classes of quantum algorithms: the simulation of a classical function on a quantum computer and the algorithm for quantum parallel computation.

Before continuing, let us illustrate a simple example of how an operation such as *addition* may be performed with a quantum algorithm. This will also allow us to establish some notation for the discussion which follows. We shall identify the standard basis vectors $|i_1 \cdots i_n\rangle$ for $\mathscr{H}_N$ with the integers $\{0, 1, \ldots, 2^n - 1\}$ via binary expansions. Then we may define a unitary U on $\mathscr{H}_N \otimes \mathscr{H}_N$ by $U|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$ where the addition $x \oplus y$ is modulo N. The corresponding quantum algorithm implements addition modulo N. (Note that the CNOT gate is obtained in the case $N = 2$.)

Towards the Deutsch algorithm, let $H_n = H^{\otimes n}$ be the n-fold tensor product of the Hadamard gate acting on $\mathscr{H}_N$. Observe that $H_n|0\rangle^{\otimes n}$ is the uniform superposition

$$H_n|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Fix positive integers $k, m \geqslant 1$. Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^k$ be a function. Consider the space $\mathscr{H}_{m,k} = \mathscr{H}_{2^m} \otimes \mathscr{H}_{2^k}$. Then $\mathscr{H}_{m,k}$ has basis $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle$ where $x \in \mathbb{Z}_2^m$ and $y \in \mathbb{Z}_2^k$. Define a unitary map $U_f : \mathscr{H}_{m,k} \to \mathscr{H}_{m,k}$ by

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle.$$

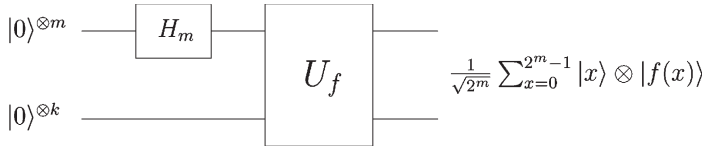
For a given $x \in \mathbb{Z}_2^m$, notice that the action of U_f is to permute the basis vectors $\{|x\rangle|y\rangle : y \in \mathbb{Z}_2^k\}$.

Note 3.1. Observe that $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for all x. Thus U_f *simulates* f on a quantum computer, and in this sense any classical function can be performed on a quantum computer.

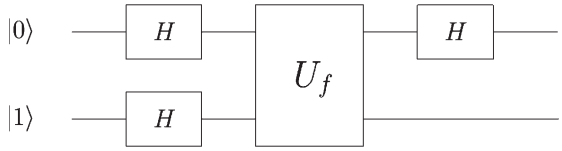
Next we compute

$$\begin{aligned} U_f((H_m|0\rangle^{\otimes m}) \otimes |0\rangle^{\otimes k}) &= U_f\left(\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |0\rangle\right) \\ &= \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} U_f(|x\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |f(x)\rangle. \end{aligned}$$

Hence an application of $H_m \otimes \mathbb{1}_{2^k}$ followed by U_f yields a simultaneous parallel computation of f on *all* possible values of x. The corresponding 'circuit-gate' diagram for *quantum parallelism* for f is given below. In such a diagram, the 'circuits' correspond to states from the component systems (in this case $|0\rangle^{\otimes m}$ and $|0\rangle^{\otimes k}$ from the systems $\mathscr{H}_{2^m}$ and $\mathscr{H}_{2^k}$ respectively). The 'gates', drawn as boxes, indicate unitary operators applied as the system evolves with a left-to-right convention in the diagram (so here $H_m \otimes \mathbb{1}_{2^k}$ is applied first, then U_f is applied).



Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a function. Then call f *constant* if $f(0) = f(1)$ and *balanced* if $f(0) \neq f(1)$. The problem addressed by *Deutsch's algorithm* is the following: Given $f : \mathbb{Z}_2 \to \mathbb{Z}_2$, determine if it is constant or balanced. Classically an answer to this problem requires two evaluations of f. On the other hand, Deutsch's algorithm shows how to do this with one quantum operation. The circuit-gate diagram for the algorithm is given below.



The initial state is given by $|01\rangle = |0\rangle \otimes |1\rangle$. The first stage of the algorithm evolves this state to

$$(H \otimes H)(|0\rangle \otimes |1\rangle) = (H|0\rangle) \otimes (H|1\rangle) = |+\rangle \otimes |-\rangle,$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Observe that the action of U_f as defined above yields

$$U_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)}|x\rangle \otimes |-\rangle \quad \text{for } x \in \mathbb{Z}_2.$$

Thus, after the second stage of the algorithm the system has evolved to

$$\begin{aligned} U_f(|+\rangle \otimes |-\rangle) &= \frac{1}{\sqrt{2}} U_f((|0\rangle + |1\rangle) \otimes |-\rangle) \\ &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \otimes |-\rangle \\ &= \begin{cases} \pm|+\rangle \otimes |-\rangle & \text{if } f \text{ is constant,} \\ \pm|-\rangle \otimes |-\rangle & \text{if } f \text{ is balanced.} \end{cases} \end{aligned}$$

Finally, we apply a Hadamard gate H to the first qubit; that is, we apply $H \otimes \mathbb{1}_2$ to the full system. Thus the system evolves to

$$\begin{cases} (H \otimes \mathbb{1}_2)(\pm|+\rangle \otimes |-\rangle) = \pm|0\rangle \otimes |-\rangle & \text{if } f \text{ is constant,} \\ (H \otimes \mathbb{1}_2)(\pm|-\rangle \otimes |-\rangle) = \pm|1\rangle \otimes |-\rangle & \text{if } f \text{ is balanced.} \end{cases}$$

In particular, if we measure the first qubit we get

$$\begin{cases} \pm|0\rangle & \text{if } f \text{ is constant,} \\ \pm|1\rangle & \text{if } f \text{ is balanced.} \end{cases}$$

Note that there is no uncertainty in the result: If we measure the first qubit and obtain $\pm|0\rangle$ (respectively $\pm|1\rangle$), then we know f is constant (respectively balanced) with probability 1.

Remark 3.2. The Deutsch–Josza generalization [20] yields a more dramatic result. Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ be a function. Define f to be constant if $f(x) = f(y)$ for $x, y \in \mathbb{Z}_2^m$, and balanced if $|f^{-1}(0)| = 2^{m-1} = |f^{-1}(1)|$. Suppose we know f is either constant or balanced and that we wish to determine which one f is. Classically, this requires $2^{m-1} + 1$ evaluations to know with certainty what type f is. The Deutsch–Josza algorithm shows how this may be accomplished with a single operation on a quantum computer. The algorithm acts on $\mathscr{H}_{2^m} \otimes \mathscr{H}_2$ with initial state $|0\rangle^{\otimes m} \otimes |1\rangle$. The circuit-gate diagram may be obtained by adjusting the Deutsch diagram with $|0\rangle^{\otimes m} \otimes |1\rangle$ in place of $|0\rangle \otimes |1\rangle$, m circuits at the top instead of one, H_m in place of H in the top circuits prior to U_f, and H_m in place of the final H. Thus,

$$|0\rangle^{\otimes m} \otimes |1\rangle \mapsto (H_m \otimes \mathbb{1}_2)U_f(H_m \otimes H)(|0\rangle^{\otimes m} \otimes |1\rangle).$$

Note 3.3. As a starting point for more recent work on quantum algorithms we mention [11,59,78]. Also see [7] for an extensive mathematical introduction to the study of quantum algorithms.

4. Quantum channels

While evolution in a closed quantum system is unitary (see postulate (ii)), experimentally evolution occurs in an 'open quantum system'. In such a system evolution is described mathematically by completely positive trace preserving maps [61]. The physical motivation for this is discussed below.

A (linear) map $\mathscr{E} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})$ where $\mathscr{H}$ is a Hilbert space is *completely positive* if for all $k \geqslant 1$ the 'ampliation map'

$$\mathscr{E}^{(k)} : \mathscr{M}_k(\mathscr{B}(\mathscr{H})) \to \mathscr{M}_k(\mathscr{B}(\mathscr{H}))$$

given by $\mathscr{E}^{(k)}((\rho_{ij})) = (\mathscr{E}(\rho_{ij}))$ is a positive map. (We could also write $\mathscr{E}^{(k)} = \mathbb{1}_k \otimes \mathscr{E}$.) This is a rather strong condition; for instance, the transpose map is the standard example of a positive map which is not completely positive. The study of completely positive maps has been an active area of research in both the quantum physics and operator theory communities for at least thirty years. (In fact, it seems that many general results on completely positive maps have been obtained in the two fields without knowledge of the other.) See the texts of Kraus [51] and Paulsen [62,63] for good treatments of the subject from the two perspectives and [37,38] for other early work.

Thus, in the general setting quantum information evolves through an open quantum system via completely positive trace preserving maps.

Definition 4.1. A *quantum channel* $\mathscr{E} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})$ is a map which is completely positive and trace preserving.

Trace preservation for a channel is equivalent to requiring the preservation of probabilities as states evolve through a quantum system. A channel is positive since density operators must evolve to density operators, and it is completely positive because this property must be preserved when the initial system is tensored with other systems (as part of a composite system). Physically, an open system can be regarded as lying inside a larger closed quantum system where all evolution occurs in a unitary manner. Thus, evolution in the open system can be regarded as a 'compression' of the unitary evolution on the larger closed system. The mathematical formalism for this physical description is provided by Stinespring's dilation theorem [72].

The following fundamental result for completely positive maps was proved independently by Choi [15] and Kraus [52]. We present Choi's short operator proof.

Theorem 4.2. *Let $\mathscr{E} : \mathscr{B}(\mathscr{H}_N) \to \mathscr{B}(\mathscr{H}_N)$ be a completely positive map. Then there are operators $E_k \in \mathscr{B}(\mathscr{H}_N)$, $1 \leqslant k \leqslant N^2$, such that*

$$\mathscr{E}(\rho) = \sum_{k=1}^{N^2} E_k \rho E_k^\dagger \quad \text{for all } \rho \in \mathscr{B}(\mathscr{H}_N). \tag{1}$$

Proof. Let $e_{ij} = |i\rangle\langle j|$ be the matrix units associated with the standard basis for $\mathscr{H}_N$. Let $R = \mathscr{E}^{(N)}((e_{ij}))$. This matrix is positive by the N-positivity of $\mathscr{E}$. (In fact, Choi proved that the positivity of R characterizes complete positivity of $\mathscr{E}$.) Consider a decomposition $R = \sum_{k=1}^{N^2} |a_k\rangle\langle a_k|$, where $|a_k\rangle \in \mathbb{C}^{N^2}$ are (appropriately normalized) eigenvectors for R. Let $\{P_i : 1 \leqslant i \leqslant N\}$ be the family of rank N projections on $\mathbb{C}^{N^2}$ which have mutually orthogonal ranges and satisfy $P_i R P_j = \mathscr{E}(e_{ij})$. Then $|a_k\rangle = \sum_{i=1}^{N} P_i|a_k\rangle$. Define operators $E_k : \mathbb{C}^N \to \mathbb{C}^N$ by $E_k|i\rangle \equiv P_i|a_k\rangle$, so that

$$R = \sum_k \sum_{i,j} P_i|a_k\rangle\langle a_k|P_j = \sum_{i,j} P_i \left(\sum_k E_k|i\rangle\langle j|E_k^\dagger \right) P_j.$$

Hence,

$$\mathscr{E}(e_{ij}) = \mathscr{E}(|i\rangle\langle j|) = P_i R P_j = \sum_{k=1}^{N^2} E_k|i\rangle\langle j|E_k^\dagger,$$

and Eq. (1) holds by the linearity of $\mathscr{E}$. □

The decomposition (1) is referred to as the *operator-sum representation* of $\mathscr{E}$ in quantum information theory. The operators E_k are called the *noise operators* or *errors* of the channel. Note that trace preservation of a channel is equivalent to its noise operators E_k satisfying

$$\sum_k E_k^\dagger E_k = \mathbb{1}.$$

Remark 4.3. Choi's proof of this theorem provided the impetus for a recent application of Leung [56] to 'quantum process tomography'. This is a procedure by which an unknown quantum channel can be fully recovered from experimental data. To accomplish this for a given channel, (1) shows that it is enough to recover the noise operators E_i. As Leung observes, Choi's proof shows the only experimental data required to fully reconstruct the E_i are the output states $\mathscr{E}(|i\rangle|j\rangle)$. This fact is the core of the tomography procedure outlined in [56].

The following result, which we state without proof, shows precisely how different sets of noise operators for the same channel are related.

Proposition 4.4. *Let* $\{E_1, \ldots, E_r\}$ *and* $\{E'_1, \ldots, E'_r\}$ *be the noise operators for channels* $\mathscr{E}$ *and* $\mathscr{E}'$ *respectively. Then* $\mathscr{E} = \mathscr{E}'$ *if and only if there is an* $r \times r$ *scalar unitary matrix* $U = (u_{ij})$ *such that* $E = UE'$ *where* $E^t = [E_1 \cdots E_r]$ *and* $(E')^t = [E'_1 \cdots E'_r]$. *In other words*,

$$E_i = \sum_{j=1}^{r} u_{ij} E'_j \quad \text{for } 1 \leqslant i \leqslant r.$$

Let $\mathscr{A} = \mathrm{Alg}\{E_i, E_i^\dagger\}$ be the algebra generated by the E_i and $E_i^\dagger$. This is the set of polynomials in the E_i and $E_i^\dagger$. An application of the Cayley–Hamilton theorem on minimal polynomials from linear algebra shows that all such polynomials may be written as polynomials with degree below some global bound. In quantum computing, $\mathscr{A}$ is called the *interaction algebra* for the channel. It is †-closed by definition, hence it is a finite dimensional C*-algebra [3,17,73]. Observe that, as a direct consequence of the previous result, $\mathscr{A}$ can be seen to be a relic of the channel; in other words, it is independent of the choice of noise operators which satisfy (1) for the channel. This is most succinctly seen in the case of unital channels, see Section 6 for details.

Note 4.5. We mention that an interesting and highly active area of current research in quantum information theory revolves around the study of quantum channel capacities. Specifically, there are a number of deep mathematical problems which are concerned with computing the capacity of a quantum channel to carry classical or quantum information. The following references give a starting point into the literature [8,21,34–36,39,40,44,53,58,65,66,79].

Note that the quantum measurement process (postulate (iii)) naturally determines a quantum channel. Let us consider more specific examples. (The final section includes further examples.)

Example 4.6. (i) Let $0 < p < 1$ and define operators on $\mathscr{H}_2$ by

$$E_1 = (\sqrt{1-p})\,\mathbb{1}_2, \quad E_2 = (\sqrt{p})X,$$

with respect to $\{|0\rangle, |1\rangle\}$. The *bit flip* channel $\mathscr{E}(\rho) = E_1\rho E_1^\dagger + E_2\rho E_2^\dagger$ flips the state $|0\rangle$ to $|1\rangle$ and vice versa with probability p. For instance, observe that the projection $|0\rangle\langle 0|$ evolves to the superposition $\mathscr{E}(|0\rangle\langle 0|) = (1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|$.

(ii) Let $E_1 = \frac{\mathbb{1}_2}{2}$ and define a channel by $\mathscr{E}(\rho) = E_1\rho E_1 + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z$. Observe that $\mathscr{E}(\rho) = \frac{\mathbb{1}_2}{2}$ for every density operator $\rho \in \mathscr{M}_2$. This property, distinct density matrices evolving in a channel to the same density matrix, has recently been exploited as part of a scheme for quantum cryptography [5].

(iii) Let $0 < r < 1$ and define operators on $\mathscr{H}_2$ by

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-r} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & \sqrt{r} \\ 0 & 0 \end{pmatrix}.$$

These noise operators define an *amplitude damping* channel $\mathscr{E}(\rho) = E_1\rho E_1^\dagger + E_2\rho E_2^\dagger$. Such channels characterize energy dissipation within a quantum system.

(iv) Let $U_1, \ldots, U_d$ be unitaries which act on a common Hilbert space and let $r_1, \ldots, r_d$ be positive scalars such that $\sum_i r_i = 1$. Then we may define a channel by $\mathscr{E}(\rho) = \sum_{i=1}^d r_i U_i \rho U_i^\dagger$. These are the prototypical examples of 'unital' ($\mathscr{E}(\mathbb{1}) = \mathbb{1}$) channels (see Section 6). In fact, every unital channel on $\mathscr{M}_2$ may be written as a convex sum of unitaries in this way. This is not the case in higher dimensions however.

(v) The class of *entanglement breaking channels* was introduced in [35] and studied in [39]. These are quantum channels which can be written in the form

$$\mathscr{E}(\rho) = \sum_k |\psi_k\rangle\langle\psi_k|\langle\phi_k|\rho|\phi_k\rangle,$$

for some vectors $|\psi_k\rangle$ and $|\phi_k\rangle$. With this representation, trace preservation is equivalent to $\sum_k |\phi_k\rangle\langle\phi_k| = \mathbb{1}$, as $\mathrm{Tr}(\rho|\phi_k\rangle\langle\phi_k|) = \langle\phi_k|\rho|\phi_k\rangle$. Such channels derive their name from the fact that for $d \geqslant 1$, a density operator $\mathscr{E}^{(d)}(\Gamma)$ is never entangled, even if Γ was initially entangled.

5. Quantum error correction

In this section we present the central aspects of the 'standard model' for quantum error detection and correction. For an extensive introduction to the subject we point the reader to the articles [28,47,64]. The general error correction problem in quantum computing is much more delicate when compared to error correction in classical computing. The possible errors that can occur include all possible unitary matrices, whereas in classical computing the only errors are bit flips. Nonetheless, methods have been (and are being) developed for quantum error correction.

5.1. Error detection

Let $\mathscr{H}$ be the Hilbert space for a given quantum system. Then a *quantum code* $\mathscr{C}$ on $\mathscr{H}$ is a subspace of $\mathscr{H}$. Let $P_{\mathscr{C}}$ be the projection of $\mathscr{H}$ onto $\mathscr{C}$. Then $P_{\mathscr{C}}$ and $P_{\mathscr{C}}^\perp$ describe a measurement of the system which can be used to determine if a given

state $|\psi\rangle \in \mathscr{H}$ belongs to the code. The basic idea of an error-detection scheme in this setting is to first prepare an initial state in $\mathscr{C}$, for brevity let us restrict ourselves to unit vectors $|\psi\rangle$ in $\mathscr{C}$. The state $|\psi\rangle\langle\psi|$ is then transmitted through the quantum channel $\mathscr{E}$ of interest, evolving to $\mathscr{E}(|\psi\rangle\langle\psi|)$. Finally, the measurement $P_{\mathscr{C}}$, $P_{\mathscr{C}}^{\perp}$ is performed on this final state. This motivates the following definition.

Definition 5.1. Let $\mathscr{C}$ be a quantum code on $\mathscr{H}$ and let E be an error (noise) operator associated with a given quantum channel on $\mathscr{H}$. Then $\mathscr{C}$ *detects the error* E if the states which are accepted after E acts are unchanged, up to a scaling factor. In other words, there is a scalar λ_E such that

$$P_{\mathscr{C}} E|\psi\rangle = \lambda_E|\psi\rangle \text{ for all } |\psi\rangle \in \mathscr{C}.$$

Observe that the set of error operators E which are detectable for a fixed quantum code $\mathscr{C}$ form a subspace of operators, or a so-called operator space [62]. There are a number of equivalent conditions for detectable errors.

Theorem 5.2. *Let $\mathscr{C}$ be a quantum code and let E be an error operator associated with a given quantum channel. Then the following conditions are equivalent*:

(i) *E is detectable by $\mathscr{C}$, with scaling factor λ_E.*
(ii) $P_{\mathscr{C}} E P_{\mathscr{C}} = \lambda_E P_{\mathscr{C}}$.
(iii) $\langle\psi_1|E|\psi_2\rangle = \lambda_E\langle\psi_1||\psi_2\rangle$ *for all* $|\psi_i\rangle \in \mathscr{C}$, $i = 1, 2$.
(iv) *For every pair of vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ in $\mathscr{C}$ which are orthogonal, the vectors $E|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal.*

Proof. We shall prove the implication (iv) $\Rightarrow$ (iii). The other directions are either trivial or easy to see. We may clearly assume that $\dim \mathscr{C} \geqslant 2$. Let $\{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$ be an orthonormal basis for $\mathscr{C}$. We first claim that (iv) implies

$$\langle\psi_i|E|\psi_i\rangle = \langle\psi_j|E|\psi_j\rangle \text{ for all } i, j. \tag{2}$$

Indeed, to see this, fix i, j and define

$$|+\rangle = |\psi_i\rangle + |\psi_j\rangle \quad \text{and} \quad |-\rangle = |\psi_i\rangle - |\psi_j\rangle.$$

Then by (iv) we have

$$0 = \langle+|E|-\rangle = \langle\psi_i|E|\psi_i\rangle - \langle\psi_j|E|\psi_j\rangle.$$

Thus define $\lambda_E = \langle\psi_i|E|\psi_i\rangle$, and note that this is independent of i. Now let $|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \ldots$ and $|\phi\rangle = \beta_1|\psi_1\rangle + \beta_2|\psi_2\rangle + \cdots$ be vectors in $\mathscr{C}$. Then by (iv) and (2) we have

$$\langle\psi|E|\phi\rangle = \sum_{i,j} \alpha_i\overline{\beta_j}\langle\psi_i|E|\psi_j\rangle = \sum_i \alpha_i\overline{\beta_i}\langle\psi_i|E|\psi_i\rangle = \lambda_E\langle\psi||\phi\rangle,$$

and this completes the proof. □

Let us describe a matrix perspective for detectable errors. This can be seen through a simple example.

Example 5.3. Let $\mathscr{C}$ be the quantum code given by

$$\mathscr{C} = \text{span}\{|000\rangle, |111\rangle\} \subseteq \mathscr{H}_8.$$

The (unnormalized) error operators for the n-qubit depolarizing channel [61,44] are $\mathfrak{E} = \{\mathbb{1}_{2^n}, Z_1, \ldots, Z_n\}$. In the 3-qubit case consider the error operator $E \equiv Z_1$. Observe that $E|000\rangle = |000\rangle$ whereas $E|111\rangle = -|111\rangle$. Thus if E was detectable by $\mathscr{C}$ we would have,

$$\lambda_E = \langle 000|E|000\rangle = 1 \quad \text{and} \quad \lambda_E = \langle 111|E|111\rangle = -1.$$

From this contradiction it follows that none of the depolarizing errors Z_k are detectable by the code $\mathscr{C}$. In fact, from Theorem 5.2 the detectable errors for $\mathscr{C}$ may be realized in matrix form as the operator space $\left\{\begin{pmatrix} \lambda\mathbb{1}_2 & * \\ * & * \end{pmatrix} : \lambda \in \mathbb{C}\right\}$, with respect to an ordered orthonormal basis for $\mathscr{H}_8$ of the form $\{|000\rangle, |111\rangle, \ldots\}$, and where the $*$ entries indicate that any choice is admissible.

More generally, the conditions of Theorem 5.2 show that the detectable errors for a given quantum code $\mathscr{C}$ form the subspace of operators

$$\left\{\begin{pmatrix} \lambda\mathbb{1} & * \\ * & * \end{pmatrix} : \lambda \in \mathbb{C}\right\},$$

where the matrix form is given with respect to the spatial decomposition $\mathscr{H} = P_{\mathscr{C}}\mathscr{H} \oplus P_{\mathscr{C}}^{\perp}\mathscr{H}$.

5.2. Error correction

Let $\mathfrak{E} = \{E_i\}$ be a set of errors that act as noise operators for a given quantum channel. If $\mathscr{C}$ is a quantum code, then the basic error-correction problem for $\mathscr{C}$ is to determine when there is a decoding procedure for $\mathscr{C}$ such that all the errors in $\mathfrak{E}$ are corrected. The simplest possible case occurs when every error E_i is the multiple of a unitary operator and the subspaces $E_i\mathscr{C}$ are mutually orthogonal. The obvious decoding procedure in this situation is to first make a projective measurement to determine which of the subspaces $E_i\mathscr{C}$ a given state $|\psi\rangle \in \mathscr{C}$ has evolved to, then apply the inverse of the error operator E_i. This particular case motivates the following general definition in the standard model for quantum error correction.

Definition 5.4. Let $\mathscr{E}$ be a quantum channel and let $\mathscr{C}$ be a quantum code with projection $P_{\mathscr{C}}$. Then $\mathscr{C}$ is *correctable for* $\mathscr{E}$ if there is a quantum channel $\mathscr{R}$ such that

$$\mathscr{R} \circ \mathscr{E}(\rho) = \rho$$

for all ρ supported on $\mathscr{C}$; that is, all ρ with $\rho = P_{\mathscr{C}}\rho P_{\mathscr{C}}$.

There are a number of useful characterizations of correctable codes. Note that in the proof of (iii) $\Rightarrow$ (i) below, the error correction operation $\mathscr{R}$ is explicitly constructed and hence this gives a constructive approach for decoding within this error correction model.

Theorem 5.5. *Let $\mathscr{E}$ be a quantum channel with errors $\mathfrak{E} = \{E_i\}$ and let $\mathscr{C}$ be a quantum code with projection $P_{\mathscr{C}}$. Then the following conditions are equivalent*:

(i) *$\mathscr{C}$ is correctable for $\mathscr{E}$.*
(ii) *The operators in the set $\mathfrak{E}^\dagger\mathfrak{E} = \{E_1^\dagger E_2 : E_i \in \mathfrak{E}\}$ are detectable by $\mathscr{C}$.*
(iii) *There are scalars $\Lambda = (\lambda_{ij})$ such that*

$$P_{\mathscr{C}} E_i^\dagger E_j P_{\mathscr{C}} = \lambda_{ij} P_{\mathscr{C}} \text{ for all } i, j. \tag{3}$$

(iv) *There is a linear transformation $E_i \mapsto E_i'$ on $\mathfrak{E}$ such that the new error operators E_i' satisfy the following properties*:
  (a) *The subspaces $E_i'\mathscr{C}$ are mutually orthogonal.*
  (b) *The restriction of every E_i' to $\mathscr{C}$ is proportional to a restriction to $\mathscr{C}$ of a unitary operator.*

Proof. Observe that any matrix Λ which satisfies (3) must be positive since this equation may be written as a matrix product $A^\dagger A = (\lambda_{ij} P_{\mathscr{C}})$ where $A = [E_1 P_{\mathscr{C}}\ E_2 P_{\mathscr{C}} \cdots]$ is a row matrix. Conditions (ii) and (iii) are equivalent by definition. We shall prove (i) is necessary and sufficient for (iii) and leave the connection with (iv) for the interested reader.

For (i) $\Rightarrow$ (iii), let $\mathscr{C}$ be a quantum code with code projection $P_{\mathscr{C}}$. Suppose $\mathscr{E}$ is a quantum channel with errors $\{E_i\}$ and that $\mathscr{C}$ is correctable for $\mathscr{E}$ via the error-correction operation $\mathscr{R}$ with noise operators $\{R_j\}$. Define a compressed channel by $\mathscr{E}_{\mathscr{C}}(\rho) \equiv \mathscr{E}(P_{\mathscr{C}} \rho P_{\mathscr{C}})$. Then by hypothesis $\mathscr{R}(\mathscr{E}_{\mathscr{C}}(\rho)) = \mathscr{R}(\mathscr{E}(P_{\mathscr{C}} \rho P_{\mathscr{C}})) = P_{\mathscr{C}} \rho P_{\mathscr{C}}$. In particular,

$$\sum_{i,j} R_j E_i P_{\mathscr{C}} \rho P_{\mathscr{C}} E_i^\dagger R_j^\dagger = P_{\mathscr{C}} \rho P_{\mathscr{C}} \quad \text{for all } \rho.$$

Thus by Proposition 4.4 there are scalars α_{ki} such that

$$R_k E_i P_{\mathscr{C}} = \alpha_{ki} P_{\mathscr{C}} \quad \text{for all } i, k.$$

Hence,

$$P_{\mathscr{C}} E_i^\dagger R_k^\dagger R_k E_j P_{\mathscr{C}} = \overline{\alpha}_{ki} \alpha_{kj} P_{\mathscr{C}} \quad \text{for all } i, j, k. \tag{4}$$

But $\mathscr{R}$ preserves traces, so that $\sum_k R_k^\dagger R_k = \mathbb{1}$, and thus when we sum (4) over k we find

$$P_{\mathscr{C}} E_i^\dagger E_j P_{\mathscr{C}} = \lambda_{ij} P_{\mathscr{C}} \quad \text{for all } i, j,$$

where $\lambda_{ij} = \sum_k \overline{\alpha}_{ki} \alpha_{kj}$.

Conversely, let us assume that $\mathscr{E}$ is a channel with errors $\{E_i\}$ and $\mathscr{C}$ is a code with projection $P_{\mathscr{C}}$ such that (3) holds for a positive scalar matrix $\Lambda = \{\lambda_{ij}\}$. Let U be a unitary operator such that $D = U^\dagger \Lambda U = (d_{kl})$ is diagonal (so that $D = \mathrm{diag}(d_{kk})$). Note that $\sum_k d_{kk} = 1$ by trace preservation of $\mathscr{E}$. By Proposition 4.4 the operators $F_k = \sum_i u_{ik} E_i$ also implement $\mathscr{E}$. A simple computation shows that

$$P_{\mathscr{C}} F_k^\dagger F_l P_{\mathscr{C}} = d_{kl} P_{\mathscr{C}} \quad \text{for all } k, l.$$

The polar decomposition of $F_k P_{\mathscr{C}}$ gives

$$F_k P_{\mathscr{C}} = U_k \sqrt{P_{\mathscr{C}} F_k^\dagger F_k P_{\mathscr{C}}} = \sqrt{d_k} U_k P_{\mathscr{C}}$$

for some unitary U_k. Define projections $P_k \equiv U_k P_{\mathscr{C}} U_k^\dagger$. Then

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P_{\mathscr{C}} F_l^\dagger F_k P_{\mathscr{C}} U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = 0 \quad \text{for } k \neq l,$$

and hence the ranges of the P_k are mutually orthogonal.

Without loss of generality assume that $\sum_k P_k = \mathbb{1}$ (otherwise just add the projection onto the orthogonal complement and define $U_k = \mathbb{1}$). The candidate error-correction operation is defined by

$$\mathscr{R}(\rho) = \sum_k U_k^\dagger P_k \rho P_k U_k.$$

Observe that for all ρ with $\rho = P_{\mathscr{C}} \rho P_{\mathscr{C}}$,

$$\begin{aligned} U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger P_k^\dagger F_l \sqrt{\rho} &= \frac{U_k^\dagger U_k P_{\mathscr{C}} F_k^\dagger F_l P_{\mathscr{C}} \sqrt{\rho}}{\sqrt{d_{kk}}} \\ &= \delta_{kl} \sqrt{d_{kk}} P_{\mathscr{C}} \rho = \delta_{kl} \sqrt{d_{kk}} \rho. \end{aligned}$$

Thus we have

$$\mathscr{R}(\mathscr{E}(\rho)) = \sum_{k,l} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k = \sum_{k,l} \delta_{kl} d_{kk} \rho = \rho$$

for all $\rho = P_{\mathscr{C}} \rho P_{\mathscr{C}}$, and we have proved that (iii) $\Rightarrow$ (i). □

Let us discuss a pair of illustrative applications of Theorem 5.5.

Example 5.6. (i) With $\mathscr{C} = \mathrm{span}\{|000\rangle, |111\rangle\}$ inside $\mathscr{H}_8$ as in Example 5.3, it is easy to see that $\mathscr{C}$ satisfies (3) for the errors $\mathscr{E} = \{\mathbb{1}, X_1, X_2, X_3\}$. Let P_0 be the projection onto $\mathscr{C}$, let P_1 be the projection onto the subspace $X_1\mathscr{C} = \mathrm{span}\{|100\rangle, |011\rangle\}$ and similarly define projections P_2 and P_3. Then the correction operation given by the proof above is $\mathscr{R} = \{P_0, X_1 P_1, X_2 P_2, X_3 P_3\}$.

(ii) Shor's 9-qubit code [69] is defined by two orthonormal vectors in $\mathscr{H}_{2^9}$ given by

$$|0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}},$$

$$|1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

Let $\mathscr{C} = \text{span}\{|0_L\rangle, |1_L\rangle\}$. Given $1 \leqslant k \leqslant 9$, the code $\mathscr{C}$ is correctable for the errors $\{X_k, Y_k, Z_k\}$ as (3) is satisfied for this triple. Let $P_{x,k}$ be the projection onto the subspace $X_k\mathscr{C}$ and similarly define projections $P_{y,k}$ and $P_{z,k}$. Then the correction operation given by the theorem is $\mathscr{R} = \{X_k P_{x,k},\ Y_k P_{y,k},\ Z_k P_{z,k}\}$.

Since the Pauli matrices, together with the identity operator $\mathbb{1}_2$, form a linear basis for $\mathscr{M}_2$ that is closed under multiplication up to scalar multiples, it follows that $\mathscr{C}$ is correctable for any set of errors $\mathfrak{E}$ which act on one of the nine possible qubits. (In fact the Shor code also corrects for errors on multiple qubits [61].)

Note 5.7. The quantum error correction conditions of Theorems 5.2 and 5.5 were established independently by Bennett et al. [9] and Knill and Laflamme [50]. As a collection of entry point references for particular methods of quantum error correction we mention [14,29,30,45,46,49,54,68,71,83].

6. Noiseless subsystems via the noise commutant

In this section we describe a specific method of passive quantum error correction, by which we mean no active intervention is required after information is encoded. The basic idea in a 'noiseless subsystem method' of error correction, classical or quantum, is to encode information on subsystems of the system of interest in such a way that it remains immune to the effects of the channel that the information is evolving through. Let $\mathscr{E} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})$ be a quantum channel with noise operators $\{E_i\}$ and interaction algebra $\mathscr{A} = \text{Alg}\{E_i, E_i^\dagger\}$. Recall that $\mathscr{E}$ is *unital* if $\mathscr{E}(\mathbb{1}) = \sum_i E_i E_i^\dagger = \mathbb{1}$. The *noise commutant* for $\mathscr{E}$ is the †-algebra

$$\begin{aligned}\mathscr{A}' &= \{\rho \in \mathscr{B}(\mathscr{H}) : \rho A = A\rho \text{ for } A \in \mathscr{A}\} \\ &= \{\rho \in \mathscr{B}(\mathscr{H}) : [\rho, E_i] = 0 = [\rho, E_i^\dagger] \text{ for } i = 1, \ldots, n\}.\end{aligned}$$

The procedure in the *noiseless subsystem via noise commutant* method of quantum error correction [23,26,32,47,48,57,81,82] is to use the structure of $\mathscr{A}'$ to produce noiseless subsystems (which are also called 'decoherence-free subspaces' in special cases, see Remark 6.3).

The illustrations of this method that appear in the literature all involve unital channels. The following discussion shows why this is the case. Let $\text{Fix}(\mathscr{E}) = \{\rho \in \mathscr{B}(\mathscr{H}) : \mathscr{E}(\rho) = \rho\}$. Observe that $\text{Fix}(\mathscr{E})$ is a †-closed subspace of $\mathscr{B}(\mathscr{H})$. Now consider a unital channel $\mathscr{E}$. Let ρ belong to $\mathscr{A}'$. Then $\rho E_i = E_i \rho$ for all i and hence

$$\mathscr{E}(\rho) = \sum_i E_i \rho E_i^\dagger = \rho \mathscr{E}(\mathbb{1}) = \rho.$$

Thus ρ belongs to $\mathrm{Fix}(\mathscr{E})$. The converse inclusion was proved independently in [13] and [55] (see also [32] for another proof and [2] for the infinite dimensional extension): The set $\mathrm{Fix}(\mathscr{E})$ coincides with the noise commutant in the case of a unital channel. In fact, it is not hard to show that the identity $\mathrm{Fix}(\mathscr{E}) = \mathscr{A}'$ characterizes unital channels. Thus, by building on the proofs from [13,32,55] we may state the following.

Theorem 6.1. *Let $\mathscr{E}$ be a quantum channel. Then $\mathrm{Fix}(\mathscr{E}) = \mathscr{A}'$ if and only if $\mathscr{E}$ is unital. Moreover, in this case $\mathscr{A}$ is equal to the algebra $\mathscr{A}_0$ generated by the E_i. In other words, the operators $E_i^\dagger$ belong to $\mathscr{A}_0$.*

Note 6.2. Notice how the algebra $\mathscr{A} = (\mathscr{A})'' = \mathrm{Fix}(\mathscr{E})'$ is a relic of the channel in the unital case (see the discussion after Proposition 4.4).

Remark 6.3. In the case of unital channels, Theorem 6.1 shows that the noiseless subsystem via noise commutant method can be presented as follows: Let $\mathscr{E}$ be a unital quantum channel. Then the interaction algebra $\mathscr{A}$ is generated by the E_i and $\mathscr{A}' = \mathrm{Fix}(\mathscr{E})$ is a finite dimensional C*-algebra. As such, $\mathscr{A}'$ is unitarily equivalent to a unique direct sum of ampliated full matrix algebras, $\mathscr{A}' \cong \oplus_k (\mathbb{1}_{m_k} \otimes \mathscr{M}_{n_k})$. Hence, a density operator ρ that encodes the initial states of a quantum system will be immune to the noise of the channel as it evolves through, $\mathscr{E}(\rho) = \rho$, provided that ρ is initially prepared on one of the ampliated matrix blocks $\mathbb{1}_{m_k} \otimes \mathscr{M}_{n_k}$ inside the noise commutant $\mathscr{A}' = \mathrm{Fix}(\mathscr{E})$. The decoherence-free subspace method may be regarded as the special case of this method that occurs when matrix blocks $\mathbb{1}_{m_k} \otimes \mathscr{M}_{n_k}$ with $m_k = 1$ are utilized.

In the case of a general quantum channel, however, the full structure of $\mathscr{A}'$ cannot be used for error correction. This can be seen most dramatically in the following simple case.

Proposition 6.4. *Let $\mathscr{E}$ be a completely positive map such that $A_\mathscr{E} \equiv \mathscr{E}(\mathbb{1})$ is not invertible. Let $P_\mathscr{E}$ be the projection onto the subspace $\mathscr{H}_\mathscr{E} \equiv \mathrm{Ran}(A_\mathscr{E})$. Suppose that $E_i = P_\mathscr{E} E_i P_\mathscr{E}$ for all i. Then $\mathscr{H}_\mathscr{E}^\perp$ is non-zero and every operator $\rho \in \mathscr{B}(\mathscr{H}_\mathscr{E}^\perp)$ belongs to $\mathscr{A}'$ and satisfies $\mathscr{E}(\rho) = 0$.*

Proof. The non-invertibility of $A_\mathscr{E}$ implies $\mathscr{H}_\mathscr{E}^\perp$ is non-zero. Let $\rho \geqslant 0$ belong to $\mathscr{B}(\mathscr{H}_\mathscr{E}^\perp)$, by which we mean ρ acts on $\mathscr{H}$ with $\rho = P_\mathscr{E}^\perp \rho P_\mathscr{E}^\perp$. Then ρ trivially belongs to $\mathscr{A}'$ since $\rho E_i = 0 = E_i \rho$ for all i. Further, $\mathscr{E}(\rho) = \mathscr{E}(P_\mathscr{E}^\perp \rho) = 0$. □

Remark 6.5. It would be interesting to know if the noise commutant can be used to produce noiseless subsystems for classes of non-unital channels. For instance, a natural generalization of unital channels is the class of channels for which the identity evolves to a multiple of a projection. Notice that if $\mathscr{E}(\mathbb{1}_\mathscr{H}) = mP$ for some

projection P, then m divides the dimension of $\mathscr{H}$ by trace preservation of $\mathscr{E}$. A simple example of this phenomena is given by the channel $\mathscr{E}$ with noise operators $A_i = |0\rangle\langle i|$ for $1 \leqslant i \leqslant \dim \mathscr{H} \equiv d$. Trace preservation of $\mathscr{E}$ may be readily verified, and in this case

$$\mathscr{E}(\mathbb{1}_d) = \sum_{i=1}^{d} A_i A_i^\dagger = \sum_{i=1}^{d} (|0\rangle\langle i|)(|i\rangle\langle 0|) = d|0\rangle\langle 0|.$$

Note 6.6. There are a number of other quantum error correction schemes that have been investigated and some of these will be of interest to operator researchers (see [1,23,25,43,54,57,80–82]).

We finish by considering noiseless subsystems for some special cases of unital channels.

Example 6.7. (i) Let $0 < p < 1$ and let E_1, E_2 be operators on $\mathscr{H}_2$ defined on the standard basis by $E_1 = (\sqrt{1-p})\mathbb{1}_2$ and $E_2 = (\sqrt{p})Z$. Then E_1 and E_2 are the noise operators for a unital channel $\mathscr{E}$ on $\mathscr{M}_2$ which is a variant on the bit flip channel discussed earlier. The quantum operation corresponding to this channel is equivalent to the *phase flip* or *phase damping* operation on single qubits [61]. It is so named because, for instance, $\mathscr{E}(|+\rangle\langle +|) = (1-p)|+\rangle\langle +| + p|-\rangle\langle -|$ and hence $\mathscr{E}$ flips the phase of $|+\rangle\langle +|$ and $|-\rangle\langle -|$ with probability p. It is easy to see in this case that

$$\begin{aligned}\mathrm{Fix}(\Phi) = \mathscr{A}' &= \{E_1, E_2\}' \\ &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{C} \right\} \cong \mathbb{C}\mathbf{1} \oplus \mathbb{C}\mathbf{1},\end{aligned}$$

and hence this channel has no non-trivial noiseless subsystems.

(ii) Let $0 < p < 1$ and let E_1, E_2 be operators on $\mathscr{H}_4$ defined on the standard basis by $E_1 = \sqrt{1-p}(\mathbb{1}_2 \otimes \mathbb{1}_2)$ and $E_2 = \sqrt{p}(Z \otimes Z)$. These noise operators determine a unital channel $\mathscr{E}$ on $\mathscr{M}_4$ which can be regarded as an ampliation of the phase flip channel. Compute

$$\begin{aligned}\mathrm{Fix}(\Phi) = \mathscr{A}' &= \{E_1, E_2\}' \\ &= \left\{ \begin{pmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ a_{41} & 0 & 0 & a_{44} \end{pmatrix} : a_{ij} \in \mathbb{C} \right\}.\end{aligned}$$

Thus $\mathscr{A}'$ is unitarily equivalent to the direct sum $\mathscr{A}' \cong \mathscr{M}_2 \oplus \mathscr{M}_2$ and there is a pair of 2-dimensional noiseless subsystems.

(iii) More generally, let $E_1 = U_1, \ldots, E_d = U_d$ be unitaries on a Hilbert space $\mathscr{H}$. If we are given scalars λ_i such that $\sum_i |\lambda_i|^2 = 1$, then the operators $\lambda_i E_i$ are the

noise operators for a unital channel $\mathscr{E}$ with $\mathrm{Fix}(\mathscr{E}) = \mathscr{A}' = \{U_1, \ldots, U_d\}'$. In this case the automatic self-adjointness of $\mathscr{A}$ can be seen directly through an application of the Cayley–Hamilton theorem. (The algebra generated by any unitary U can be seen to include $U^\dagger$ via minimal polynomial considerations.)

(iv) An important special case of such channels is the class of 'collective rotation channels' [6,10,25,26,32,43,48,74,75,76,80,81]. The n-qubit example has noise operators given by weighted exponentiations of the operators $J_k = \sum_{m=1}^{n} J_k^{(m)}$ for $k = x, y, z$, where $J_k^{(1)} = \sigma_k \otimes (\mathbb{1}_2)^{\otimes(n-1)}$, etc. There is an abundance of noiseless subsystems for these channels and they can be computed directly [33] or through combinatorial techniques discussed below.

(v) A generalization of the collective rotation class is presented in [42] and noiseless subsystems for this class of 'universal collective rotation (ucr) channels' are computed using Young tableaux combinatorics. For each pair of positive integers $d, n \geqslant 2$ there is a family of such channels with the case $d = 2$ yielding the class from (iv). It is proved in [42] that every ucr-channel possesses an abundance of noiseless subsystems. In fact, it is shown that the noise commutant for every channel in this class (for fixed d and n) contains the algebra $\mathscr{A}_\pi = \mathrm{Alg}\{\pi(\sigma) : \sigma \in S_n\}$ where S_n is the symmetric group on n letters and $\pi : S_n \to \mathscr{U}(d^n)$ is the unitary representation of S_n on $\mathscr{H}_{d^n}$ given by

$$\pi(\sigma)(h_1 \otimes \cdots \otimes h_n) = h_{\sigma(1)} \otimes \cdots \otimes h_{\sigma(n)},$$

for all $h_1, \ldots, h_n \in \mathscr{H}_d$ and $\sigma \in S_n$. In particular, the Young tableaux machine can be used to explicitly compute the structure of $\mathscr{A}_\pi$ and identify noiseless subsystems for the corresponding ucr-channel. Further, a recent paper of Bacon et al. [4], has shown that the change of basis transformation from the standard basis to the Young tableaux basis can be implemented efficiently with a quantum algorithm.

Acknowledgments

I am grateful to the referees for helpful comments. I would like to thank all the participants in the Quantum Information Theory Learning Seminar organized by the author and John Holbrook at the University of Guelph during the fall of 2003. I am also grateful for enlightening conversations with Daniel Gottesman, John Holbrook, Peter Kim, Raymond Laflamme, Michele Mosca, Ashwin Nayak, Eric Poisson, David Poulin, Martin Roetteler, Jean-Pierre Schoch, Robert Spekkens and Paolo Zanardi. Support from NSERC, the University of Guelph, the Institute for Quantum Computing and the Perimeter Institute is kindly acknowledged.

References

[1] D. Aharonov, M. Ben-Or, Fault-tolerant quantum computation with constant error, in: Proc. 29th. Ann. ACM Symp. on Theory of Computing, New York, ACM, 1998, p. 176. Available from: <arxiv.org/quant-ph/9906129, quant-ph/9611025>.

[2] A. Arias, A. Gheondea, S. Gudder, Fixed points of quantum operations, J. Math. Phys. 43 (2002) 5872–5881.
[3] W. Arveson, An invitation to C*-algebras, Graduate Texts in Mathematics, No. 39, Springer-Verlag, New York–Heidelberg, 1976.
[4] D. Bacon, I.L. Chuang, A.W. Harrow, Efficient quantum circuits for Schur and Clebsch–Gordon transforms. Available from: <arxiv.org/quant-ph/0407082>.
[5] S.D. Bartlett, T. Rudolph, R.W. Spekkens, Decoherence-full subsystems and the cryptographic power of a private shared reference frame, Phys. Rev. A 70 (2004) 032307.
[6] S.D. Bartlett, T. Rudolph, R.W. Spekkens, Classical and quantum communication without a shared reference frame, Phys. Rev. Lett. 91 (2003) 027901.
[7] M. Batty, S.L. Braunstein, A.J. Duncan, S. Rees, Quantum algorithms in group theory. Available from: <arxiv.org/quant-ph/0310133>.
[8] C.H. Bennett, P.W. Shor, J.A. Smolin, A.V. Thapliyal, Entanglement-assisted classical capacity of noisy quantum channels, Phys. Rev. Lett. 83 (1999) 3081.
[9] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wooters, Mixed state entanglement and quantum error correction, Phys. Rev. Lett. 78 (1996) 3824.
[10] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, R.W. Spekkens, Robust polarization-based quantum key distribution over collective-noise channel, Phys. Rev. Lett. 92 (2004) 17901.
[11] G. Brassard, P. Hoyer, M. Mosca, A. Tapp, Quantum amplitude amplification and estimation, Quantum Computation and Information, Washington, DC, 2000, Contemp. Math., vol. 305, Amer. Math. Soc., Providence, RI, 2002, pp. 53–74.
[12] M. Brooks (Ed.), Quantum Computing and Communications, Springer-Verlag, London, 1999.
[13] P. Busch, J. Singh, Luders theorem for unsharp quantum effects, Phys. Lett. A 249 (1998) 10–24.
[14] J.I. Cirac, T. Pellizzari, P. Zoller, Enforcing coherent evolution in dissipative quantum dynamics, Science 273 (1996) 1207.
[15] M.D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Appl. 10 (1975) 285–290.
[16] C. Cohen-Tannoudji, B. Diu, F. Laloe, Quantum Mechanics, Volume One & Two, John Wiley & Sons, Toronto, 1977.
[17] K.R. Davidson, C*-algebras by example, Fields Institute Monographs, vol. 6, Amer. Math. Soc., Providence, 1996.
[19] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, Proc. R. Soc. Lond. A 400 (1985) 97–117.
[20] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proc. R. Soc. Lond. A 459 (1992) 553–558.
[21] I. Devetak, P. Shor, The capacity of a quantum channel for simultaneous transmission of classical and quantum information. Available from: <arxiv.org/quant-ph/0311131>.
[23] L.-M. Duan, G.-C. Guo, Preserving coherence in quantum computation by pairing quantum bits, Phys. Rev. Lett. 79 (1997) 1953.
[24] R. Feynman, Simulating physics with computers, Int. J. Theor. Phys. 21 (1982) 467–488.
[25] S. De Filippo, Quantum computation using decoherence-free states of the physical operator algebra, Phys. Rev. A 62 (2000) 052307.
[26] E.M. Fortunato, L. Viola, M.A. Pravia, E. Knill, R. Laflamme, T.F. Havel, D.G. Cory, Exploring noiseless subsystems via nuclear magnetic resonance, Phys. Rev. A 67 (2003) 062303.
[27] A. Galindo, M.A. Martin-Delgado, Information and computation: classical and quantum aspects, Rev. Mod. Phys. 74 (2002) 347–423.
[28] D. Gottesman, An introduction to quantum error correction, in: S.J. Lomonaco Jr. (Ed.), Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millenium, American Mathematical Society, Providence, RI, 2002, 221–235, Available from: <arxiv.org/quant-ph/0004072>.

[29] D. Gottesman, Stabilizer codes and quantum error correction, PhD thesis, California Institute of Technology, 1997.
[30] D. Gottesman, Class of quantum error correcting codes saturating the quantum Hamming bound, Phys. Rev. A 54 (1996) 1862.
[31] L.K. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th ACM Symp. Theory of Computing, 1996, pp. 212–219.
[32] J.A. Holbrook, D.W. Kribs, R. Laflamme, Noiseless subsystems and the structure of the commutant in quantum error correction, Quantum Inf. Proc. 2 (2004) 381–419.
[33] J.A. Holbrook, D.W. Kribs, R. Laflamme, D. Poulin, Noiseless subsystems for collective rotation channels in quantum information theory, Integral Equations Operator Theory, in press.
[34] A.S. Holevo, R.F. Werner, Counterexample to an additivity conjecture for output purity of quantum channels, Quantum Information Theory, J. Math. Phys. 43 (2002) 4353.
[35] A.S. Holevo, Coding theorems for quantum channels, Rev. Math. Phys. 53 (1999) 1295–1331.
[36] A.S. Holevo, The capacity of the quantum channel with general signal states, IEEE Trans. Inform. Theory 44 (1998) 269–273.
[37] A.S. Holevo, Problems in the mathematical theory of quantum communication channels, Rep. Math. Phys. 12 (1977) 273–278.
[38] A.S. Holevo, On the mathematical theory of quantum communication channels, (Russian) Problemy Peredachi Informacii 8 (1972) 62–71.
[39] M. Horodecki, P. Shor, M.B. Ruskai, Entanglement breaking channels, Rev. Math. Phys. 15 (2003) 629–641.
[40] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, B. Terhal, Classical capacity of a noiseless quantum channel assisted by noisy entanglement, Quantum Inform. and Comput. 1 (2001) 70–78.
[41] G. Johnson, A Shortcut Through Time: The Path to the Quantum Computer, Alfred A. Knopf, New York, 2003.
[42] M. Junge, P. Kim, D.W. Kribs, Universal collective rotation channels and quantum error correction, J. Math. Phys., in press.
[43] J. Kempe, D. Bacon, D.A. Lidar, K.B. Whaley, Theory of decoherence-free fault-tolerant universal quantum computation, Phys. Rev. A 63 (2001) 042307.
[44] C. King, The capacity of the quantum depolarizing channel, IEEE Trans. Inform. Theory 49 (2003) 221–229.
[45] A.Y. Kitaev, Quantum error correction with imperfect gates, in: O. Hirota et al. (Eds.), Quantum Communication and Computing and Measurement, New York, 1997.
[46] A.Y. Kitaev, Quantum computations: algorithms and error correction, Russ. Math. Surv. 52 (1997) 1191–1249.
[47] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W.H. Zurek, Introduction to Quantum Error Correction, Los Alamos Science, November 27, 2002.
[48] E. Knill, R. Laflamme, L. Viola, Theory of quantum error correction for general noise, Phys. Rev. Lett. 84 (2000) 2525–2528.
[49] E. Knill, R. Laflamme, W.H. Zurek, Resilient quantum computation: error models and thresholds, Science 279 (1998) 342–345.
[50] E. Knill, R. Laflamme, A theory of quantum error-correcting codes, Phys. Rev. A 55 (1997) 900.
[51] K. Kraus, States, Effects and Operations: Fundamental Notions of Quantum Theory, Lecture Notes in Physics, vol. 190, Springer-Verlag, Berlin, 1983.
[52] K. Kraus, General state changes in quantum theory, Ann. Phys. 64 (1971) 311–335.
[53] D. Kretschmann, R.F. Werner, Tema con variazioni: quantum channel capacity, New J. Phys. 6 (2004) 26.
[54] D.W. Kribs, R. Laflamme, D. Poulin, A unified and generalized approach to quantum error correction, Preprint.
[55] D.W. Kribs, Quantum channels, wavelets, dilations, and representations of $\mathcal{O}_n$, Proc. Edin. Math. Soc. 46 (2003).

[56] D.W. Leung, Choi's proof and quantum process tomography, J. Math. Phys. 44 (2003) 528–533.
[57] D.A. Lidar, I.L. Chuang, K.B. Whaley, Decoherence free subspaces for quantum computation, Phys. Rev. Lett. 81 (1998) 2594.
[58] S. Lloyd, The capacity of a noisy quantum channel, Phys. Rev. A 55 (1997) 1613.
[59] M. Mosca, C. Zalka, Exact quantum Fourier transforms and discrete logarithm algorithms. Available from: <arxiv.org/0301093>.
[60] M.A. Nielsen, Rules for a complex quantum world, Scientific American, November 2002.
[61] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[62] V. Paulsen, Completely bounded maps and dilations, Pitman Res. Notes Math., vol. 146, Longman Sci. Tech., Harlow, 1986.
[63] V. Paulsen, Completely Bounded Maps and Operator Algebras, Cambridge University Press, Cambridge, UK, 2002.
[64] J. Preskill, Reliable quantum computers, Proc. R. Soc. Lond. A 454 (1998) 385–410.
[65] B. Schumacher, M.D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev. A 56 (1997) 131–138.
[66] P.W. Shor, Equivalence of additivity questions in quantum information theory, Commun. Math. Phys. 246 (2004) 453–472.
[67] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484–1509.
[68] P.W. Shor, Fault-tolerant quantum communication, in: Proceedings of 37th Annual Symposium on Fundamentals of Computer Science, IEEE Press, 1996, pp. 56–65.
[69] P.W. Shor, Scheme for reducing decoherence in quantum computing memory, Phys. Rev. A 52 (1995) 2493.
[70] P.W. Shor, Algorithms for quantum computation: discrete logs and factoring, in: Proceedings of the 35th Symposium on the Foundations of Computer Science, 1994, pp. 124–134.
[71] A.M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. 77 (1996) 793.
[72] W.F. Stinespring, Positive functions on C^*-algebras, Proc. Amer. Math. Soc. 6 (1955) 211–216.
[73] M. Takesaki, Theory of Operator Algebras I, Springer-Verlag, New York–Heidelberg, 1979.
[74] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, D.G. Cory, Experimental realization of noiseless subsystems for quantum information processing, Science 293 (2001) 2059.
[75] L. Viola, E. Knill, R. Laflamme, Constructing qubits in physical systems, J. Phys. A 34 (2001) 7067.
[76] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, D.G. Cory, Experimental realization of noiseless subsystems for quantum information processing, Science 293 (2001) 2059.
[77] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton University Press, Princeton, 1955.
[78] J. Watrous, Quantum algorithms for solvable groups, in: Proceedings of the 33rd ACM Symposium on the Theory of Computing, 2001, pp. 60–67.
[79] A. Winter, Quantum and classical message identification via quantum channels. Available from: <arxiv.org/0401060>.
[80] P. Zanardi, S. Lloyd, Topological protection and quantum noiseless subsystems, Phys. Rev. Lett. 90 (2003) 067902.
[81] P. Zanardi, Stabilizing quantum information, Phys. Rev. A 63 (2001) 012301.
[82] P. Zanardi, M. Rasetti, Noiseless quantum codes, Phys. Rev. Lett. 79 (1997) 3306.
[83] W.H. Zurek, R. Laflamme, Quantum logical operations on encoded qubits, Phys. Rev. Lett. 77 (1996) 4683–4686.