The multiplicative domain in quantum error correction

2009 J. Phys. A: Math. Theor. 42 245303

(http://iopscience.iop.org/1751-8121/42/24/245303)

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **42** (2009) 245303 (15pp) doi:10.1088/1751-8113/42/24/245303

The multiplicative domain in quantum error correction

Man-Duen Choi[1], **Nathaniel Johnston**[2] **and David W Kribs**[2,3]

[1] Department of Mathematics, University of Toronto, ON M5S 3G3, Canada
[2] Department of Mathematics & Statistics, University of Guelph, Guelph, ON N1G 2W1, Canada
[3] Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Received 3 November 2008, in final form 3 March 2009
Published 28 May 2009
Online at stacks.iop.org/JPhysA/42/245303

Abstract

We show that the multiplicative domain of a completely positive map yields a new class of quantum error correcting codes. In the case of a unital quantum channel, these are precisely the codes that do not require a measurement as part of the recovery process, the so-called unitarily correctable codes. In the arbitrary, not necessarily unital case, they form a proper subset of unitarily correctable codes that can be computed from the properties of the channel. As part of the analysis, we derive a representation theoretic characterization of subsystem codes. We also present a number of illustrative examples.

PACS numbers: 03.67.Pp, 03.67.Hk, 03.67.Lx

1. Introduction and preliminaries

Quantum error correction lies at the heart of many investigations in quantum information science [1–3]. As theoretical and experimental efforts become more ramified, and in particular as attempts are made to bring the two perspectives closer together, the need grows for techniques that can identify error correcting codes for wider classes of noise models. Indeed, whereas many approaches to quantum error correction rely on special features of the noise operators under consideration, such as the stabilizer formalism [4] and group theoretic properties of Pauli operators for instance, in the general setting of Hamiltonian-driven noise descriptions an arbitrary noise model will in general have no tractable algebraic properties. Recent work in quantum error correction has thus included considerable effort toward the goal of identifying quantum codes for ever wider classes of noise models. See [5–17] and the references therein for a variety of results, discussions and analysis.

In this paper, we contribute to this line of investigation by showing that the multiplicative domain of a completely positive map yields a new class of quantum error correcting codes. Interestingly, the multiplicative domain is a notion that was first studied in operator theory over 30 years ago for very different reasons [18, 19]. We show that the multiplicative domain codes form a subclass of what are known as 'unitarily correctable codes' (UCCs) [9, 17, 21]. These are codes that do not require a measurement as part of the recovery process; in other words, they are highly degenerate codes for which a unitary recovery operation can be obtained. The UCC class also includes decoherence-free subspaces and noiseless subsystems [10, 11, 22–28] and other special codes such as unitarily noiseless subsystems [16]. Additionally, our analysis includes a derivation of a representation theoretic description of subspace and subsystem codes that we believe is of independent interest. Specifically, we show that every code can be characterized in the Schrödinger picture for quantum dynamics as a representation up to multiplication by the image of the code projection. This complements other recently obtained descriptions of subsystem codes [9, 11, 35, 36].

Before moving to the core of the paper, we briefly present our notation and nomenclature.

For our purposes, $\mathcal{H}$ will be a finite-dimensional Hilbert space, $\mathcal{L}(\mathcal{H})$ is the set of linear operators on $\mathcal{H}$ and $\mathcal{L}_1(\mathcal{H})$ denotes the set of trace class operators. The latter two sets of operators are isomorphic in the finite-dimensional case, and so we will use this identification when convenient. In the Schrödinger picture for quantum dynamics, a *quantum channel* is a completely positive (CP) trace-preserving map $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$, for which a family of operators $\mathcal{E} \equiv \{E_i\}$ can be found with $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ for all $\rho \in \mathcal{L}_1(\mathcal{H})$ and $\sum_i E_i^\dagger E_i = I$. (Here, we use $E^\dagger$ for the operator adjoint or conjugate transpose for matrices.) On the other hand, evolution in the Heisenberg picture is described by the dual map $\mathcal{E}^\dagger : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ defined via $\mathrm{Tr}(\mathcal{E}(\rho)X) = \mathrm{Tr}(\rho\mathcal{E}^\dagger(X))$. Observe that $\mathcal{E} \equiv \{E_i\}$ if and only if $\mathcal{E}^\dagger \equiv \left\{E_i^\dagger\right\}$, and $\mathcal{E}$ is trace preserving if and only if $\mathcal{E}^\dagger$ is unital ($\mathcal{E}^\dagger(I) = I$).

Standard quantum error correction considers quantum codes as subspaces $\mathcal{C} \subseteq \mathcal{H}$ [4, 29–31]. The code $\mathcal{C}$ is said to be *correctable* for $\mathcal{E}$ if there is a channel $\mathcal{R} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ such that $\mathcal{R} \circ \mathcal{E} \circ \mathcal{P}_\mathcal{C} = \mathcal{P}_\mathcal{C}$, where $\mathcal{P}_\mathcal{C}(\rho) = P_\mathcal{C} \rho P_\mathcal{C}$ and $P_\mathcal{C}$ is the orthogonal projection of $\mathcal{H}$ onto $\mathcal{C}$. Given $\mathcal{E} \equiv \{E_i\}$, the Knill–Laflamme theorem [32] shows that $\mathcal{C}$ is correctable for $\mathcal{E}$ if and only if there is a complex matrix $\Lambda = (\lambda_{ij})$ such that $P_\mathcal{C} E_i^\dagger E_j P_\mathcal{C} = \lambda_{ij} P_\mathcal{C}$ for all i, j. Observe that the matrix Λ is necessarily a density matrix, i.e. positive with trace equal to 1.

A generalization called 'operator quantum error correction' [5, 21] leads to the notion of *subsystem codes* [6, 8, 12, 13]. Two Hilbert spaces $\mathcal{A}, \mathcal{B}$ are *subsystems* of $\mathcal{H}$ when $\mathcal{H}$ decomposes as $\mathcal{H} = \mathcal{C} \oplus \mathcal{C}^\perp$ with $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$. Notationally, we shall write $\rho_\mathcal{A}$ for operators in $\mathcal{L}_1(\mathcal{A})$, etc. A subsystem $\mathcal{B}$ is *correctable* for $\mathcal{E}$ if there is a channel $\mathcal{R} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ and a channel $\mathcal{F}_\mathcal{A} : \mathcal{L}_1(\mathcal{A}) \to \mathcal{L}_1(\mathcal{A})$ such that $\mathcal{R} \circ \mathcal{E} \circ \mathcal{P}_\mathcal{C} = (\mathcal{F}_\mathcal{A} \otimes \mathrm{id}_\mathcal{B}) \circ \mathcal{P}_\mathcal{C}$. An extension of the Knill–Laflamme theorem to subsystems [5, 21, 33] shows that $\mathcal{B}$ is correctable for $\mathcal{E}$ if and only if there are operators $F_{ij} \in \mathcal{L}(\mathcal{A})$ such that $P_\mathcal{C} E_i^\dagger E_j P_\mathcal{C} = (F_{ij} \otimes I_\mathcal{B}) P_\mathcal{C}$, where $I_\mathcal{B}$ is the identity operator on $\mathcal{B}$. This is equivalent to the existence of a CP map $\mathcal{F}_\mathcal{A}$ such that $\mathcal{P}_\mathcal{C} \circ \mathcal{E}^\dagger \circ \mathcal{E} \circ \mathcal{P}_\mathcal{C} = (\mathcal{F}_\mathcal{A} \otimes \mathrm{id}_\mathcal{B}) \circ \mathcal{P}_\mathcal{C}$. As a notational convenience, given operators $X \in \mathcal{L}(\mathcal{A})$ and $Y \in \mathcal{L}(\mathcal{B})$, we will write $X \otimes Y$ for the operator on $\mathcal{H}$ given by $(X \otimes Y) \oplus 0_{\mathcal{C}^\perp}$.

It is often convenient in quantum information to work in an operator algebraic setting. For our purposes, an *operator algebra* $\mathfrak{A}$ will refer to a finite-dimensional $*$-algebra [34], that is, a set of operators inside $\mathcal{L}(\mathcal{H})$ that is closed under taking linear combinations, multiplication and adjoints. Every algebra $\mathfrak{A} \subseteq \mathcal{L}(\mathcal{H})$ induces an orthogonal direct sum decomposition of the Hilbert space $\mathcal{H} = \oplus_k (\mathcal{A}_k \otimes \mathcal{B}_k) \oplus \mathcal{K}$ such that the algebra $\mathfrak{A}$ consists of all operators belonging to the set

$$\mathfrak{A} = \oplus_k (I_{\mathcal{A}_k} \otimes \mathcal{L}(\mathcal{B}_k)) \oplus 0_\mathcal{K}, \tag{1}$$

where $0_\mathcal{K}$ is the zero operator on $\mathcal{K}$.

2. Representation theoretic description of subsystem codes

Suppose that $\mathfrak{A}$ is an operator algebra on a Hilbert space $\mathcal{H}$. By a *representation* or a $*$-*homomorphism* of $\mathfrak{A}$, we mean a linear map $\pi : \mathfrak{A} \to \mathcal{L}(\mathcal{H})$ that is multiplicative and preserves the adjoint operation:

$$\pi(ab) = \pi(a)\pi(b) \qquad \forall\, a, b \in \mathfrak{A}$$
$$\pi(a^\dagger) = \pi(a)^\dagger \qquad \forall\, a \in \mathfrak{A}.$$

Every representation π of $\mathfrak{A} = 1_n \otimes \mathcal{L}(\mathcal{H})$, where $\mathcal{H}$ is finite dimensional, has a very special form [34]: there is a positive integer m and a unitary U from $\mathcal{H}^{\otimes m}$ into the range Hilbert space for π such that

$$\pi(1_n \otimes X) = U(1_m \otimes X)U^\dagger \qquad \forall\, X \in \mathcal{L}(\mathcal{H}). \tag{2}$$

We shall refer to the integer m as the *multiplicity* of the representation π. In what follows, we will apply this representation theory to the algebras $\mathcal{L}_1(\mathcal{C})$ and $\mathfrak{A}_\mathcal{B} := 1_\mathcal{A} \otimes \mathcal{L}_1(\mathcal{B})$.

2.1. Subspace codes

The following results are subsumed by the results of the subsequent subsection, but we feel that the presentation is enhanced by deriving the subspace case first since it can be proved in a more elementary fashion. We begin with a refinement of the Knill–Laflamme theorem that will be useful for our purposes.

Lemma 1. *Let $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ be a quantum channel and $\mathcal{C} \subseteq \mathcal{H}$ be a subspace. Then $\mathcal{C}$ is correctable for $\mathcal{E}$ if and only if there is a mixed unitary channel $\mathcal{F} \equiv \{\sqrt{p_i}U_i\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{L}_1(\mathcal{C})$ and $P_\mathcal{C} U_i^\dagger U_j P_\mathcal{C} = 0$ for all $i \neq j$.*

Proof. The code matrix $\Lambda = (\lambda_{ij})$ for $\mathcal{C}$ and $\mathcal{E} \equiv \{E_j\}$ is a density matrix, and thus there is a unitary matrix $U = (u_{ij})$ such that $U\Lambda U^\dagger$ is diagonal (call this diagonal matrix $D = (d_{ij})$). Define a map $\mathcal{F} \equiv \{F_i\}$ where

$$F_i = \sum_j \overline{u_{ij}} E_j.$$

Note that $\mathcal{E} = \mathcal{F}$. Furthermore, for all i, j, it is the case that

$$P_\mathcal{C} F_i^\dagger F_j P_\mathcal{C} = \sum_{k,l} u_{ik}\overline{u_{jl}} P_\mathcal{C} E_k^\dagger E_l P_\mathcal{C} = \sum_{k,l} u_{ik}\overline{u_{jl}}\lambda_{kl} P_\mathcal{C} = d_{ij} P_\mathcal{C}.$$

Thus, $P_\mathcal{C} F_i^\dagger F_j P_\mathcal{C} = 0$ for all $i \neq j$. For each i, we can apply the polar decomposition to obtain unitary operators U_i such that

$$F_i P_\mathcal{C} = U_i \sqrt{P_\mathcal{C} F_i^\dagger F_i P_\mathcal{C}} = \sqrt{d_{ii}} U_i P_\mathcal{C}.$$

When restricted to $\mathcal{L}_1(\mathcal{C})$, the mixed unitary channel $\mathcal{F}' \equiv \{\sqrt{d_{ii}}U_i\}$ is equivalent to the restriction of $\mathcal{F}$ (and hence $\mathcal{E}$) to $\mathcal{L}_1(\mathcal{C})$, and has the desired orthogonality property. □

To illustrate lemma 1, we introduce a simple example.

Example 2. Let I be the 2×2 identity matrix, U and V be 2×2 unitary matrices, $q \in (0, 1)$ and $\mathcal{H}$ be the two-qubit (four-dimensional) Hilbert space with standard basis

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Then consider the channel $\mathcal{E}$ given by the four Kraus operators represented in the standard basis as

$$\alpha\begin{bmatrix} I & U \\ 0 & 0 \end{bmatrix}, \qquad \alpha\begin{bmatrix} I & -U \\ 0 & 0 \end{bmatrix}, \qquad \beta\begin{bmatrix} I & V \\ I & V \end{bmatrix}, \qquad \beta\begin{bmatrix} -I & V \\ I & -V \end{bmatrix},$$

where $\alpha = \frac{\sqrt{q}}{\sqrt{2}}$ and $\beta = \frac{\sqrt{1-q}}{2}$. It is easily verified that $C = \mathrm{span}\{|00\rangle, |01\rangle\}$ is a correctable subspace for $\mathcal{E}$ with projection $P_C = |00\rangle\langle 00| + |01\rangle\langle 01|$.

Lemma 1 then tells us that there exists a mixed unitary channel $\mathcal{F}$ such that $\mathcal{E}|_{\mathcal{L}_1(\mathcal{C})} = \mathcal{F}|_{\mathcal{L}_1(\mathcal{C})}$. Indeed, it is not difficult to verify that

$$\mathcal{F} = \left\{ \frac{\sqrt{1+q}}{\sqrt{2}} I \otimes I, \frac{\sqrt{1-q}}{\sqrt{2}} X \otimes I \right\}$$

is such a channel because for all $\rho \in \mathcal{L}_1(\mathbb{C}^2)$, we have

$$\mathcal{E}(|0\rangle\langle 0| \otimes \rho) = \mathcal{F}(|0\rangle\langle 0| \otimes \rho) = \left(\frac{1}{2}I + \frac{q}{2}Z\right) \otimes \rho.$$

The following result shows that any quantum channel restricted to a correctable code subspace can be described by a representation, up to 'smearing' by a fixed operator given by the image of the code projection under the map.

Theorem 3. *Let $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ be a quantum channel and $\mathcal{C} \subseteq \mathcal{H}$ be a subspace. Then the following are equivalent:*

(1) $\mathcal{C}$ is correctable for $\mathcal{E}$,

(2) there is a representation $\pi : \mathcal{L}_1(\mathcal{C}) \to \mathcal{L}_1(\mathcal{H})$ such that

$$\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_\mathcal{C}) = \mathcal{E}(P_\mathcal{C})\pi(\rho) \qquad \forall\, \rho \in \mathcal{L}_1(\mathcal{C}).$$

Furthermore, $\pi^\dagger$ is a quantum channel that acts as a correction operation for $\mathcal{E}$ on $\mathcal{C}$.

Proof. We first prove the implication (1) $\Rightarrow$ (2). Since $\mathcal{C}$ is correctable for $\mathcal{E}$, we know by lemma 1 that there exists a mixed unitary channel $\mathcal{F} = \{\sqrt{p_i}U_i\}$ such that $\mathcal{F}(\rho) = \mathcal{E}(\rho)$ for all $\rho \in \mathcal{L}_1(\mathcal{C})$ and $P_\mathcal{C}U_i^\dagger U_j P_\mathcal{C} = 0$ whenever $i \neq j$. Define partial isometries $V_i = U_i P_\mathcal{C}$. It follows that the map $\pi : \mathcal{L}_1(\mathcal{C}) \to \mathcal{L}_1(\mathcal{H})$ defined by $\pi(\rho) = \sum_j V_j \rho V_j^\dagger$ is a *-homomorphism. Since V_j have mutually orthogonal ranges, we have $\sum_j V_j V_j^\dagger \leqslant I$, and thus the map $\pi^\dagger \equiv \{V_j^\dagger\}$ is trace non-increasing. (We can assume with no loss of generality that $\pi^\dagger$ is trace preserving by including the projection onto the orthogonal complement of the ranges of V_j.) We further have for all $\rho \in \mathcal{L}_1(\mathcal{C})$,

$$\mathcal{E}(P_\mathcal{C})\pi(\rho) = \sum_{i,j} p_i V_i V_i^\dagger V_j \rho V_j^\dagger = \sum_i p_i V_i \rho V_i^\dagger = \sum_i p_i U_i \rho U_i^\dagger = \mathcal{E}(\rho).$$

A similar argument shows that $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_\mathcal{C})$.

To see (2) $\Rightarrow$ (1), observe that the equation $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_\mathcal{C})$ and trace preservation of $\mathcal{E}$ implies

$$\mathrm{Tr}(\rho) = \mathrm{Tr}(\mathcal{E}(\rho)) = \mathrm{Tr}(\pi(\rho)\mathcal{E}(P_\mathcal{C})) = \mathrm{Tr}(\rho\pi^\dagger(\mathcal{E}(P_\mathcal{C}))).$$

Since this equation holds for all $\rho \in \mathcal{L}_1(\mathcal{C})$, we have $P_\mathcal{C} = P_\mathcal{C}\pi^\dagger(\mathcal{E}(P_\mathcal{C}))P_\mathcal{C}$, and hence by trace preservation of $\pi^\dagger \circ \mathcal{E}$

$$P_\mathcal{C} = \pi^\dagger(\mathcal{E}(P_\mathcal{C})). \tag{3}$$

Note that $\mathrm{Tr}(\pi^\dagger(\alpha)\beta\gamma) = \mathrm{Tr}(\alpha\pi(\beta\gamma)) = \mathrm{Tr}(\alpha\pi(\beta)\pi(\gamma)) = \mathrm{Tr}(\pi^\dagger(\alpha\pi(\beta))\gamma)$ for all $\alpha \in \mathcal{L}_1(\mathcal{H}), \beta, \gamma \in \mathcal{L}_1(\mathcal{C})$. Since this equation holds for all $\gamma \in \mathcal{L}_1(\mathcal{C})$ in particular, we have that

$$P_C\pi^\dagger(\alpha)\beta P_C = P_C\pi^\dagger(\alpha\pi(\beta))P_C \qquad \forall\, \alpha \in \mathcal{L}_1(\mathcal{H}), \beta \in \mathcal{L}_1(\mathcal{C}). \tag{4}$$

Multiplying equation (3) on the right by an arbitrary $\rho \in \mathcal{L}_1(\mathcal{C})$ now shows that $\rho = \pi^\dagger(\mathcal{E}(P_\mathcal{C}))\rho$. If we then apply equation (4) with $\alpha = \mathcal{E}(P_\mathcal{C})$ and $\beta = \rho$, we see that

$$\rho = \pi^\dagger(\mathcal{E}(P_\mathcal{C}))\rho = \pi^\dagger(\mathcal{E}(P_\mathcal{C})\pi(\rho)) = \pi^\dagger(\mathcal{E}(\rho)),$$

and this completes the proof. □

Observe from the above proof that if $\mathcal{F} = \{\sqrt{p_i}U_i\}$ is the mixed unitary channel described by lemma 1, then the representation described by theorem 3 is given by $\pi(\rho) = \sum_i V_i\rho V_i^\dagger$, where $V_i = U_i P_\mathcal{C}$. Similarly, the correction operation is given by $\pi^\dagger(\sigma) = \sum_i V_i^\dagger\sigma V_i$.

Example 4. Returning to example 2, we see that

$$\pi(\rho) = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} \rho \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix} \rho \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix}$$

and

$$\pi^\dagger(\sigma) = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} \sigma \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix} \sigma \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix}.$$

Note that $\pi^\dagger$ is indeed a correction operation for this channel on the subspace $\mathcal{C}$ because for all $\rho \in \mathcal{L}_1(\mathbb{C}^2)$,

$$\pi^\dagger \circ \mathcal{E}(|0\rangle\langle 0| \otimes \rho) = \pi^\dagger\left(\left(\frac{1}{2}I + \frac{q}{2}Z\right) \otimes \rho\right) = |0\rangle\langle 0| \otimes \rho.$$

2.2. Subsystem codes

We next extend the results of the previous subsection to the more general case of subsystem codes. We begin with a pair of technical results, first the direct generalization of lemma 1 for subsystem codes. This result formalizes a key component of the proof of the main result from [9]. Recall that we use the notation $\mathfrak{A}_\mathcal{B} := 1_\mathcal{A} \otimes \mathcal{L}_1(\mathcal{B})$.

Lemma 5. *Let $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ be a quantum channel and $\mathcal{C} = \mathcal{A}\otimes\mathcal{B} \subseteq \mathcal{H}$ be a subspace. Then $\mathcal{B}$ is correctable for $\mathcal{E}$ if and only if there is a channel $\mathcal{G}$ with $\mathcal{G} \circ \mathcal{P}_\mathcal{C} \equiv \{V_i(D_i \otimes I_\mathcal{B})\}$ such that $\mathcal{E}(\rho) = \mathcal{G}(\rho)$ for all $\rho \in \mathfrak{A}_\mathcal{B}$, where V_i are unitary operators, D_i are mutually commuting positive operators and $P_{\mathcal{C}_i} V_i^\dagger V_j P_{\mathcal{C}_j} = \delta_{ij} P_{\mathcal{C}_i}$ for all i, j, where $\mathcal{C}_i = \mathrm{Ran}(D_i) \otimes \mathcal{B} \subseteq \mathcal{C}$.*

Proof. If there is such a channel $\mathcal{G}$, then we can easily see that the channel $\mathcal{R} \equiv \left\{P_{\mathcal{C}_i} V_i^\dagger\right\}$ acts as a $\mathcal{B}$ subsystem recovery operation for $\mathcal{E}$:

$$\begin{aligned} \mathcal{R} \circ \mathcal{E}(I_\mathcal{A} \otimes \rho_\mathcal{B}) &= \sum_i P_{\mathcal{C}_i} V_i^\dagger \left(\sum_j V_j\big(D_j^2 \otimes \rho_\mathcal{B}\big)V_j^\dagger\right) V_i P_{\mathcal{C}_i} \\ &= \left(\sum_i D_i^2\right) \otimes \rho_\mathcal{B}. \end{aligned}$$

For the other direction, begin by noting that if $\mathcal{B}$ is correctable for $\mathcal{E}$, then there exist operators F_{ij} on $\mathcal{A}$ such that

$$P_{\mathcal{C}}E_i^{\dagger}E_jP_{\mathcal{C}} = F_{ij} \otimes I_{\mathcal{B}} \qquad \forall\, i, j. \tag{5}$$

Observe that the operator block matrix $F = (F_{ij})$ is positive since

$$(I_m \otimes P_{\mathcal{C}})E^{\dagger}E(I_m \otimes P_{\mathcal{C}}) = F \otimes I_{\mathcal{B}},$$

where the row matrix $E = [E_1E_2 \ldots E_m]$, the number of E_i is m and I_m is the identity operator on an m-dimensional Hilbert space. Assume that we have a matrix representation for each of F_{ij}, and hence for $F = (F_{ij})$, defined by a fixed basis for $\mathcal{A}$. Thus, we let U be a unitary matrix such that $UFU^{\dagger} = D$ is diagonal and $U = (U_{ij})$ and $D = (D_{ij})$ be the associated block decompositions. We may naturally regard each U_{ij} as the matrix representation (in the fixed basis) for an operator on $\mathcal{A}$. Then,

$$\sum_{k,l} U_{ik}F_{kl}U_{jl}^{\dagger} = \delta_{ij}D_{ii} \qquad \forall\, i, j, \tag{6}$$

$$\sum_{k} U_{ki}^{\dagger}U_{kj} = \delta_{ij}I_{\mathcal{A}} \qquad \forall\, i, j. \tag{7}$$

Next, define a channel $\mathcal{G} \equiv \{G_i\}$ where for all i,

$$G_i = \sum_j E_j\left(U_{ij}^{\dagger} \otimes I_{\mathcal{B}}\right)P_{\mathcal{C}} + E_iP_{\mathcal{C}}^{\perp}.$$

Let $X_{ij} = E_j\left(U_{ij}^{\dagger} \otimes I_{\mathcal{B}}\right)P_{\mathcal{C}}$. Then by equations (5) and (6), one can verify that for all i, j,

$$P_{\mathcal{C}}G_i^{\dagger}G_jP_{\mathcal{C}} = \sum_{k,l} X_{ik}^{\dagger}X_{jl} = \left(\sum_{k,l} U_{ik}F_{kl}U_{jl}^{\dagger}\right) \otimes I_{\mathcal{B}} = D_{ij} \otimes I_{\mathcal{B}},$$

and $D_{ij} = 0$ for all $i \neq j$. Moreover, equation (7) yields for all $I_{\mathcal{A}} \otimes \rho_{\mathcal{B}} \in \mathfrak{A}_{\mathcal{B}}$

$$\begin{aligned}
\mathcal{G}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) &= \sum_i G_i(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})G_i^{\dagger} \\
&= \sum_{i,j,k} X_{ij}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})X_{ik}^{\dagger} \\
&= \sum_{j,k} E_j\left(\left(\sum_i U_{ij}^{\dagger}U_{ik}\right) \otimes \rho_{\mathcal{B}}\right)E_k^{\dagger} \\
&= \sum_j E_j(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})E_j^{\dagger} \\
&= \mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}).
\end{aligned}$$

By the polar decomposition applied to each $G_iP_{\mathcal{C}}$, and the fact that these operators have mutually orthogonal ranges, there are unitaries V_i such that

$$G_iP_{\mathcal{C}} = V_i\sqrt{P_{\mathcal{C}}G_i^{\dagger}G_iP_{\mathcal{C}}} = V_i(\sqrt{D_{ii}} \otimes I_{\mathcal{B}}).$$

Let $D_i = \sqrt{D_{ii}}$ and $\mathcal{C}_i = \mathrm{Ran}(D_i) \otimes \mathcal{B}$. Observe that each partial isometry $V_iP_{\mathcal{C}}$ has $\mathcal{C}_i$ as its initial projection and that the final projections are onto mutually orthogonal subspaces. Hence, we have $P_{\mathcal{C}_i}V_i^{\dagger}V_jP_{\mathcal{C}_j} = \delta_{ij}P_{\mathcal{C}_i}$. Thus any channel $\mathcal{G}'$ with $\mathcal{G}' \circ \mathcal{P}_{\mathcal{C}} \equiv \{V_i(D_i \otimes I_{\mathcal{B}})\}$ has the desired properties, up to the mutually commuting condition. However, observe that each D_i can be replaced by $U_iD_iU_i^{\dagger}$, where U_i is an arbitrary unitary operator on $\mathcal{A}$, without affecting the result. Thus, we can arrange things so that D_i are simultaneously diagonalizable and commute. □

This is all we need to prove theorem 7. However, note that the preceding result shows what the map $\mathcal{E}$ looks like when restricted to the algebra $\mathfrak{A}_\mathcal{B}$, but it is not clear how, or even if, this extends to the entire subspace $\mathcal{C}$. We extend this result as follows.

Theorem 6. *Let $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ be a quantum channel and $\mathcal{C} = \mathcal{A} \otimes \mathcal{B} \subseteq \mathcal{H}$ be a subspace. Then $\mathcal{B}$ is correctable for $\mathcal{E}$ if and only if there is a family of unitary operators $\{U_i\}$ with $P_\mathcal{C} U_i^\dagger U_j P_\mathcal{C} = 0$ for all $i \neq j$ and a channel $\mathcal{N}_\mathcal{A} : \mathcal{L}_1(\mathcal{A}) \to \mathcal{L}_1(\mathcal{A})$ with Kraus operators $\{N_{i,j}\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{L}_1(\mathcal{C})$, where $\mathcal{F} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ is the channel given by the Kraus operators $\{U_i(N_{i,j} \otimes I_\mathcal{B})\}$.*

Proof. First, let $|\psi\rangle \in B$ be a unit vector and set $P = |\psi\rangle\langle\psi|$. Suppose that $\{|\alpha_k\rangle\}$ is an orthonormal basis for $\mathcal{A}$ and set $A_k = |\alpha_k\rangle\langle\alpha_k|$. Now define $Q_i = U_i(I_\mathcal{A} \otimes P)U_i^\dagger$, where $\{U_i\}$ is the family of unitary operators given by lemma 5. Note that each Q_i is an orthogonal projection. Furthermore, it is not difficult to verify that

$$0 \leqslant \sum_i Q_i \mathcal{E}(A_k \otimes P) Q_i \leqslant \mathcal{E}(A_k \otimes P) \leqslant \mathcal{E}(I_\mathcal{A} \otimes P) = \sum_i U_i\big(D_i^2 \otimes P\big)U_i^\dagger,$$

where $\{D_i\}$ is the family of positive diagonal operators given by lemma 5. Since the above inequalities hold for all k and

$$\mathcal{E}(I_\mathcal{A} \otimes P) = \sum_k \mathcal{E}(A_k \otimes P) = \sum_{i,k} Q_i \mathcal{E}(A_k \otimes P) Q_i,$$

it follows that $\sum_i Q_i \mathcal{E}(A_k \otimes P) Q_i = \mathcal{E}(A_k \otimes P)$ for all k. A simple dimension-counting argument then shows that $\mathcal{E}(A_k \otimes P)$ must be of the form

$$\mathcal{E}(A_k \otimes P) = \sum_i U_i(\sigma_{i,k,\psi} \otimes P)U_i^\dagger.$$

It can also be shown via a standard linearity argument that the operators $\{\sigma_{i,k,\psi}\}$ do not depend on $|\psi\rangle$. Thus, it follows from the linearity of $\mathcal{E}$ that for all $\sigma_\mathcal{A}$ there exist positive operators $\{\tau_{\mathcal{A},i}\}$ such that

$$\mathcal{E}(\sigma_\mathcal{A} \otimes \rho_\mathcal{B}) = \sum_i U_i(\tau_{\mathcal{A},i} \otimes \rho_\mathcal{B})U_i^\dagger \qquad \forall\, \rho_\mathcal{B}.$$

The proof is completed by defining $\mathcal{N}_\mathcal{A}(\sigma_\mathcal{A}) = \sum_i \tau_{\mathcal{A},i}$. □

The following description of subsystem codes in the Schrödinger picture complements other descriptions such as those found in [9, 11, 35, 36].

Theorem 7. *Let $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$ and $\mathcal{C} = \mathcal{A} \otimes \mathcal{B} \subseteq \mathcal{H}$ be a subspace. Then the following are equivalent:*

(i) $\mathcal{B}$ is a correctable subsystem for $\mathcal{E}$,
(ii) there is a representation $\pi : \mathfrak{A}_\mathcal{B} \to \mathcal{L}_1(\mathcal{H})$ such that

$$\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_\mathcal{C}) = \mathcal{E}(P_\mathcal{C})\pi(\rho) \qquad \forall\, \rho \in \mathfrak{A}_\mathcal{B}.$$

Proof. To prove the implication (1) $\Rightarrow$ (2), note that since $\mathcal{B}$ is correctable for $\mathcal{E}$, we know by lemma 5 that there exists a channel $\mathcal{G}$ with $\mathcal{G} \circ \mathcal{P}_{\mathcal{C}} \equiv \{V_i(D_i \otimes I_{\mathcal{B}})\}$ such that $\mathcal{G}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})$ for all $\rho_{\mathcal{B}}$ and $\{V_i\}$ is a family of partial isometries such that $V_i^\dagger V_j = 0$ whenever $i \neq j$ and $V_i^\dagger V_i = P_{\mathcal{C}_i}$, where $P_{\mathcal{C}_i}$ is the orthogonal projection onto $\mathcal{C}_i = \mathrm{Ran}(D_i) \otimes \mathcal{B}$.

Now define $\pi : \mathfrak{A}_{\mathcal{B}} \to \mathcal{L}_1(\mathcal{H})$ by $\pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \sum_i V_i(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})V_i^\dagger$. Then π is easily seen to be a *-homomorphism on $\mathfrak{A}_{\mathcal{B}}$ (using the fact that $P_{\mathcal{C}_i} = Q_i \otimes I_{\mathcal{B}}$ for some projection Q_i on $\mathcal{A}$). Its dual $\pi^\dagger = \{V_i^\dagger\}$ is trace non-increasing and can be trivially extended to a trace-preserving map as before. It then follows that

$$\begin{aligned}
\mathcal{E}(P_{\mathcal{C}})\pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) &= \left(\sum_i V_i(D_i \otimes I_{\mathcal{B}})P_{\mathcal{C}}\big(D_i^\dagger \otimes I_{\mathcal{B}}\big)V_i^\dagger\right)\left(\sum_j V_j(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})V_j^\dagger\right) \\
&= \sum_i V_i(D_i \otimes I_{\mathcal{B}})P_{\mathcal{C}}\big(D_i^\dagger \otimes I_{\mathcal{B}}\big)P_{\mathcal{C}_i}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})V_i^\dagger \\
&= \sum_i V_i(D_i \otimes I_{\mathcal{B}})(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})\big(D_i^\dagger \otimes I_{\mathcal{B}}\big)V_i^\dagger \\
&= \mathcal{G}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}).
\end{aligned}$$

A similar argument shows that $\mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})\mathcal{E}(P_{\mathcal{C}})$.

To see (2) $\Rightarrow$ (1), we show that the algebra $\mathfrak{A}_{\mathcal{B}}$ may be precisely corrected, which is equivalent to correcting the subsystem $\mathcal{B}$ (see theorem 3.2 of [21] for instance). First, note that the representation π defines a subspace and subsystems $\mathcal{C}' = \mathcal{A}' \otimes \mathcal{B}'$ with $\mathcal{B}'$ being of the same dimension as $\mathcal{B}$ and an isometry $V : \mathcal{B} \to \mathcal{B}'$ such that

$$\pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}) \qquad \forall\, \rho_{\mathcal{B}},$$

where $\mathcal{V}(\rho_{\mathcal{B}}) = V\rho_{\mathcal{B}}V^\dagger$. Further, as $\mathcal{E}(P_{\mathcal{C}})$ commutes with $\pi(\mathfrak{A}_{\mathcal{B}})$, it follows that $P_{\mathcal{C}'}\mathcal{E}(P_{\mathcal{C}})P_{\mathcal{C}'} = \sigma_{\mathcal{A}'} \otimes I_{\mathcal{B}'}$ for some positive operator $\sigma_{\mathcal{A}'} \in \mathcal{L}(\mathcal{A}')$ with trace equal to $\dim \mathcal{C}$. Thus we have for all $\rho_{\mathcal{B}}$,

$$\mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \pi(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}})\mathcal{E}(P_{\mathcal{C}}) = (I_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}))(\sigma_{\mathcal{A}'} \otimes I_{\mathcal{B}'}) = \sigma_{\mathcal{A}'} \otimes \mathcal{V}(\rho_{\mathcal{B}}).$$

Now define a channel $\mathcal{R}$ on $\mathcal{H}$ such that $\mathcal{R} \circ \mathcal{P}_{\mathcal{C}'} = (\mathcal{D}_{\mathcal{A}|\mathcal{A}'} \otimes \mathcal{V}^\dagger) \circ \mathcal{P}_{\mathcal{C}'}$, where $\mathcal{D}_{\mathcal{A}|\mathcal{A}'}$ is the complete depolarizing channel from $\mathcal{A}'$ to $\mathcal{A}$, and it follows that $(\mathcal{R} \circ \mathcal{E})(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$ for all $\rho_{\mathcal{B}}$. This shows that $\mathfrak{A}_{\mathcal{B}}$ can be exactly corrected, and completes the proof. $\square$

3. The multiplicative domain and unitarily correctable codes

Given a CP map $\phi : \mathfrak{A} \to \mathfrak{B}$ between two operator algebras, the *multiplicative domain* of ϕ, denoted $MD(\phi)$, is defined as follows:

$$MD(\phi) := \{a \in \mathfrak{A} : \phi(a)\phi(b) = \phi(ab) \text{ and } \phi(b)\phi(a) = \phi(ba) \text{ for all } b \in \mathfrak{A}\}.$$

It is clear that $MD(\phi)$ is an algebra, and hence has a structure as in equation (1). In this section, we address this basic question: what role, if any, does the multiplicative domain play in quantum error correction?

The unital case ($\phi(I) = I$) often stands out in the CP theory, and this is the case for multiplicative domains. The following result [18, 19] shows how the multiplicative domain simplifies in the unital case. Note that in particular, if $\mathcal{E}$ is a quantum channel then theorem 8 applies to $\mathcal{E}^\dagger$.

Theorem 8. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be algebras and $\phi : \mathcal{A} \mapsto \mathcal{B}$ be a completely positive, unital map. Then,*

$$MD(\phi) = \{a \in \mathcal{A} : \phi(a)^\dagger\phi(a) = \phi(a^\dagger a) \text{ and } \phi(a)\phi(a)^\dagger = \phi(aa^\dagger)\}.$$

*Furthermore, ϕ is a *-homomorphism when restricted to this set.*

Turning to quantum error correction, an important class of quantum codes is the so-called unitarily correctable codes (UCCs). These are codes for which a unitary recovery operation can be obtained. Alternatively, UCCs are the highly degenerate codes for which a recovery operation can be implemented without a measurement. As such, they are potentially quite useful in fault-tolerant quantum computing since these codes and their recovery operations do not require more of the system Hilbert space than what is required by the initial code. A subsystem code $\mathcal{B}$ is *unitarily correctable* for $\mathcal{E}$ if there is a unitary channel $\mathcal{U}$ and channel $\mathcal{F}_\mathcal{A} : \mathcal{L}_1(\mathcal{A}) \to \mathcal{L}_1(\mathcal{A})$ such that

$$\mathcal{E} \circ \mathcal{P}_{\mathcal{AB}} = \mathcal{U} \circ (\mathcal{F}_\mathcal{A} \otimes \mathrm{id}_\mathcal{B}) \circ \mathcal{P}_{\mathcal{AB}}.$$

The UCC class includes decoherence-free subspaces and noiseless subsystems in the case that $\mathcal{U} = \mathrm{i}d$.

The results of the previous section motivate a new notion for codes in which UCCs stand out as a special case.

Definition 9. *Let $\mathcal{C} = \mathcal{A} \otimes \mathcal{B} \subseteq \mathcal{H}$, and suppose $\mathcal{B}$ is correctable for $\mathcal{E} : \mathcal{L}_1(\mathcal{H}) \to \mathcal{L}_1(\mathcal{H})$. Then we define the correction multiplicity of $\mathcal{B}$ for $\mathcal{E}$ to be the multiplicity of the representation π determined by $\mathcal{E}$ and $\mathcal{B}$ as in theorem 7.*

Observe that in the case of subspace codes, the UCCs for a given channel $\mathcal{E}$ are precisely its correction multiplicity-1 codes.

One of the main results from [9] shows in the unital case ($\mathcal{E}(I) = I$) that UCCs are precisely the passive codes for the map composed with its dual.

Theorem 10. *[9] Let $\mathcal{E}$ be a unital quantum channel. Then the following are equivalent:*

(i) $\mathcal{B}$ is a unitarily correctable subsystem for $\mathcal{E}$,
(ii) $\mathcal{B}$ is a noiseless subsystem for $\mathcal{E}^\dagger \circ \mathcal{E}$.

Theorem 10 shows that we may unambiguously define *the* UCC algebra for a unital channel $\mathcal{E} \equiv \{E_i\}$ as

$$UCC(\mathcal{E}) := \{\rho : \mathcal{E}^\dagger \circ \mathcal{E}(\rho) = \rho\} = \left\{\rho : \left[\rho, E_i^\dagger E_j\right] = 0\right\},$$

as we know from the theory of passive quantum error correction that the latter algebra encodes all noiseless subsystems for $\mathcal{E}^\dagger \circ \mathcal{E}$. (See [9] and references therein for further discussions on this point.)

The following theorem shows the intimate relationship among a unital channel's unitarily correctable codes, its multiplicative domain, and the unitarily correctable codes and multiplicative domain of its dual map. Interestingly, in the case of a unital channel this shows that a naturally arising object in the theory of CP maps, the multiplicative domain, describes a class of quantum codes that have arisen in quantum error correction for completely different reasons.

Theorem 11. *Let $\mathcal{E}$ be a unital quantum channel. Then the following four algebras coincide:*

(i) $MD(\mathcal{E})$
(ii) $UCC(\mathcal{E})$

(iii) $\mathcal{E}^\dagger(MD(\mathcal{E}^\dagger))$
(iv) $\mathcal{E}^\dagger(UCC(\mathcal{E}^\dagger))$.

Proof. As $\mathcal{E}$ is a unital channel if and only if $\mathcal{E}^\dagger$ is the same, this result is symmetric in $\mathcal{E}$ and $\mathcal{E}^\dagger$. We first show that $MD(\mathcal{E}^\dagger) \subseteq UCC(\mathcal{E}^\dagger)$. Note that if $a \in MD(\mathcal{E}^\dagger)$, then $\mathrm{Tr}(\mathcal{E}^\dagger(a)\mathcal{E}^\dagger(b)) = \mathrm{Tr}(\mathcal{E}^\dagger(ab))$ for all $b \in \mathcal{L}_1(\mathcal{H})$. Then $\mathrm{Tr}(\mathcal{E}\circ\mathcal{E}^\dagger(a)b) = \mathrm{Tr}(\mathcal{E}(1)ab) = \mathrm{Tr}(ab)$ for all $b \in \mathcal{L}_1(\mathcal{H})$ and so it follows that $\mathcal{E}\circ\mathcal{E}^\dagger(a) = a$ for all $a \in MD(\mathcal{E}^\dagger)$. The inclusion then follows from theorem 10.

To see the opposite inclusion, note that if $\mathcal{B}$ is a unitarily correctable subsystem for $\mathcal{E}^\dagger$ then lemma 5 says that $\mathcal{E}^\dagger\circ\mathcal{P}_\mathcal{C} \equiv \{U(D\otimes I_\mathcal{B})P_\mathcal{C}\}$ for some unitary U and diagonal operator D. In fact, since $\mathcal{B}$ is noiseless for the unital channel $\mathcal{U}^\dagger\circ\mathcal{E}^\dagger$, it follows that $\mathcal{U}^\dagger\circ\mathcal{E}^\dagger(I_\mathcal{A}\otimes\rho_\mathcal{B}) = I_\mathcal{A}\otimes\rho_\mathcal{B}$ for all $\rho_\mathcal{B}$. Hence we have $D = I_\mathcal{A}$, and so $\mathcal{E}^\dagger(a) = \mathcal{U}(a)$ for all $a \in \mathfrak{A}_\mathcal{B}$. Theorem 8 now shows that the algebra $\mathfrak{A}_\mathcal{B}$, and hence $UCC(\mathcal{E}^\dagger)$, is contained inside $MD(\mathcal{E}^\dagger)$. Thus, $MD(\mathcal{E}^\dagger) = UCC(\mathcal{E}^\dagger)$ (and similarly $\mathcal{E}(MD(\mathcal{E})) = \mathcal{E}(UCC(\mathcal{E}))$).

We next show that $\mathcal{E}(UCC(\mathcal{E})) \subseteq MD(\mathcal{E}^\dagger)$. Now theorem 10 says that if $\mathcal{B}$ is unitarily correctable for $\mathcal{E}$, then $\mathcal{B}$ is noiseless for the unital channel $\mathcal{E}^\dagger\circ\mathcal{E}$. Moreover, the restriction of $\mathcal{E}$ to $\mathfrak{A}_\mathcal{B}$ is multiplicative by the previous paragraph. Hence, it follows that the restricted map satisfies $\mathcal{E}^\dagger\circ\mathcal{E}|_{\mathfrak{A}_\mathcal{B}} = \mathcal{P}_\mathcal{C}|_{\mathfrak{A}_\mathcal{B}}$ and that $\mathcal{E}^\dagger$ is a multiplicative map when restricted to the image algebra $\mathcal{E}(\mathfrak{A}_\mathcal{B})$. Therefore from theorem 8 we have $\mathcal{E}(\mathfrak{A}_\mathcal{B}) \subseteq MD(\mathcal{E}^\dagger)$, and the inclusion follows.

To get the opposite inclusion, note that $\mathcal{E}^\dagger(UCC(\mathcal{E}^\dagger)) \subseteq MD(\mathcal{E})$ implies

$$MD(\mathcal{E}^\dagger) = UCC(\mathcal{E}^\dagger) = \mathcal{E}\circ\mathcal{E}^\dagger(UCC(\mathcal{E}^\dagger)) \subseteq \mathcal{E}(MD(\mathcal{E})) = \mathcal{E}(UCC(\mathcal{E})).$$

The second equality above comes from theorem 10. This completes the proof. □

Note that the equivalence of algebras $MD(\mathcal{E}^\dagger)$ and $\mathcal{E}(UCC(\mathcal{E}))$ in theorem 11 does not imply that correctable codes with multiplicity 2 or more cannot be found in the multiplicative domain of $\mathcal{E}^\dagger$. The following example highlights this fact and presents a map that has a non-unitarily correctable code with an image under $\mathcal{E}$ that coincides with the image of a unitarily correctable subsystem.

Example 12. Let $U, V, W \in \mathcal{L}(\mathcal{H})$ be unitary operators, let $q \in [0, 1]$ and define a quantum channel $\mathcal{E} : M_2(\mathcal{L}(\mathcal{H})) \mapsto M_2(\mathcal{L}(\mathcal{H}))$ by the following pair of Kraus operators:

$$E_1 = q\begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix}, \qquad E_2 = \sqrt{1-q^2}\begin{bmatrix} 0 & U \\ W & 0 \end{bmatrix}.$$

Then $\mathcal{E}$ is a unital quantum channel and a correctable subspace for $\mathcal{E}$ is projected onto by the projection

$$P_\mathcal{C} = \begin{bmatrix} I_\mathcal{H} & 0 \\ 0 & 0 \end{bmatrix}.$$

If $q \in \{0, 1\}$, then $\mathcal{C}$ is unitarily correctable. Otherwise, $\mathcal{C}$ is multiplicity-2 correctable. The image algebra under the action of $\mathcal{E}\circ\mathcal{P}_\mathcal{C}$ is given by the operators of the form

$$\begin{bmatrix} U\rho U^\dagger & 0 \\ 0 & W\rho W^\dagger \end{bmatrix}, \tag{8}$$

where $\rho \in M_2$. Moreover,

$$\mathcal{E}^\dagger\left(\begin{bmatrix} U\rho U^\dagger & 0 \\ 0 & W\rho W^\dagger \end{bmatrix}\right) = \begin{bmatrix} \rho & 0 \\ 0 & q^2V^\dagger W\rho W^\dagger V + (1-q^2)\rho \end{bmatrix},$$

from which it follows that $\mathcal{E}^\dagger$ is a *-homomorphism when restricted to this algebra if and only if $q \in \{0, 1\}$ (in which case $\mathcal{C}$ is unitarily correctable) or $W = V$. It is not difficult to verify, however, that $W = V$ is exactly the condition under which $\mathcal{L}(\mathcal{H})$ becomes a unitarily correctable subsystem when the space is decomposed as $M_2 \otimes \mathcal{L}(\mathcal{H})$. Further, the image of the algebra $1_A \otimes \mathcal{L}(\mathcal{H})$ under $\mathcal{E}$ is exactly the algebra of operators of the form in equation (8).

It is also worth noting that if $\mathcal{E}$ is not unital, then theorem 11 does not hold, even just when considering $MD(\mathcal{E}^\dagger)$ and $\mathcal{E}(UCC(\mathcal{E}))$. This can be seen explicitly by the following example, which gives a non-unital channel $\mathcal{E}$ with a noiseless subspace that is not captured under the image of $\mathcal{E}$ by the multiplicative domain of $\mathcal{E}^\dagger$. Nevertheless, it will be seen in theorem 14 that the multiplicative domain can help us find a subclass of unitarily correctable codes for non-unital quantum channels.

Example 13. Let $q \in \left[0, \frac{1}{2}\right]$ and define a quantum channel $\mathcal{E}$ on a four-dimensional Hilbert space $\mathcal{H}$ by the following three Kraus operators in the standard basis:

$$E_1 = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha \end{bmatrix}, \qquad E_2 = \beta \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad E_3 = \beta \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

where $\alpha = \sqrt{1-2q}$ and $\beta = \sqrt{q/2}$. It is straightforward to verify that $\mathcal{E}$ is a non-unital quantum channel. It is similarly not difficult to verify that a decoherence-free subspace of dimension 2 for $\mathcal{E}$ is projected onto by the projection

$$P_C = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The image algebra under the action of $\mathcal{E} \circ \mathcal{P}_C$ is then simply $\mathcal{L}_1(P_C\mathcal{H})$. Observe that

$$\mathcal{E}^\dagger \left(\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & r & s & 0 \\ 0 & t & u & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & r & s & 0 \\ 0 & t & u & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + q \begin{bmatrix} u & 0 & 0 & t \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ s & 0 & 0 & r \end{bmatrix},$$

from which it follows that $\mathcal{E}^\dagger$ is a *-homomorphism when restricted to this algebra if and only if $q = 0$ (in which case $\mathcal{E}$ is unital) or $q = 1$ (in which case $\mathcal{E}$ is not trace preserving).

For an arbitrary non-unital channel $\mathcal{E}$, it is not at all clear how one could go about computing its UCCs. For instance, there does not appear to be an analogue of the algebra UCC ($\mathcal{E}$) in the general non-unital case. However, the following theorem shows how the previous results on the multiplicative domain can be extended to the non-unital case, and hence that it yields a subclass of UCCs that can be directly computed. On terminology, when we say the 'codes encoded in an algebra', we mean the subsystem (and subspace) codes determined by the structure of the algebra as in equation (1).

Theorem 14. *Let $\mathcal{E}$ be a quantum channel. Then the quantum codes encoded in $MD(\mathcal{E})$ are UCC for $\mathcal{E}$.*

Proof. Proceeding similar to the proof of theorem 11, note that if $a \in MD(\mathcal{E})$ then $\mathrm{Tr}(\mathcal{E}(a)\mathcal{E}(b)) = \mathrm{Tr}(\mathcal{E}(ab))$ for all $b \in \mathcal{L}_1(\mathcal{H})$. Thus, $\mathrm{Tr}(\mathcal{E}^\dagger \circ \mathcal{E}(a)b) = \mathrm{Tr}(\mathcal{E}^\dagger(I)ab) = \mathrm{Tr}(ab)$ for all $b \in \mathcal{L}_1(\mathcal{H})$ and so it follows that $\mathcal{E}^\dagger \circ \mathcal{E}(a) = a$ for all $a \in MD(\mathcal{E})$. The remainder of this proof shows that this implies that a is contained in a unitarily correctable subsystem of $\mathcal{E}$.

Assume without loss of generality that a is of the form $I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$. Then we have that $\mathcal{E}^{\dagger} \circ \mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$ for all $\rho_{\mathcal{B}}$. This implies from the positivity and linearity of $\mathcal{E}^{\dagger} \circ \mathcal{E}$ that for any $\sigma_{\mathcal{A}}$, there is $\tau_{\mathcal{A}}$ such that $\mathcal{E}^{\dagger} \circ \mathcal{E}(\sigma_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = \tau_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$ for all $\rho_{\mathcal{B}}$ (see [20] for a proof of this fact). Thus, multiplying on the left by $\mathcal{P}_{\mathcal{C}}$ gives us $\mathcal{P}_{\mathcal{C}} \circ \mathcal{E}^{\dagger} \circ \mathcal{E} \circ \mathcal{P}_{\mathcal{C}} = (\mathcal{F}_{\mathcal{A}} \otimes \mathrm{id}_{\mathcal{B}}) \circ \mathcal{P}_{\mathcal{C}}$ for some CP map $\mathcal{F}_{\mathcal{A}}$, and hence $\mathcal{B}$ is correctable for $\mathcal{E}$.

Now note that $P_{\mathcal{C}} := I_{\mathcal{A}} \otimes I_{\mathcal{B}} \in MD(\mathcal{E})$, so $\mathcal{E}(P_{\mathcal{C}})^2 = \mathcal{E}(P_{\mathcal{C}})$ and thus $\mathcal{E}(P_{\mathcal{C}})$ is a projection. We can further see via trace preservation that the dimension of the range of $\mathcal{E}(P_{\mathcal{C}})$ is the same as that of $P_{\mathcal{C}}$. It follows by theorem 7 that $\mathcal{B}$ must in fact be unitarily correctable for $\mathcal{E}$. □

As one characterization of $\mathcal{B}$ being a noiseless subsystem for $\mathcal{E}$ is the existence of a channel $\mathcal{F}_{\mathcal{A}}$ such that $\mathcal{E} \circ \mathcal{P}_{\mathcal{C}} = (\mathcal{F}_{\mathcal{A}} \otimes \mathrm{id}_{\mathcal{B}}) \circ \mathcal{P}_{\mathcal{C}}$, we see that $\mathcal{E}(P_{\mathcal{C}}) = P_{\mathcal{C}}$ implies that $\mathcal{F}_{\mathcal{A}}$ is unital and hence that $\mathcal{E}(I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}) = I_{\mathcal{A}} \otimes \rho_{\mathcal{B}}$ for all $\rho_{\mathcal{B}}$. This implies, along with the proof of theorem 14, that the implication (2) ⇒ (1) of theorem 10 holds for non-unital channels as long as $\mathcal{E}^{\dagger} \circ \mathcal{E}(P_{\mathcal{C}}) = P_{\mathcal{C}}$. In particular, this implication always holds for noiseless and unitarily correctable *subspaces*.

Example 15. We give a simple example of a channel with a non-trivial multiplicative domain that does not capture all UCCs. Let $\mathcal{E}$ be the channel defined on 6×6 matrices, broken up into nine 2×2 blocks, as follows:

$$\mathcal{E}\left[\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}\right] = \begin{bmatrix} 0 & 0 & 0 \\ 0 & A_{11} + A_{22} & 0 \\ 0 & 0 & A_{33} \end{bmatrix}.$$

Clearly, each of the three block entries $(i, i), i = 1, 2, 3$, defines single qubit unitarily correctable codes, but only the third is encoded in the multiplicative domain. In fact, in this case the 2×2 block determined by the $(3, 3)$ entry is precisely the multiplicative domain for $\mathcal{E}$.

Remark 16. This example is very much in the spirit of the spontaneous emission or amplitude dampening channels [1], which are the standard physical examples of non-unital quantum channels. It would be interesting to know if the non-unital behavior of arbitrary channels could somehow be characterized by such channels and what role, if any, the multiplicative domain might have in the description. We plan to undertake this investigation elsewhere.

3.1. Computing the multiplicative domain

While it is not known how to compute UCCs for an arbitrary channel, the multiplicative domain codes can be computed with available software. In order to compute the multiplicative domain of a linear map $\phi : M_n \mapsto M_k$, note that it suffices to solve the following system of $2k^2n^2$ linear equations in n^2 unknowns:

$$\phi(E_{l,m}(\sigma_{i,j})) = \phi(E_{l,m})\phi((\sigma_{i,j}))$$

and

$$\phi((\sigma_{i,j})E_{l,m}) = \phi((\sigma_{i,j}))\phi(E_{l,m}),$$

for all $1 \leqslant l, m \leqslant n$, where $\{E_{l,m}\}$ is the family of standard matrix units associated with a fixed basis. If we let $\phi = \{A_p\}$, where $A_p = (a_{ijp})$ (where i indexes the rows of A_p and j indexes the columns of A_p), then the above matrix equations can be written out more explicitly as the following system of linear equations:

$$\sum_{b,e} a_{ywe}\overline{a_{zbe}}\sigma_{xb} = \sum_{b,c,d,e,f} a_{ywe}\overline{a_{dxe}}a_{dcf}\overline{a_{zbf}}\sigma_{cb} \qquad \forall\, 1 \leqslant w, x \leqslant n, 1 \leqslant y, z \leqslant k,$$

and

$$\sum_{b,e} a_{ybe}\overline{a_{zxe}}\sigma_{bw} = \sum_{b,c,d,e,f} a_{yce}\overline{a_{dbe}}a_{dwf}\overline{a_{zxf}}\sigma_{cb} \qquad \forall\, 1 \leqslant w, x \leqslant n, 1 \leqslant y, z \leqslant k.$$

This is simply a system of linear equations and thus can be solved by computer software such as MATLAB. For large-scale quantum systems, however, it is clear that more refined approaches would be required to compute these (as well as any other) codes. We leave such scalability issues for investigation elsewhere.

Example 17. This example illustrates how the above linear system of equations can be used to compute the multiplicative domain of an arbitrary map, and find unitarily correctable codes from it. Again, consider the channel from example 2, but choose $U = V = I$. That is, consider the 2-qubit channel $\mathcal{E}$ defined by the four Kraus operators

$$\alpha\begin{bmatrix} I & I \\ 0 & 0 \end{bmatrix}, \qquad \alpha\begin{bmatrix} I & -I \\ 0 & 0 \end{bmatrix}, \qquad \beta\begin{bmatrix} I & I \\ I & I \end{bmatrix}, \qquad \beta\begin{bmatrix} -I & I \\ I & -I \end{bmatrix},$$

where $\alpha = \frac{\sqrt{q}}{\sqrt{2}}$, $\beta = \frac{\sqrt{1-q}}{2}$, and $q \in [0, 1]$. Then if we write $\sigma = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$, where $A, B, C, D \in M_2$ are 2×2 matrices, then the linear equations that need to be solved reduce to

$$\begin{aligned} (1-q)A &= (1+q)D, \qquad & (1-q)B &= (1+q)C \\ (1+q)A &= (1-q)D, \qquad & (1+q)B &= (1-q)C. \end{aligned}$$

We will consider the solutions of these linear equations in three cases.

Case 1. $q = 0$. In this case the solutions are $A = D$ and $B = C$, so the multiplicative domain of $\mathcal{E}$ consists of exactly the matrices of the form $\left[\begin{smallmatrix} A & B \\ B & A \end{smallmatrix}\right]$. Because this channel is unital when $q = 0$, it follows by theorem 11 that the algebra of unitarily correctable codes is exactly the same:

$$\mathrm{UCC}(\mathcal{E}) = \left\{ \begin{bmatrix} A & B \\ B & A \end{bmatrix} : A, B \in M_2 \right\}. \tag{9}$$

Indeed, it is not difficult to verify that this algebra encodes, in the sense discussed above, a pair of decoherence-free subspaces for $\mathcal{E}$.

Case 2. $0 < q < 1$. The solutions here are $A = B = C = D = 0$, so the multiplicative domain contains only the zero matrix and thus does not capture any correctable codes. It appears that these channels also do not have unitarily correctable codes, though they do have multiplicity-2 correctable codes as described in example 2.

Case 3. $q = 1$. The solutions here are $A = B = C = D = 0$, so the multiplicative domain contains only the zero matrix and thus does not capture any correctable codes. However, it is easily verified that the two subspaces defined by the ranges of the following two algebras are unitarily correctable:

$$\left\{ \begin{bmatrix} A & -A \\ -A & A \end{bmatrix} : A \in M_2 \right\} \qquad \text{and} \qquad \left\{ \begin{bmatrix} A & A \\ A & A \end{bmatrix} : A \in M_2 \right\},$$

where the unitary correction operators are $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix} I & I \\ -I & I \end{smallmatrix}\right]$ and $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix} I & -I \\ I & I \end{smallmatrix}\right]$, respectively. The fact that the multiplicative domain does not capture all unitarily correctable codes highlights the fact that the converse of theorem 14 does not hold in general for non-unital quantum channels.

Also, the smallest algebra containing these two subspaces is exactly the algebra described by equation (9). However,

$$\mathcal{E}\left(\begin{bmatrix} A & B \\ B & A \end{bmatrix}\right) = \begin{bmatrix} 2A & 0 \\ 0 & 0 \end{bmatrix},$$

so clearly that the algebra is not unitarily correctable as there is no way to recover the 'B' blocks. This highlights the fact that in general, there is no way to define the UCC algebra of a non-unital quantum channel.

Acknowledgments

We are grateful to the referees for several helpful suggestions. M-D C was supported by an NSERC Discovery Grant. NJ was supported by an NSERC Canada Graduate Scholarship and the University of Guelph Brock Scholarship. DWK was supported by an NSERC Discovery Grant and Discovery Accelerator Supplement, an Ontario Early Researcher Award, and CIF, OIT.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Gottesman D 2002 An introduction to quantum error correction *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium* ed S J Lomonaco Jr (Providence, RI: American Mathematical Society) pp 221–235
[3] Knill E, Laflamme R, Ashikhmin A, Barnum H N, Viola L and Zurek W H 2002 Introduction to quantum error correction *Los Alamos Sci.* **27** 188–225
[4] Gottesman D 1996 *Phys. Rev.* A **54** 1862
[5] Kribs D, Laflamme R and Poulin D 2005 *Phys. Rev. Lett.* **94** 180501
[6] Poulin D 2005 *Phys. Rev. Lett.* **95** 230504
[7] Shabani A and Lidar D A 2005 *Phys. Rev.* A **72** 042303
[8] Bacon D 2006 *Phys. Rev.* A **73** 012340
[9] Kribs D W and Spekkens R W 2006 *Phys. Rev.* A **74** 042329
[10] Choi M D and Kribs D W 2006 *Phys. Rev. Lett.* **96** 050501
[11] Knill E 2006 *Phys. Rev.* A **74** 042301
[12] Klappenecker A and Sarvepalli P K 2006 arXiv:org/quant-ph/0604161
[13] Aly S A and Klappenecker A 2007 arXiv:0712.4321
[14] Emerson J, Silva M, Moussa O, Ryan C, Laforest M, Baugh J, Cory D G and Laflamme R 2007 *Science* **317** 1893
[15] Beny C, Kempf A and Kribs D W 2007 *Phys. Rev. Lett.* **98** 100502
[16] Blume-Kohout R, Ng H K, Poulin D and Viola L 2008 *Phys. Rev. Lett.* **100** 030501
[17] Silva M, Magesan E, Kribs D W and Emerson J 2008 *Phys. Rev.* A **78** 012347
[18] Choi M-D 1974 *Illinois J. Math.* **18** 565–74
[19] Paulsen V I 2003 *Completely Bounded Maps and Operator Algebras* (Cambridge: Cambridge University Press)
[20] Kribs D W, Laflamme R, Poulin D and Lesosky M 2005 arXiv:org/quant-ph/0504189v2
[21] Kribs D W, Laflamme R, Poulin D and Lesosky M 2006 *Quantum Inf. Comput.* **6** 383–99
[22] Zanardi P and Rasetti M 1997 *Phys. Rev. Lett.* **79** 3306
[23] Palma G, Suominen K-A and Ekert A 1996 *Proc. R. Soc.* A **452** 567
[24] Duan L-M and Guo G-C 1997 *Phys. Rev. Lett.* **79** 1953
[25] Lidar D A, Chuang I L and Whaley K B 1998 *Phys. Rev. Lett.* **81** 2594
[26] Knill E, Laflamme R and Viola L 2000 *Phys. Rev. Lett.* **84** 2525
[27] Zanardi P 2001 *Phys. Rev.* A **63** 12301
[28] Kempe J, Bacon D, Lidar D A and Whaley K B 2001 *Phys. Rev.* A **63** 42307
[29] Shor P W 1995 *Phys. Rev.* A **52** R2493
[30] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
[31] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824

[32] Knill E and Laflamme R 1997 *Phys. Rev.* A **55** 900
[33] Nielsen M A and Poulin D 2007 *Phys. Rev.* A **75** 64304
[34] Davidson K R 1996 C^**-Algebras by Example (Fields Institute Monographs* vol 6*)* (Providence, RI: American Mathematical Society)
[35] Beny C, Kribs D W and Pasieka A 2008 *Int. J. Quantum Inf.* **6** 597–603
[36] Beny C, Kempf A and Kribs D W 2008 *Phys. Rev.* A **76** 042303