The Multiplicative Domain in Quantum Error Correction

Nathaniel Johnston
Collaborative work with Man-Duen Choi and David Kribs

University of Guelph

December 6, 2008

Completely Positive Maps

Given a (finite-dimensional) Hilbert space $\mathcal{H}$, a linear map $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ will be said to be **Completely Positive** (CP) if $(id_k \otimes \Phi)$ is positive for all $k \in \mathbb{N}$.

Completely Positive Maps

Given a (finite-dimensional) Hilbert space $\mathcal{H}$, a linear map $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ will be said to be **Completely Positive** (CP) if $(id_k \otimes \Phi)$ is positive for all $k \in \mathbb{N}$.

By Choi's theorem, we know that Φ is completely positive if and only if there exist **Kraus Operators** $\{A_i\}$ such that

$$\Phi(a) = \sum_i A_i a A_i^\dagger \quad \forall\, a \in \mathcal{L}(\mathcal{H}),$$

where $A_i^\dagger$ refers to the operator adjoint (ie. conjugate transpose) of A_i. For brevity we will sometimes say that $\Phi = \{A_i\}$.

Schrödinger Picture

In the Schrödinger picture of quantum dynamics, time evolution of open quantum systems is described by completely positive trace-preserving maps. Trace preservation of the completely positive map $\mathcal{E} = \{E_i\}$ is equivalent to

$$\sum_i E_i^\dagger E_i = I.$$

Schrödinger Picture

In the Schrödinger picture of quantum dynamics, time evolution of open quantum systems is described by completely positive trace-preserving maps. Trace preservation of the completely positive map $\mathcal{E} = \{E_i\}$ is equivalent to

$$\sum_i E_i^\dagger E_i = I.$$

We will refer to maps of this type as **Quantum Channels**.

Heisenberg Picture

In the Heisenberg picture, time evolution is described by the dual map $\mathcal{E}^\dagger : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ defined by

$$\mathrm{Tr}(\mathcal{E}(\rho)X) = \mathrm{Tr}(\rho\mathcal{E}^\dagger(X)).$$

Heisenberg Picture

In the Heisenberg picture, time evolution is described by the dual map $\mathcal{E}^\dagger : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ defined by

$$\mathrm{Tr}(\mathcal{E}(\rho)X) = \mathrm{Tr}(\rho\mathcal{E}^\dagger(X)).$$

- $\mathcal{E} = \{E_i\}$ if and only if $\mathcal{E}^\dagger = \{E_i^\dagger\}$, and

Heisenberg Picture

In the Heisenberg picture, time evolution is described by the dual map $\mathcal{E}^\dagger : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ defined by

$$\mathrm{Tr}(\mathcal{E}(\rho)X) = \mathrm{Tr}(\rho\mathcal{E}^\dagger(X)).$$

- $\mathcal{E} = \{E_i\}$ if and only if $\mathcal{E}^\dagger = \{E_i^\dagger\}$, and
- $\mathcal{E}$ is trace-preserving if and only if $\mathcal{E}^\dagger$ is unital (ie. $\mathcal{E}^\dagger(I) = I$).

Correctable Subspaces

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C \subseteq \mathcal{H}$ is a subspace, then C is said to be a **Correctable Subspace** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho \in \mathcal{L}(C).$$

Correctable Subspaces

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C \subseteq \mathcal{H}$ is a subspace, then C is said to be a **Correctable Subspace** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho \in \mathcal{L}(C).$$

- $\mathcal{R}$ is called a **Correction Operation**.

Correctable Subspaces

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C \subseteq \mathcal{H}$ is a subspace, then C is said to be a **Correctable Subspace** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho \in \mathcal{L}(C).$$

- $\mathcal{R}$ is called a **Correction Operation**.
- If $\mathcal{R} = id_{\mathcal{H}}$ is a valid correction operation, then C is called a **Decoherence-free Subspace**.

Correctable Subsystems

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C = A \otimes B \subseteq \mathcal{H}$ is a subspace, then B is said to be a **Correctable Subsystem** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$\forall \rho^A, \ \forall \rho^B, \ \exists \tau^A \text{ such that } (\mathcal{R} \circ \mathcal{E})(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B.$$

Correctable Subsystems

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C = A \otimes B \subseteq \mathcal{H}$ is a subspace, then B is said to be a **Correctable Subsystem** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$\forall\, \rho^A,\ \forall\, \rho^B,\ \exists\, \tau^A \text{ such that } (\mathcal{R} \circ \mathcal{E})(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B.$$

- If $\mathcal{R} = id_{\mathcal{H}}$ is a valid correction operation, then B is called a **Noiseless Subsystem**.

Correctable Subsystems

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel. If $C = A \otimes B \subseteq \mathcal{H}$ is a subspace, then B is said to be a **Correctable Subsystem** if there exists another quantum channel $\mathcal{R} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ such that

$$\forall \rho^A, \ \forall \rho^B, \ \exists \tau^A \text{ such that } (\mathcal{R} \circ \mathcal{E})(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B.$$

- If $\mathcal{R} = id_{\mathcal{H}}$ is a valid correction operation, then B is called a **Noiseless Subsystem**.
- We will sometimes refer to correctable subspaces and correctable subsystems as **Codes**.

Unitarily Correctable Codes

A code is said to be a **Unitarily-Correctable Code** (UCC) if it admits a unitary correction operation – a channel $\mathcal{U} = \{U\}$, where U is unitary.

Unitarily Correctable Codes

A code is said to be a **Unitarily-Correctable Code** (UCC) if it admits a unitary correction operation – a channel $\mathcal{U} = \{U\}$, where U is unitary.

- Unitarily-correctable codes are exactly the codes for which the correction operation can be implemented without a measurement.

Unitarily Correctable Codes

A code is said to be a **Unitarily-Correctable Code** (UCC) if it admits a unitary correction operation – a channel $\mathcal{U} = \{U\}$, where U is unitary.

- Unitarily-correctable codes are exactly the codes for which the correction operation can be implemented without a measurement.
- Noiseless subsystems and decoherence-free subspaces are both subclasses of unitarily-correctable codes.

The Multiplicative Domain

Given a CP map $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$, the **Multiplicative Domain** of Φ, denoted $MD(\Phi)$, is effectively the largest subalgebra of $\mathcal{L}(\mathcal{H})$ for which the restriction of Φ is a multiplicative map. That is,

$$MD(\Phi) := \big\{ a \in \mathcal{L}(\mathcal{H}) : \Phi(a)\Phi(b) = \Phi(ab) \text{ and } \Phi(b)\Phi(a) = \Phi(ba) \quad \forall\, b \in \mathcal{L}(\mathcal{H}) \big\}.$$

The Multiplicative Domain

Given a CP map $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$, the **Multiplicative Domain** of Φ, denoted $MD(\Phi)$, is effectively the largest subalgebra of $\mathcal{L}(\mathcal{H})$ for which the restriction of Φ is a multiplicative map. That is,

$$MD(\Phi) := \big\{ a \in \mathcal{L}(\mathcal{H}) : \Phi(a)\Phi(b) = \Phi(ab) \text{ and } \Phi(b)\Phi(a) = \Phi(ba) \quad \forall\, b \in \mathcal{L}(\mathcal{H}) \big\}.$$

- Notice that $MD(\Phi)$ is an algebra.

The Multiplicative Domain

Given a CP map $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$, the **Multiplicative Domain** of Φ, denoted $MD(\Phi)$, is effectively the largest subalgebra of $\mathcal{L}(\mathcal{H})$ for which the restriction of Φ is a multiplicative map. That is,

$$MD(\Phi) := \big\{ a \in \mathcal{L}(\mathcal{H}) : \Phi(a)\Phi(b) = \Phi(ab) \text{ and } \Phi(b)\Phi(a) = \Phi(ba) \quad \forall\, b \in \mathcal{L}(\mathcal{H}) \big\}.$$

- Notice that $MD(\Phi)$ is an algebra.
- We will now investigate what role (if any) that the multiplicative domain plays in quantum error correction.

Unital Maps

The following result of [Choi, '74] shows that the multiplicative domain simplifies considerably in the case of a unital map (ie. a map such that $\Phi(I) = I$).

Unital Maps

The following result of [Choi, '74] shows that the multiplicative domain simplifies considerably in the case of a unital map (ie. a map such that $\Phi(I) = I$).

Theorem

Let $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a completely positive, unital map. Then

$$MD(\Phi) = \big\{a \in \mathcal{L}(\mathcal{H}) : \Phi(a)^\dagger\Phi(a) = \Phi(a^\dagger a) \text{ and } \Phi(a)\Phi(a)^\dagger = \Phi(aa^\dagger)\big\}.$$

Unital Maps

The following result of [Choi, '74] shows that the multiplicative domain simplifies considerably in the case of a unital map (ie. a map such that $\Phi(I) = I$).

Theorem

Let $\Phi : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a completely positive, unital map. Then

$$MD(\Phi) = \big\{a \in \mathcal{L}(\mathcal{H}) : \Phi(a)^\dagger \Phi(a) = \Phi(a^\dagger a) \text{ and } \Phi(a)\Phi(a)^\dagger = \Phi(aa^\dagger)\big\}.$$

Note in particular that if $\mathcal{E}$ is a quantum channel, then this theorem applies to $\mathcal{E}^\dagger$.

Unital Channels

For unital quantum channels, we also have the following result due to [Kribs and Spekkens, '06].

Unital Channels

For unital quantum channels, we also have the following result due to [Kribs and Spekkens, '06].

Theorem

Let $\mathcal{E}$ be a unital quantum channel. Then the following are equivalent:

1. *B is a unitarily correctable subsystem for $\mathcal{E}$.*
2. *B is a noiseless subsystem for $\mathcal{E}^\dagger \circ \mathcal{E}$.*

Unital Channels

Kribs and Spekkens' Theorem shows that we may unambiguously define *the* UCC algebra for a unital channel $\mathcal{E} = \{E_i\}$ as

$$UCC(\mathcal{E}) := \{\rho : \mathcal{E}^\dagger \circ \mathcal{E}(\rho) = \rho\},$$

as we know from the theory of passive quantum error correction that the above algebra encodes all noiseless subsystems for $\mathcal{E}^\dagger \circ \mathcal{E}$ and is equal to the commutant of the operators $\{E_i^\dagger E_j\}$.

Unital Channels

Kribs and Spekkens' Theorem shows that we may unambiguously define *the* UCC algebra for a unital channel $\mathcal{E} = \{E_i\}$ as

$$UCC(\mathcal{E}) := \{\rho : \mathcal{E}^\dagger \circ \mathcal{E}(\rho) = \rho\},$$

as we know from the theory of passive quantum error correction that the above algebra encodes all noiseless subsystems for $\mathcal{E}^\dagger \circ \mathcal{E}$ and is equal to the commutant of the operators $\{E_i^\dagger E_j\}$.

Trying to define the UCC algebra of non-unital channels is problematic, as we will see an example where the smallest algebra containing the unitarily correctable codes is not itself correctable.

MD-UCC Theorem

We will now investigate how $UCC(\mathcal{E})$ is related to $MD(\mathcal{E})$ when $\mathcal{E}$ is a unital quantum channel.

MD-UCC Theorem

We will now investigate how $UCC(\mathcal{E})$ is related to $MD(\mathcal{E})$ when $\mathcal{E}$ is a unital quantum channel.

Theorem (MD-UCC)

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

1. $MD(\mathcal{E})$
2. $UCC(\mathcal{E})$
3. $\mathcal{E}^\dagger(MD(\mathcal{E}^\dagger))$
4. $\mathcal{E}^\dagger(UCC(\mathcal{E}^\dagger))$.

MD-UCC Theorem

We will now investigate how $UCC(\mathcal{E})$ is related to $MD(\mathcal{E})$ when $\mathcal{E}$ is a unital quantum channel.

Theorem (MD-UCC)

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

1. $MD(\mathcal{E})$
2. $UCC(\mathcal{E})$
3. $\mathcal{E}^\dagger(MD(\mathcal{E}^\dagger))$
4. $\mathcal{E}^\dagger(UCC(\mathcal{E}^\dagger))$.

The roles of $\mathcal{E}$ and $\mathcal{E}^\dagger$ can be switched in the statement of this theorem.

MD-UCC Theorem Example (Part I)

Let $I \in \mathcal{L}(\mathcal{H})$ be the identity on the Hilbert space $\mathcal{H}$ and let $q \in [0,1]$. Then consider the channel $\mathcal{E} : M_2(\mathcal{L}(\mathcal{H})) \mapsto M_2(\mathcal{L}(\mathcal{H}))$ given by the following four Kraus operators:

MD-UCC Theorem Example (Part I)

Let $I \in \mathcal{L}(\mathcal{H})$ be the identity on the Hilbert space $\mathcal{H}$ and let $q \in [0,1]$. Then consider the channel $\mathcal{E} : M_2(\mathcal{L}(\mathcal{H})) \mapsto M_2(\mathcal{L}(\mathcal{H}))$ given by the following four Kraus operators:

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

where $\alpha = \frac{\sqrt{q}}{\sqrt{2}}$ and $\beta = \frac{\sqrt{1-q}}{2}$.

MD-UCC Theorem Example (Part I)

Let $I \in \mathcal{L}(\mathcal{H})$ be the identity on the Hilbert space $\mathcal{H}$ and let $q \in [0,1]$. Then consider the channel $\mathcal{E} : M_2(\mathcal{L}(\mathcal{H})) \mapsto M_2(\mathcal{L}(\mathcal{H}))$ given by the following four Kraus operators:

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

where $\alpha = \frac{\sqrt{q}}{\sqrt{2}}$ and $\beta = \frac{\sqrt{1-q}}{2}$.

Notice that if $q = 0$ then this is in fact a unital quantum channel, so the MD-UCC Theorem applies to it.

MD-UCC Theorem Example (Part II)

It is not difficult to compute that

$$MD(\mathcal{E}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathcal{L}(\mathcal{H}) \right\}.$$

MD-UCC Theorem Example (Part II)

It is not difficult to compute that

$$MD(\mathcal{E}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathcal{L}(\mathcal{H}) \right\}.$$

The MD-UCC Theorem then implies that this algebra is exactly the algebra of unitarily correctable codes for $\mathcal{E}$.

MD-UCC Theorem Example (Part II)

It is not difficult to compute that

$$MD(\mathcal{E}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathcal{L}(\mathcal{H}) \right\}.$$

The MD-UCC Theorem then implies that this algebra is exactly the algebra of unitarily correctable codes for $\mathcal{E}$.

Indeed, it is not difficult to verify that this algebra encodes a pair of noiseless subsystems for $\mathcal{E}$.

Non-Unital Channels

For non-unital maps, the multiplicative domain shares a much weaker relationship with unitarily correctable codes than in the unital case; it is not difficult to construct counter-examples to almost every inclusion asserted by the MD-UCC theorem.

Non-Unital Channels

For non-unital maps, the multiplicative domain shares a much weaker relationship with unitarily correctable codes than in the unital case; it is not difficult to construct counter-examples to almost every inclusion asserted by the MD-UCC theorem.

However, one inclusion does still hold in the general setting:

Theorem

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

Non-Unital Channels Example (Part I)

Consider the same channel $\mathcal{E}$ defined earlier, but take $q = 1$. Then we can compute $MD(\mathcal{E}) = \{0\}$, so the multiplicative domain in this case does not capture any unitarily correctable codes.

Non-Unital Channels Example (Part I)

Consider the same channel $\mathcal{E}$ defined earlier, but take $q = 1$. Then we can compute $MD(\mathcal{E}) = \{0\}$, so the multiplicative domain in this case does not capture any unitarily correctable codes.

However, it is easily verified that the two subspaces defined by the ranges of the following two algebras are unitarily correctable:

$$\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \,\middle|\, a \in \mathcal{L}(\mathcal{H}) \right\} \quad \text{and} \quad \left\{ \begin{bmatrix} a & -a \\ -a & a \end{bmatrix} \,\middle|\, a \in \mathcal{L}(\mathcal{H}) \right\}.$$

Non-Unital Channels Example (Part I)

Consider the same channel $\mathcal{E}$ defined earlier, but take $q = 1$. Then we can compute $MD(\mathcal{E}) = \{0\}$, so the multiplicative domain in this case does not capture any unitarily correctable codes.

However, it is easily verified that the two subspaces defined by the ranges of the following two algebras are unitarily correctable:

$$\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \,\middle|\, a \in \mathcal{L}(\mathcal{H}) \right\} \quad \text{and} \quad \left\{ \begin{bmatrix} a & -a \\ -a & a \end{bmatrix} \,\middle|\, a \in \mathcal{L}(\mathcal{H}) \right\}.$$

This shows that even though anything captured by the multiplicative domain will be unitarily correctable, in general there will be unitarily correctable codes not captured by the multiplicative domain.

Non-Unital Channels Example (Part II)

Also, the smallest algebra containing both of the algebras described on the previous slide is simply

$$\left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathcal{L}(\mathcal{H}) \right\}.$$

Non-Unital Channels Example (Part II)

Also, the smallest algebra containing both of the algebras described on the previous slide is simply

$$\left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathcal{L}(\mathcal{H}) \right\}.$$

Notice that

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

so this algebra is certainly not unitarily correctable, as there is no way to recover the “b” blocks.

The Subspace Case

The following result is well-known in the world of quantum error correction. It shows that a channel looks like a special type of randomized unitary channel when restricted to a subspace if and only if that subspace is correctable.

The Subspace Case

The following result is well-known in the world of quantum error correction. It shows that a channel looks like a special type of randomized unitary channel when restricted to a subspace if and only if that subspace is correctable.

Lemma (Correctability on a Subspace)

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel and let $C \subseteq \mathcal{H}$ be a subspace. Then C is correctable for $\mathcal{E}$ if and only if there is a randomized unitary channel $\mathcal{F} = \left\{ \sqrt{p_i} U_i \right\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{L}(C)$ and $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$, where P_C is the orthogonal projection onto C.

The Subspace Case Example

Consider again the example introduced earlier with the following Kraus operators:

$$\mathcal{E} = \left\{ \alpha \begin{bmatrix} I & I \\ 0 & 0 \end{bmatrix}, \quad \alpha \begin{bmatrix} I & -I \\ 0 & 0 \end{bmatrix}, \quad \beta \begin{bmatrix} I & I \\ I & I \end{bmatrix}, \quad \beta \begin{bmatrix} -I & I \\ I & -I \end{bmatrix} \right\}.$$

The Subspace Case Example

Consider again the example introduced earlier with the following Kraus operators:

$$\mathcal{E} = \left\{ \alpha \begin{bmatrix} I & I \\ 0 & 0 \end{bmatrix}, \quad \alpha \begin{bmatrix} I & -I \\ 0 & 0 \end{bmatrix}, \quad \beta \begin{bmatrix} I & I \\ I & I \end{bmatrix}, \quad \beta \begin{bmatrix} -I & I \\ I & -I \end{bmatrix} \right\}.$$

We can see that the range of the operators living in the top-left corner forms a correctable subspace for $\mathcal{E}$ by observing that the randomized unitary channel $\mathcal{F}$ given by the following two Kraus operators:

$$\mathcal{F} = \left\{ \frac{\sqrt{1+q}}{\sqrt{2}} \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}, \quad \frac{\sqrt{1-q}}{\sqrt{2}} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \right\}$$

satisfies the conditions of the previous lemma.

The Subsystem Case (Part I)

The previous result can be generalized to show what a channel looks like when restricted to $1_A \otimes \mathcal{L}(B)$, where B is a correctable subsystem. This result was originally derived in [Kribs and Spekkens, '06].

The Subsystem Case (Part I)

The previous result can be generalized to show what a channel looks like when restricted to $1_A \otimes \mathcal{L}(B)$, where B is a correctable subsystem. This result was originally derived in [Kribs and Spekkens, '06].

Lemma (Correctability on $1_A \otimes \mathcal{L}(B)$)

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel and let $C = A \otimes B \subseteq \mathcal{H}$ be a subspace. Then B is correctable for $\mathcal{E}$ if and only if there is a completely positive (not necessarily trace-preserving) map $\mathcal{G} = \{U_i(D_i \otimes I_B)\}$ such that $\mathcal{E}(\rho) = \mathcal{G}(\rho)$ for all $\rho \in 1_A \otimes \mathcal{L}(B)$, $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$, and D_i is a positive diagonal operator for all i.

The Subsystem Case (Part II)

Most generally, this result can be generalized to show what a channel looks like when restricted to $\mathcal{L}(A \otimes B)$, where B is a correctable subsystem.

The Subsystem Case (Part II)

Most generally, this result can be generalized to show what a channel looks like when restricted to $\mathcal{L}(A \otimes B)$, where B is a correctable subsystem.

Lemma (Correctability on $\mathcal{L}(A \otimes B)$)

Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \mapsto \mathcal{L}(\mathcal{H})$ be a quantum channel and let $C \equiv A \otimes B \subseteq \mathcal{H}$ be a subspace. Then B is correctable for $\mathcal{E}$ if and only if there is a family of unitary operators $\{U_i\}$ with $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$ and quantum channels $\mathcal{N}_j : \mathcal{L}(A) \mapsto \mathcal{L}(A)$ with Kraus operators $\{N_{j,i}\}$ such that $\mathcal{E}(\rho) = \mathcal{F}(\rho)$ for all $\rho \in \mathcal{L}(C)$, where $\mathcal{F} = \{U_i(N_{j,i} \otimes I_B)\}$.

The Subspace Case

The previous results can in particular be used to derive a characterization of correctable subspaces and subsystems in terms of representations.

The Subspace Case

The previous results can in particular be used to derive a characterization of correctable subspaces and subsystems in terms of representations.

Theorem (Correctable Subspace Representation Theorem)

Let $C \subseteq \mathcal{H}$ be a subspace. Then the following are equivalent:

1. *C is a correctable subspace for $\mathcal{E}$.*
2. *$\exists$ a $\dagger$-homomorphism $\pi : \mathcal{L}(C) \mapsto \mathcal{L}(\mathcal{H})$ such that $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_C) = \mathcal{E}(P_C)\pi(\rho) \quad \forall\, \rho \in \mathcal{L}(C)$.*

The Subspace Case

The idea of the proof for the Correctable Subspace Representation Theorem is that if the subspace C is correctable for $\mathcal{E}$ then the Subspace Correctability Lemma says that there exist unitaries $\{U_i\}$ such that $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$ and $\mathcal{E}(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ for all $\rho \in \mathcal{L}(C)$.

The Subspace Case

The idea of the proof for the Correctable Subspace Representation Theorem is that if the subspace C is correctable for $\mathcal{E}$ then the Subspace Correctability Lemma says that there exist unitaries $\{U_i\}$ such that $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$ and $\mathcal{E}(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ for all $\rho \in \mathcal{L}(C)$.

The $\dagger$-homomorphism given by $\pi(\rho) = \sum_i U_i \rho U_i^\dagger$ then satisfies the conditions of the theorem.

The Subspace Case

The idea of the proof for the Correctable Subspace Representation Theorem is that if the subspace C is correctable for $\mathcal{E}$ then the Subspace Correctability Lemma says that there exist unitaries $\{U_i\}$ such that $P_C U_i^\dagger U_j P_C = 0$ for all $i \neq j$ and $\mathcal{E}(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ for all $\rho \in \mathcal{L}(C)$.

The $\dagger$-homomorphism given by $\pi(\rho) = \sum_i U_i \rho U_i^\dagger$ then satisfies the conditions of the theorem.

It also comes out of the proof of the theorem that the correction operation $\mathcal{R}$ satisfies $\mathcal{R}|_{\mathcal{E}(\mathcal{L}(C))} = \pi^\dagger|_{\mathcal{E}(\mathcal{L}(C))}$.

The Subspace Case Example

Returning one final time to our example, we see that if $0 < q < 1$ for the channel $\mathcal{E}$ and the correctable subspace defined earlier, then

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

The Subspace Case Example

Returning one final time to our example, we see that if $0 < q < 1$ for the channel $\mathcal{E}$ and the correctable subspace defined earlier, then

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

Similarly, we can compute that

$$\mathcal{R}(\sigma) := \begin{bmatrix} \pi^{\dagger}(\sigma) & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} Tr_1(\sigma) & 0 \\ 0 & 0 \end{bmatrix}$$

is a valid correction operation for this subspace.

The Subsystem Case

The theorem for the subsystem setting is quite similar to the Correctable Subspace Representation Theorem.

The Subsystem Case

The theorem for the subsystem setting is quite similar to the Correctable Subspace Representation Theorem.

Theorem (Correctable Subsystem Representation Theorem)

Let $C = A \otimes B \subseteq \mathcal{H}$ be a subspace. The following are equivalent:

1. *B is a correctable subsystem for $\mathcal{E}$.*
2. *$\exists$ a †-homomorphism $\pi : 1_A \otimes \mathcal{L}(B) \mapsto \mathcal{L}(\mathcal{H})$ such that* $\mathcal{E}(\rho) = \pi(\rho)\mathcal{E}(P_C) = \mathcal{E}(P_C)\pi(\rho) \quad \forall\, \rho \in 1_A \otimes \mathcal{L}(B)$.

Conclusions and Future Work

- We have seen that the multiplicative domain can be used to characterize unitarily correctable subsystems for unital channels.

Conclusions and Future Work

- We have seen that the multiplicative domain can be used to characterize unitarily correctable subsystems for unital channels.
- We have also seen that there is a natural characterization of correctable codes as "smeared" representations.

Conclusions and Future Work

- We have seen that the multiplicative domain can be used to characterize unitarily correctable subsystems for unital channels.
- We have also seen that there is a natural characterization of correctable codes as "smeared" representations.
- Are there natural sets (perhaps analogous to the multiplicative domain) that capture all codes?

Bibliography

- M.-D. Choi, Illinois J. Math., **18** (1974), 565-574.
- D. W. Kribs, R. W. Spekkens, *Quantum error correcting subsystems are unitarily recoverable subsystems*, Physical Review A, **74**, 042329 (2006).