Stabilized Distance Measures and Quantum Error Correction

Nathaniel D. Johnston

June 19, 2008

1. Introduction and Preliminaries
2. CB and $\diamond$ Norms
3. Quantum Error Correction
4. Conclusions and Future Work

Notation and Preliminaries

Throughout this defence, the following notational conventions will be used:

- M_n denotes the set of $n \times n$ complex matrices
- $M_n(V)$ denotes the set of $n \times n$ matrices with entries from the ring V
- $(a_{ij}) \in M_n(V)$ denotes the element of $M_n(V)$ with a_{ij} in its (i, j)-entry

Notation and Preliminaries

The slides to follow will focus on linear maps $\phi : M_n \mapsto M_k$. This is a simplification that is made for brevity's sake; many of the results to be presented extend in a straightforward manner to maps between general operator spaces, operator systems, or C*-algebras.

Positive and Completely Positive Maps

From ϕ one can construct a family of maps $\phi_m : M_m(M_n) \mapsto M_m(M_k)$ $(m \geq 1)$ by setting

$$\phi_m((a_{ij})) \equiv (\phi(a_{ij})) = \begin{bmatrix} \phi(a_{11}) & \phi(a_{12}) & \cdots & \phi(a_{1m}) \\ \phi(a_{21}) & \phi(a_{22}) & \cdots & \phi(a_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(a_{m1}) & \phi(a_{m2}) & \cdots & \phi(a_{mm}) \end{bmatrix}.$$

Let $\phi : M_n \mapsto M_k$ be a linear map. ϕ is said to be **positive** if it maps positive-semidefinite elements of M_n to positive-semidefinite elements of M_k.

Positive and Completely Positive Maps

Building from this idea, some new classes of maps can be defined:

Definition
The map ϕ is said to be ***m-positive*** *if ϕ_m is positive.*

Definition
The map ϕ is said to be ***completely positive*** *(CP) if it is m-positive $\forall m \geq 1$.*

Positive and Completely Positive Maps

Theorem (Choi-Kraus Representation Theorem)

Let $\phi : M_n \mapsto M_k$ be a linear map. Then ϕ is completely positive if and only if there exist matrices $A_i \in M_{k,n}, 1 \leq i \leq nk$, such that $\phi(a) = \sum_i A_i a A_i^\dagger$ for all $a \in M_n$.

Note that the matrices described by this theorem are not unique. Nevertheless, when speaking about a completely positive map $\phi : M_n \mapsto M_k$, a family of matrices $\{A_i\}$ as described by the Choi-Kraus representation theorem is called a **Choi-Kraus representation** of ϕ, and the operators themselves are known as its **Kraus operators**.

Positive and Completely Positive Maps

Given a completely positive map $\phi = \{A_i\}$, one can construct its *dual map* by setting $\phi^\dagger = \{A_i^\dagger\}$.

The dual map is actually defined in terms of the Hilbert-Schmidt inner product. The definition given here is less mathematically enlightening but easier to grasp in the context of a brief talk.

Completely Bounded Maps

Definition

Let $\phi : M_n \mapsto M_k$ be a linear map. It is said that ϕ is **completely bounded** *if*

$$\|\phi\|_{cb} \equiv \sup_m \|\phi_m\|$$

is finite. Here
$||\phi_m|| = \sup\left\{||\phi_m((a_{ij}))|| \, : \, (a_{ij}) \in M_m(M_n), \, ||(a_{ij})|| \leq 1\right\}.$

Linear maps are always completely bounded if their domain space is M_n, but this is not true if the domain is a general operator space.

Completely Bounded Maps

Theorem (CB Representation Theorem)

Let $\phi : M_n \mapsto M_k$ be a linear map. Then there exist matrices $A_i \in M_{k,n}, 1 \leq i \leq nk$, and matrices $B_i \in M_{n,k}, 1 \leq i \leq nk$, such that

$$\phi(a) = \sum_{i=1}^{nk} A_i a B_i,$$

with $\|\phi\|_{cb}^2 = \|\sum_i A_i A_i^\dagger\| \|\sum_i B_i^\dagger B_i\|$.

A representation of a completely bounded map ϕ as described by the CB representation theorem is called a **generalized Choi-Kraus representation** of ϕ.

Completely Bounded Maps

As was the case with completely positive maps, this representation of a given completely bounded map is not unique.

Note that if $\phi(a) = \sum_i C_i a D_i$ then in general $\|\phi\|_{cb}^2 \leq \|\sum_i C_i C_i^\dagger\| \|\sum_i D_i^\dagger D_i\|$. The previous theorem does not say that equality holds for *any* generalized Choi-Kraus representation, but merely that it holds for *some* generalized Choi-Kraus representation.

Representing Quantum Information

Definition

A matrix $\rho \in M_n$ is said to be a **density matrix** *if it is Hermitian, positive-semidefinite and has $\mathrm{Tr}(\rho) = 1$.*

It turns out that density matrices provide a convenient way of representing quantum states. With this in mind, it is not surprising that we can model the evolution of quantum states by a linear map $\phi : M_n \mapsto M_n$ that is positive and preserves traces. It turns out that complete positivity is actually required, and this leads to the following definition.

Representing Quantum Information

Definition

A completely positive, trace-preserving linear map $\mathcal{E} : M_n \mapsto M_n$ is called a **quantum channel** *or a* **quantum operation**.

If $\mathcal{E} = \{E_i\}$ is a quantum channel then it is not difficult to see that the trace-preservation requirement of $\mathcal{E}$ is equivalent to the requirement that $\sum_i E_i^\dagger E_i = I_n$.

Representing Quantum Information

One is often interested in differences $\mathcal{E} - \mathcal{F}$ between pairs of quantum channels. Such a difference is still completely bounded, though not necessarily completely positive. Indeed, the linear span of the completely positive maps is exactly the set of completely bounded maps – a fact that is implied by the following theorem.

Theorem (Wittstock's Decomposition Theorem)

Let $\phi : M_n \mapsto M_k$ be completely bounded. Then ϕ can be written as a linear combination of four or fewer completely positive maps.

Stabilized Norms

Recall that the completely bounded (CB) norm has already been defined for a linear map ϕ as

$$\|\phi\|_{cb} \equiv \sup_m \|\phi_m\|,$$

where $\|\phi_m\|$ is the standard operator norm of ϕ_m.

The CB norm has been studied for years in operator theory, and it turns out that it is intimately related to a norm that has been used extensively in quantum information theory.

Stabilized Norms

Given a linear map $\phi : M_n \mapsto M_k$, we can define its diamond ($\diamond$) norm as

$$\|\phi\|_\diamond \equiv \|\phi_n\|_1,$$

where $\|\phi_n\|_1 = \sup_{||a||_1 \leq 1} ||\phi_n(a)||_1$, where $a \in M_n(M_n)$ and $||a||_1 = \mathrm{Tr}(\sqrt{a^\dagger a})$.

Stabilized Norms

The reason that these two norms are important for quantum information theory is that they both satisfy the **stabilization property** for distance measures of quantum channels:

$$d(\mathcal{E}_m, \mathcal{F}_m) = d(\mathcal{E}, \mathcal{F}) \quad \forall m \geq 1.$$

This property ensures that the distance between maps is unaffected by any ancillary quantum system that is independent of the original system.

Stabilized Norms

To relate the CB and $\diamond$ norms, a theorem is now presented:

Theorem

Let $\phi : M_n \mapsto M_k$ be a linear map. Then

$$\|\phi\|_{cb} = \|\phi^\dagger\|_\diamond = \|\phi_k\| \leq min\{k, \sqrt{n^3}\}\|\phi\|.$$

This theorem provides a bridge that allows decades of study of the CB norm to be applied to the $\diamond$ norm. The discussion to follow will focus primarily on computing the CB norm of a linear map, but it all applies to the $\diamond$ norm in a straightforward manner.

Computing the CB Norm

Theorem

Let $\phi : M_n \to M_k$ be a completely positive map. Then ϕ is completely bounded and $\|\phi\|_{cb} = \|\phi\| = \|\phi(1)\|$.

In this finite-dimensional setting, it is easy to see this result since we already know by the CB representation theorem that $\|\phi\|_{cb}^2 = \|\sum_i A_i A_i^\dagger\| \|\sum_i B_i^\dagger B_i\|$, where the A_i and B_i matrices form some generalized Choi-Kraus representation of ϕ. Since $B_i = A_i^\dagger$ for a completely positive map, the result follows easily.

Computing the CB Norm

Computing the CB norm of an arbitrary CB map is not as simple as with a CP map. For an arbitrary CB map, we may compute its norm through the following algorithm, which will be outlined in 4 steps. Assume to begin that you know a generalized Choi-Kraus representation of the CB map and it has generalized Choi-Kraus operators $\{A_i\}$ and $\{B_i\}$.

Step 1. Find a basis, $\{C_1, ..., C_l\}$ for the span of $\{B_1, ..., B_m\}$ and express

$$B_i = \sum_j d_{i,j} C_j.$$

Computing the CB Norm

Step 2. Using the expressions for each B_i as a linear combination of C_j one may re-write $\phi(a) = \sum_{j=1}^{l} D_j a C_j$.
In fact,

$$\phi(a) = \sum_i A_i a \Big(\sum_j d_{i,j} C_j \Big) = \sum_j \Big(\sum_i d_{i,j} A_i \Big) a C_j.$$

Thus,

$$D_j = \sum_i d_{i,j} A_i.$$

Computing the CB Norm

Step 3. Find a basis $\{E_1, ..., E_p\}$ for the span of $\{D_1, ..., D_l\}$ and express each D_j as a linear combination of E_i's.
Repeat Step 2 to obtain

$$\phi(a) = \sum_{i=1}^{p} E_i a F_i,$$

where the F_i's are the corresponding linear combinations of the C_j's.

Now it is a theorem that says that the sets $\{E_1, ..., E_p\}$ and $\{F_1, ..., F_p\}$ are linearly independent, and hence this process terminates.

Computing the CB Norm

Step 4. Given an invertible $S = (s_{i,j}) \in M_p$ with inverse $S^{-1} = (t_{i,j}) \in M_p$, let $H_i = \sum_j s_{i,j} F_j$, and $G_j = \sum_i t_{i,j} E_i$. Then

$$\|\phi\|_{cb} = \inf \Big\{ \big\| \sum_i G_i G_i^\dagger \big\|^{\frac{1}{2}} \big\| \sum_i H_i^\dagger H_i \big\|^{\frac{1}{2}} \Big\},$$

where the infimum is taken over all invertible matrices S.

Alternatively, the minimization of Step 4 can be re-written as

$$\inf \Big\{ \big\| \begin{bmatrix} E_1 & \cdots & E_p \end{bmatrix} (S^{-1} \otimes I_n) \big\| \big\| \begin{bmatrix} F_1^\dagger & \cdots & F_p^\dagger \end{bmatrix} (S^\dagger \otimes I_n) \big\| \Big\},$$

where the infimum is taken over all invertible matrices S.

Computing the CB Norm

This algorithm reduces the computation of $\|\phi\|_{cb}$ to a series of matrix computations and only the last step might involve a difficult minimization.

I will present a theorem that shows how to compute the CB norm of one particular family of maps, but in general the best we can do is approximate this final minimization by selecting several matrices S and taking the smallest resulting norm estimate.

Difference of Unitary Maps

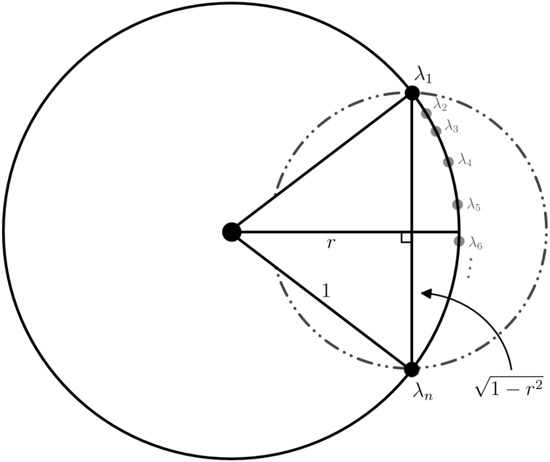
The following theorem was proved using the previously-outlined algorithm. It provides the exact stabilized norm for difference of unitary maps.

Theorem

Let $U \in M_n$ be a unitary operator and let $\phi : M_n \mapsto M_n$ be given by $\phi(a) = UaU^\dagger - a$. Then $\|\phi\|_{cb} = \|\phi^\dagger\|_{cb} = \|\phi\|_\diamond = \|\phi^\dagger\|_\diamond$ is equal to the diameter of the smallest closed disc in $\mathbb{C}$ that contains all of the eigenvalues of U.

Note that by the unitary invariance of the CB/$\diamond$ norm, observe that we can compute the norm of any map $\mathcal{U} - \mathcal{V}$ once we know how to compute it for any map of the form $\mathcal{U} - \mathrm{id}$.

Difference of Unitary Maps



Difference of Unitary Maps

The algorithm has been implemented in MATLAB by repeatedly randomly generating matrices to approximate Step 4 and taking the smallest resulting norm estimate.

As a simple example, let U be a 3×3 unitary matrix with eigenvalues $e^{\left(\frac{5i\pi}{4}\right)}$, $e^{(i\pi)}$, and $e^{\left(\frac{3i\pi}{4}\right)}$. Then the MATLAB code estimates the CB norm of the map $\phi(a) = U^\dagger a U - a$ as 1.4390 in about half of a second based on 1,000 iterations. The earlier theorem says however that $\|\phi\|_{cb} = \sqrt{2}$, so the computed estimate has a relative error of about 1.75%.

Correctable Subspaces

Focus will now be shifted from stabilized norms to the problem of quantum error correction. Though these two topics are related, for example, through the concept of approximately correctable codes, focus here will be restricted to perfectly correctable codes.

Correctable Subspaces

Let $\mathcal{E} : M_n \mapsto M_n$ be a quantum channel. If $\mathcal{C} \subseteq \mathbb{C}_n$ is a subspace, then $\mathcal{C}$ is said to be a **correctable subspace** if there exists another quantum channel $\mathcal{R} : M_n \mapsto M_n$ such that

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

where $\mathcal{B}(\mathcal{C})$ in this context means the set of linear operators acting on the subspace $\mathcal{C}$.

$\mathcal{R}$ is called a **correction operation**. If $\mathcal{R} = id_{M_n}$ is a valid correction operation, then $\mathcal{C}$ is called a **decoherence-free subspace**.

Correctable Subspaces

It is well-known that $\mathcal{C}$ being correctable is equivalent to the existence of constants $\{\lambda_{ij}\}$ such that:

$$P_{\mathcal{C}} E_i^\dagger E_j P_{\mathcal{C}} = \lambda_{ij} P_{\mathcal{C}} \quad \forall\, i, j, \tag{1}$$

where $P_{\mathcal{C}}$ is the orthogonal projection onto $\mathcal{C}$. These matrix equations are known as the **Knill-Laflamme conditions** and are easily checked once a given subspace $\mathcal{C}$ is proposed as correctable.

Correctable Subspaces

From the Knill-Laflamme conditions it is not difficult to derive a well-known result that shows what channels look like when restricted to their correctable subspaces.

Lemma

If $\mathcal{C} \subseteq \mathbb{C}_n$ is a subspace, then $\mathcal{C}$ 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 $\rho \in \mathcal{B}(\mathcal{C})$ and $P_{\mathcal{C}} U_i^\dagger U_j P_{\mathcal{C}} = 0$ for all $i \neq j$.

Correctable Subspaces

This result can be used to prove a new characterization of correctable subspaces in terms of representation theory.

Theorem

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

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

Furthermore, the correction operation looks like $\pi^\dagger$ when restricted to $\mathcal{E}\big(\mathcal{B}(\mathcal{C})\big)$.

Correctable Subspace Example

By following along through the proofs of the previous two results, a method for explicitly computing the correction operation given a correctable subspace for $\mathcal{E}$ immediately becomes clear.

The details of this procedure will not be provided here, but an example is presented to clarify the results.

Correctable Subspace Example

Let I_2 be the 2×2 identity matrix, let $U \in M_2$ and $V \in M_2$ be unitary matrices, and let $q \in [0, 1)$. Then consider the channel $\mathcal{E} : M_4 \mapsto M_4$ given by the 4 Kraus operators in the standard basis

$$E_1 = \alpha \begin{bmatrix} I_2 & U \\ 0 & 0 \end{bmatrix} \qquad E_2 = \alpha \begin{bmatrix} I_2 & -U \\ 0 & 0 \end{bmatrix}$$

$$E_3 = \beta \begin{bmatrix} I_2 & V \\ I_2 & V \end{bmatrix} \qquad E_4 = \beta \begin{bmatrix} I_2 & -V \\ -I_2 & V \end{bmatrix},$$

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

Correctable Subspace Example

It is straightforward to verify that $\sum_{i=1}^{4} E_i^\dagger E_i = I_4$ and so $\mathcal{E}$ is a valid quantum channel. Also, let's focus on the subspace defined by $\mathcal{C} \equiv \text{span}\left\{ \begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}^T, \begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}^T \right\}$. Then

$$P_{\mathcal{C}} = \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix}.$$

We will see that $\mathcal{C}$ is indeed a correctable subspace for $\mathcal{E}$ by using the Knill-Laflamme conditions, and then the results of the preceding theorem and lemma will be applied to that subspace.

Correctable Subspace Example

Indeed, let's first verify that the Knill-Laflamme conditions are satisfied for $\mathcal{C}$ and thus that $\mathcal{C}$ really is a correctable subspace for $\mathcal{E}$:

$$P_{\mathcal{C}}E_3^\dagger E_4 P_{\mathcal{C}} = 0$$

$$P_{\mathcal{C}}E_3^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}}E_4^\dagger E_4 P_{\mathcal{C}} = \left(\frac{1-q}{2}\right)P_{\mathcal{C}}$$

$$P_{\mathcal{C}}E_1^\dagger E_1 P_{\mathcal{C}} = P_{\mathcal{C}}E_2^\dagger E_2 P_{\mathcal{C}} = P_{\mathcal{C}}E_1^\dagger E_2 P_{\mathcal{C}} = \frac{q}{2}P_{\mathcal{C}}$$

$$P_{\mathcal{C}}E_1^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}}E_1^\dagger E_4 P_{\mathcal{C}} = P_{\mathcal{C}}E_2^\dagger E_3 P_{\mathcal{C}} = P_{\mathcal{C}}E_2^\dagger E_4 P_{\mathcal{C}} = \left(\frac{\sqrt{q-q^2}}{2\sqrt{2}}\right)P_{\mathcal{C}}.$$

Correctable Subspace Example

Well, it looks like the Knill-Laflamme conditions are satisfied and so $\mathcal{C}$ really is a correctable subspace for $\mathcal{E}$.

The earlier lemma then says that there exists a randomized unitary channel $\mathcal{F}$ such that $\mathcal{E}|_{\mathcal{C}} = \mathcal{F}|_{\mathcal{C}}$.

Indeed, if one recalls the Pauli X matrix $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ then it is not difficult to verify that $\mathcal{F} = \big\{ \frac{\sqrt{1+q}}{\sqrt{2}} I_2 \otimes I_2, \frac{\sqrt{1-q}}{\sqrt{2}} X \otimes I_2 \big\}$ is such a channel because for all $\rho \in M_2$ it is the case that

$$\mathcal{E}\Big(\begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix} \Big) = \begin{bmatrix} \big(\frac{1+q}{2}\big)\rho & 0 \\ 0 & \big(\frac{1-q}{2}\big)\rho \end{bmatrix} = \mathcal{F}\Big(\begin{bmatrix} \rho & 0 \\ 0 & 0 \end{bmatrix} \Big).$$

Correctable Subspace Example

Finally, the correction operation $\mathcal{R}$ and †-homomorphism π described by the earlier theorem are given by:

$$\mathcal{R} = \left\{ \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & I_2 \\ 0 & 0 \end{bmatrix} \right\}$$

and

$$\pi(\rho) = \begin{bmatrix} \rho & 0 \\ 0 & \rho \end{bmatrix} \quad \forall\, \rho \in M_2.$$

Correctable Subsystems

The results presented thus far for correctable subspaces all extend very naturally to correctable *subsystems*. These results are omitted for the sake of brevity, but they're all very pretty.

Computing Stabilized Norm Conclusions

It was seen that the algorithm presented earlier can be used to compute the exact stabilized norm for certain families of maps.

The algorithm has also been implemented in MATLAB and can provide estimates of the stabilized norm for arbitrary linear maps.

Can the algorithm be modified to compute the exact stabilized norm of arbitrary linear maps?

Quantum Error Correction Conclusions

Some results were presented that showed what channels look like on their correctable subspaces.

These results can be used to compute a correction operation once a subspace has been proposed as correctable.

Can we use these results to help us find correctable subspaces?

Acknowledgments and Thanks

- My advisors David and John
- My committees
- Kathryn
- My parents
- Everyone here for showing up