Linear Preserver Problems in Quantum Information Theory

Nathaniel Johnston

University of Guelph

October 5, 2010

What is a Linear Preserver Problem?

A linear preserver problem is the problem of characterizing linear maps on complex matrices (i.e., superoperators) that preserve some property of those matrices. For example, we could ask...

- What maps send nonsingular matrices to nonsingular matrices?
- What maps preserve the singular values of the matrices they act on?
- What maps send positive semidefinite matrices to positive semidefinite matrices?

What is a Linear Preserver Problem?

Note that the matrix transpose map works for each of those problems. That is, if M_n is the space of complex $n \times n$ matrices and X^T denotes the transpose (x_{ji}) of a matrix $X = (x_{ij}) \in M_n$, then...

- If X is nonsingular, then so is X^T.
- The singular values of X^T are the same as the singular values of X.
- If X is positive semidefinite (i.e., $X \geq 0$), then $X^T \geq 0$.

We will see repeatedly throughout this talk that the transpose map is quite special indeed.

What is a Linear Preserver Problem?

Before getting into the structure of linear maps that preserve certain properties of matrices, we should first characterize linear maps on complex matrices themselves.

Theorem

$\Phi : M_n \to M_n$ is linear if and only if there exist families of matrices $\{A_i\}$ and $\{B_i\}$ such that

$$\Phi(X) \equiv \sum_{i=1}^{n^2} A_i X B_i.$$

Invertibility Preservers

One of the earliest linear preserver problems was the problem of characterizing linear maps that send nonsingular matrices to nonsingular matrices, which was solved in 1949 by Dieudonné.

Theorem

Let $\Phi : M_n \to M_n$ be an invertible linear map. Then $\Phi(X)$ is nonsingular whenever $X \in M_n$ is nonsingular if and only if there exist nonsingular $A, B \in M_n$ such that either

$$\Phi(X) \equiv AXB \quad \textit{or} \quad \Phi(X) \equiv AX^TB.$$

Singular Value Preservers

The characterization of invertibility-preserving maps is extremely useful because it allows us to easily derive the answer to other linear preserver problems. For example, we can derive the structure of maps that preserve singular values as follows:

- Recall a square matrix is nonsingular if and only if it does not have a zero singular value. Thus, any map Φ that preserves singular values is invertibility-preserving.
- By the result on the previous slide there exist nonsingular $A, B \in M_n$ such that either

$$\Phi(X) \equiv AXB \quad \text{or} \quad \Phi(X) \equiv AX^T B.$$

- Argue that if Φ preserves singular values then A and B are both unitary.

Singular Value Preservers

What we sketched on the previous slide was a proof of the following result:

Theorem

Let $\Phi : M_n \to M_n$ be a linear map. Then the singular values of $\Phi(X)$ equal the singular values of X for all $X \in M_n$ if and only if there exist unitary matrices $U, V \in M_n$ such that either

$$\Phi(X) \equiv UXV \quad \textit{or} \quad \Phi(X) \equiv UX^TV.$$

Positivity Preservers

The linear preserver problems that we have seen so far have had relatively simple answers. But what about the problem of characterizing maps that send positive semidefinite matrices to positive semidefinite matrices?

- That is, $\Phi(X) \geq 0$ whenever $X \geq 0$.
- Such maps are called **positive**.
- Finding a characterization of these maps is an open problem!
- Deciding whether or not Φ is positive is NP-HARD. 

Completely Positive Maps

Fortunately, in quantum information theory we aren't as interested in positive maps as we are in **completely positive** maps (i.e., maps such that $id_n \otimes \Phi$ is positive for any $n \geq 1$).

The following result of Choi is well-known to the quantum information theory crowd:

Theorem

Let $\Phi : M_n \rightarrow M_n$ be a linear map. Then Φ is completely positive if and only if there exists a family of matrices $\{A_i\}$ such that

$$\Phi(X) \equiv \sum_{i=1}^{n^2} A_i X A_i^*.$$

Rank Preservers

One fundamental type of linear preserver problems is the family of problems that ask for characterizations of maps that preserve certain aspects of matrix rank. For example...

- Dieudonné's theorem about invertibility-preserving maps characterizes maps that send rank-n matrices to rank-n matrices.
- Another classical result says that if an invertible map sends rank-1 matrices to rank-1 matrices, it must also be of the form described by Dieudonné's theorem.

Rank Preservers

A much stronger version of those results is the following theorem, which was proved by Botta in 1978.

Theorem

Let $\Phi : M_n \to M_n$ be an invertible linear map and let $k < n$. Then $\mathrm{rank}(\Phi(X)) \leq k$ whenever $\mathrm{rank}(X) \leq k$ ($X \in M_n$) if and only if there exist nonsingular $A, B \in M_n$ such that either

$$\Phi(X) \equiv AXB \quad \text{or} \quad \Phi(X) \equiv AX^T B.$$

Matrix Norm Isometries

In the introductory section we saw a characterization of linear maps that preserve singular values of matrices. But what if we look at linear maps that preserve unitarily-invariant norms (which are just functions of singular values)?

- What are the isometries of the operator norm $\|\cdot\|$ (= the largest singular value)?
- What are the isometries of the trace norm $\|\cdot\|_{tr}$ (= the sum of the singular values)?
- What are the isometries of the Frobenius norm $\|\cdot\|_F$ (= the Euclidean norm of the vector of singular values)?

Operator Norm and Trace Norm Isometries

It is not difficult to show that if a linear map preserves the operator norm or the trace norm, then it must actually preserve all singular values. That is, we have the following result:

Theorem

Let $\Phi : M_n \to M_n$ be a linear map. Then the following are equivalent:

1. $\big\|\Phi(X)\big\| = \big\|X\big\|$ *for all* $X \in M_n$.
2. $\big\|\Phi(X)\big\|_{tr} = \big\|X\big\|_{tr}$ *for all* $X \in M_n$.
3. *There exist unitary matrices* $U, V \in M_n$ *such that either*

$$\Phi(X) \equiv UXV \quad \text{or} \quad \Phi(X) \equiv UX^TV.$$

Frobenius Norm Isometries

To understand the isometries of the Frobenius norm, it helps to introduce some basic quantum information theory concepts.

- We will write unit (column) vectors in $\mathbb{C}^n$ as "kets": $|v\rangle \in \mathbb{C}^n$. Dual (row) vectors are written as "bras": $\langle v| := |v\rangle^*$.
- Unit vectors $|v\rangle \in \mathbb{C}^n$ represent pure quantum states.
- We are often interested in pure states in $\mathbb{C}^n \otimes \mathbb{C}^n$. A state of the form $|v_1\rangle \otimes |v_2\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is said to be **separable**.

Frobenius Norm Isometries

There is a natural isomorphism between $\mathbb{C}^n \otimes \mathbb{C}^n$ and M_n. Simply associate the separable state $|v\rangle := |v_1\rangle \otimes |v_2\rangle$ with the rank-1 matrix $X_{|v\rangle} := |v_1\rangle\overline{\langle v_2|}$ and extend linearly.

- Under this isomorphism, separable pure states correspond to rank-1 matrices.
- The isomorphism is isometric if the norm on $\mathbb{C}^n \otimes \mathbb{C}^n$ is the Euclidean norm and the norm on M_n is the Frobenius norm.
- The isomorphism relates superoperators and operators as follows:

$$\sum_i A_i X_{|v\rangle} B_i = X_{|w\rangle}, \text{ where } |w\rangle = \left(\sum_i A_i \otimes B_i^T \right) |v\rangle.$$

Frobenius Norm Isometries

It follows that a superoperator preserves the Frobenius norm if and only if the operator associated to it through this isomorphism is unitary.

In other words, the super operator

$$\Phi(X) \equiv \sum_i A_i X B_i$$

is an isometry of the Frobenius norm if and only if the operator

$$\sum_i A_i \otimes B_i^T$$

is unitary.

Unitarily-Invariant Norm Isometries

A beautiful result of Sourour (1981) says that the Frobenius norm is in some sense unique with regards to its isometries – it is the only unitarily-invariant norm that has an isometry group different from the operator norm:

Theorem

Let $\Phi : M_n \rightarrow M_n$ be a linear map and let $\|\cdot\|_{ui}$ be a unitarily-invariant norm that is not a multiple of the Frobenius norm. Then Φ is an isometry of $\|\cdot\|_{ui}$ if and only if there exist unitary matrices $U, V \in M_n$ such that either

$$\Phi(X) \equiv UXV \quad \text{or} \quad \Phi(X) \equiv UX^TV.$$

Operators Preserving Separability (and Schmidt Rank)

Recall that any pure state of the form $|v_1\rangle \otimes |v_2\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is called separable. A natural generalization of separability is the notion of Schmidt rank...

Definition

The **Schmidt rank** *of a pure state $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$, denoted $SR(|v\rangle)$, is the least natural number k such that $|v\rangle$ can be written as a linear combination of k separable pure states.*

Operators Preserving Separability (and Schmidt Rank)

Some notes regarding the Schmidt rank are in order...

- $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is separable if and only if $SR(|v\rangle) = 1$.
- For any $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$, we have $1 \leq SR(|v\rangle) \leq n$.
- Recall the isomorphism that associates $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ with $X_{|v\rangle} \in M_n$ from earlier. Then $SR(|v\rangle) = \mathrm{rank}(X_{|v\rangle})$.

Operators Preserving Separability (and Schmidt Rank)

But wait, we already know the structure of superoperators that preserve the set of matrices with rank at most k.

So by using our favourite isomorphism again, we immediately get the following result, which characterizes operators that preserve the set of pure states with Schmidt rank at most k...

Operators Preserving Separability (and Schmidt Rank)

Theorem

Let $U \in M_n \otimes M_n$ and $1 \leq k < n$. Define

$$\mathcal{S}_k := \big\{ |v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n : SR(|v\rangle) \leq k \big\}.$$

Then $U\mathcal{S}_k \subseteq \mathcal{S}_k$ if and only if there exist unitaries $V, W \in M_n$ such that either

$$U = V \otimes W \quad \text{or} \quad U = S(V \otimes W),$$

where S is the "swap operator" defined by $S(|a\rangle \otimes |b\rangle) = |b\rangle \otimes |a\rangle$ for all $|a\rangle, |b\rangle \in \mathbb{C}^n$.

Operators Preserving Mixed Separability

The theorem on the previous slide, in the $k = 1$ case, characterized operators that send separable **pure** states to separable pure states. But what about **mixed** states?

A general quantum state is represented by a **density operator**: a positive semidefinite operator with trace 1.

If a density operator ρ can be written in the form $\rho = \sum_i |v_i\rangle\langle v_i|$, where each $|v_i\rangle$ is a separable pure state, then ρ is said to be separable.

Open Problem: If $\Phi(\rho)$ is separable whenever ρ is separable, what can we say about Φ? Does it have a nice form analogous to the form of operators that preserve pure state separability?

Isometries of s(k)- and S(k)-Norms

There are two families of norms based on the Schmidt rank of pure states that come up from time to time in quantum information theory. One family of norms for vectors $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ and one family of norms for matrices $X \in M_n \otimes M_n$:

$$\big\| |v\rangle \big\|_{s(k)} := \sup_{|w\rangle} \big\{ |\langle w|v\rangle| : SR(|w\rangle) \leq k \big\}$$

$$\big\| X \big\|_{S(k)} := \sup_{|v\rangle,|w\rangle} \big\{ |\langle w|X|v\rangle| : SR(|v\rangle), SR(|w\rangle) \leq k \big\}.$$

Isometries of s(k)-Norms

For the vector norms, we have the following result that says that $\big\||v\rangle\big\|_{s(k)}$ is actually a unitarily-invariant norm on the matrix $X_{|v\rangle}$ from the isomorphism that we have been using.

Theorem

Let $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ and let $X_{|v\rangle} \in M_n$ be the matrix associated to $|v\rangle$ via the standard vector-operator isomorphism. Let $\sigma_1 \geq \sigma_2 \geq \cdots \sigma_n \geq 0$ be the singular values of $X_{|v\rangle}$. Then

$$\big\||v\rangle\big\|_{s(k)} = \sqrt{\sum_{i=1}^{k} \sigma_i^2}.$$

Isometries of s(k)-Norms

Since that norm on $X_{|v\rangle}$ is unitarily-invariant, we can use Sourour's result on the isometries of unitarily-invariant matrix norms and go back through the vector-operator isomorphism to characterize the isometries of $\|\cdot\|_{s(k)}$:

Theorem

Let $1 \leq k < n$ and $U \in M_n \otimes M_n$. Then $\big\|U|v\rangle\big\|_{s(k)} = \big\||v\rangle\big\|_{s(k)}$ for all $|v\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ if and only if there exist unitaries $V, W \in M_n$ such that either

$$U = V \otimes W \quad \text{or} \quad U = S(V \otimes W),$$

where S is the swap operator as before.

Isometries of s(k)-Norms

Intuitively, the previous theorem makes sense because the norm $\|\cdot\|_{s(k)}$ can be thought of as a measure of "how separable" a state is (for example, $\big\||v\rangle\big\|_{s(k)} = 1$ if and only if $SR(|v\rangle) \leq k$).

The isometry result then says that the only operators that do not alter that separability measure are unitaries that act independently on each subsystem.

We will now present the analogous result for the $\|\cdot\|_{S(k)}$ norms.

Isometries of S(k)-Norms

Recall that $\big\|X\big\|_{S(k)} = \sup_{|v\rangle,|w\rangle} \big\{|\langle w|X|v\rangle| : SR(|v\rangle), SR(|w\rangle) \leq k\big\}$

The isometries of these norms are a bit more complicated to derive, but are almost exactly what someone would naively expect.

The only oddity comes in the $k = 1$ case, when we find that the isometry group is actually slightly larger than it is when $2 \leq k < n$.

In particular, there is one additional generator of the isometry group in the $k = 1$ case: the partial transpose map $(id_n \otimes T)$.

Isometries of S(k)-Norms

Theorem

Let $1 \leq k < n$ and $\Phi : M_n \otimes M_n \to M_n \otimes M_n$. Then $\big\|\Phi(X)\big\|_{S(k)} = \big\|X\big\|_{S(k)}$ for all $X \in M_n \otimes M_n$ if and only if Φ can be written as a composition of one or more of the following maps:

(a) $X \mapsto (U \otimes V)X(W \otimes Y)$, *where* $U, V, W, Y \in M_n$ *are unitary matrices,*

(b) $X \mapsto S_1 X S_2$, *where* $S_1, S_2 \in \{I, S\} \subset M_n \otimes M_n$ *and* S *is the swap operator,*

(c) *the transpose map* T, *and*

(d) *if* $k = 1$, *the partial transpose map* $(id_n \otimes T)$.

Further Reading

- N. Johnston. Characterizing Operations Preserving Separability Measures via Linear Preserver Problems. *Linear and Multilinear Algebra*, 59(10):1171–1187, 2011. arXiv:1008.3633 [quant-ph]
- A. Guterman, C.-K. Li, and P. Šemrl. Some general techniques on linear preserver problems. *Linear Algebra and its Applications*, 315:61–81, 2000.
- C.-K. Li and S. Pierce. Linear preserver problems. *The American Mathematical Monthly*, 108:591–605, 2001.
- C.-K. Li and N.-K. Tsing. Linear preserver problems: A brief introduction and some special techniques. *Linear Algebra and its Applications*, 162–164:217–235, 1992.