Complete positivity and variations on the Choi matrix

Fred Shultz
Wellesley College

MAQIT Daejeon 2016

Main Question

If $\Phi : M_n \to M_m$ is a linear map, the Choi matrix of Φ is

$$C_\Phi = \sum_{ij} E_{ij} \otimes \Phi(E_{ij}),$$

where $\{E_{ij}\}$ are the basis of M_n consisting of the standard matrix units.

Main Question

If $\Phi : M_n \to M_m$ is a linear map, the Choi matrix of Φ is

$$C_\Phi = \sum_{ij} E_{ij} \otimes \Phi(E_{ij}),$$

where $\{E_{ij}\}$ are the basis of M_n consisting of the standard matrix units.

By a result of Man-Duen Choi, Φ is completely positive iff C_Φ is positive.

Main Question

If $\Phi : M_n \to M_m$ is a linear map, the Choi matrix of Φ is

$$C_\Phi = \sum_{ij} E_{ij} \otimes \Phi(E_{ij}),$$

where $\{E_{ij}\}$ are the basis of M_n consisting of the standard matrix units.

By a result of Man-Duen Choi, Φ is completely positive iff C_Φ is positive.

Topic of this talk: to what extent can $\{E_{ij}\}$ be replaced by other bases of M_n?

Outline

I. Affine automorphisms and order isomorphisms (Review)

Outline

I. Affine automorphisms and order isomorphisms (Review)

II. Complete positivity of the map from a basis to the dual basis; variations on the Choi matrix (joint with Vern Paulsen)

Outline

I. Affine automorphisms and order isomorphisms (Review)

II. Complete positivity of the map from a basis to the dual basis; variations on the Choi matrix (joint with Vern Paulsen)

III. Unique determination of states by sets of observables (joint with J. Chen, H. Dawkins, Z. Ji, N. Johnston, D. Kribs, and B. Zeng)

H is a (finite or infinite dimensional) Hilbert space, and $\mathcal{B}(H)$ is the *-algebra of bounded operators on H.

H is a (finite or infinite dimensional) Hilbert space, and $\mathcal{B}(H)$ is the *-algebra of bounded operators on H.

A state on $\mathcal{B}(H)$ is a positive linear functional ρ such that $\rho(I) = 1$.

H is a (finite or infinite dimensional) Hilbert space, and $\mathcal{B}(H)$ is the *-algebra of bounded operators on H.

A state on $\mathcal{B}(H)$ is a positive linear functional ρ such that $\rho(I) = 1$.

If x is a unit vector in H, then ω_x denotes the vector state $\omega_x(A) = (Ax, x)$.

A state ω on $\mathcal{B}(H)$ is *normal* if there is a trace class operator D such that $\omega(A) = \text{tr}(AD)$ for $A \in \mathcal{B}(H)$.

A state ω on $\mathcal{B}(H)$ is *normal* if there is a trace class operator D such that $\omega(A) = \mathrm{tr}(AD)$ for $A \in \mathcal{B}(H)$.

Normal states are the countable convex combinations of vector states: $\omega(A) = \sum_i \lambda_i \omega_{x_i}(A)$.

K denotes the set of normal states on $\mathcal{B}(H)$. Note that K is convex, and the extreme points of K are the vector states.

A state ω on $\mathcal{B}(H)$ is *normal* if there is a trace class operator D such that $\omega(A) = \mathrm{tr}(AD)$ for $A \in \mathcal{B}(H)$.

Normal states are the countable convex combinations of vector states: $\omega(A) = \sum_i \lambda_i \omega_{x_i}(A)$.

K denotes the set of normal states on $\mathcal{B}(H)$. Note that K is convex, and the extreme points of K are the vector states.

A map $\Phi : K \to K$ is an *affine automorphism* if Φ is bijective and Φ preserves convex combinations, i.e.,

$$\Phi(t\rho_1 + (1-t)\rho_2) = t\Phi(\rho_1) + (1-t)\Phi(\rho_2)$$

for $0 \le t \le 1$ and all ρ_1, ρ_2 in K.

Why we care about affine automorphisms

In the quantum mechanical formalism,

- observables are self-adjoint operators in $\mathcal{B}(H)$.

- A state represents an ensemble of physical systems each prepared in the same fashion.

- If ρ is a state and A is an observable, then $\rho(A)$ is the expected value of the observable A in the state ρ.

- A convex combination of states is thought of as a statistical mixture.

- Physical symmetries (e.g., rotation) and time evolution act on states, are reversible, and preserve mixtures, hence are affine automorphisms of K.

Order automorphisms

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$: the space of observables (bounded self adjoint operators on H). We order $\mathcal{A}$ in the usual way: $A \leq B$ if $B - A$ is positive semi-definite, i.e., if $\langle A\xi, \xi\rangle \leq \langle B\xi, \xi\rangle$ for all $\xi \in H$.

Definition

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. A linear map $\Phi : \mathcal{A} \to \mathcal{A}$ is an *order isomorphism* if Φ is bijective and Φ and Φ^{-1} are order preserving, and is *unital* if $\Phi(I) = I$.

Order automorphisms

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$: the space of observables (bounded self adjoint operators on H). We order $\mathcal{A}$ in the usual way: $A \leq B$ if $B - A$ is positive semi-definite, i.e., if $\langle A\xi, \xi\rangle \leq \langle B\xi, \xi\rangle$ for all $\xi \in H$.

Definition

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. A linear map $\Phi : \mathcal{A} \to \mathcal{A}$ is an *order isomorphism* if Φ is bijective and Φ and Φ^{-1} are order preserving, and is *unital* if $\Phi(I) = I$.

Example

If $C \in \mathcal{B}(H)$ is invertible, then the map $X \mapsto C^*XC$ is an order automorphism of $\mathcal{A} = \mathcal{B}(H)_{sa}$.

*-automorphisms of $B(H)$

Definition

Let $\Phi : \mathcal{B}(H) \to \mathcal{B}(H)$ be a linear map. Then Φ is a *-automorphism

$$\Phi(X^*) = \Phi(X)^* \text{ and } \Phi(XY) = \Phi(X)\Phi(Y)$$

If Φ reverses products so that $\Phi(XY) = \Phi(Y)\Phi(X)$ then Φ is said to be a *-anti-automorphism.

Note there is no notion of *-automorphism on $\mathcal{A} = \mathcal{B}(H)_{sa}$ since products of observables need not be observables.

Examples

Theorem

If U is a unitary on H, then $X \mapsto UXU^*$ is a *-automorphism of $B(H)$ and every *-automorphism has this form.

Examples

Theorem

If U is a unitary on H, then $X \mapsto UXU^*$ is a *-automorphism of $B(H)$ and every *-automorphism has this form.

Theorem

If $t : \mathcal{B}(H) \to \mathcal{B}(H)$ is the transpose map (with respect to an orthonormal basis), then t is a *-anti-automorphism of $\mathcal{B}(H)$, and every *-anti-automorphism of $\mathcal{B}(H)$ has the form $X \mapsto UX^tU^*$ for some unitary U.

Jordan automorphisms

Definition

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. The Jordan product on $\mathcal{A}$ is given by $a \circ b = \frac{1}{2}(ab + ba)$. A Jordan automorphism $\Phi : \mathcal{A} \to \mathcal{A}$ is an linear bijection that preserves the Jordan product.

Jordan automorphisms

Definition

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. The Jordan product on $\mathcal{A}$ is given by $a \circ b = \frac{1}{2}(ab + ba)$. A Jordan automorphism $\Phi : \mathcal{A} \to \mathcal{A}$ is an linear bijection that preserves the Jordan product.

If $\Phi : \mathcal{B}(H) \to \mathcal{B}(H)$ is a *-automorphism or *-anti-automorphism, then Φ restricted to $\mathcal{A} = \mathcal{B}(H)_{sa}$ is a Jordan automorphism.

Physical importance of Jordan structure

The Jordan structure of a C*-algebra or von Neumann algebra was viewed as physically meaningful since it takes Hermitian operators to Hermitian operators, and is computable from the functional calculus:

$$a \circ b = \frac{1}{2}(ab + ba) = \frac{1}{4}((a+b)^2 - (a-b)^2).$$

Physical importance of Jordan structure

The Jordan structure of a C*-algebra or von Neumann algebra was viewed as physically meaningful since it takes Hermitian operators to Hermitian operators, and is computable from the functional calculus:

$$a \circ b = \frac{1}{2}(ab + ba) = \frac{1}{4}((a+b)^2 - (a-b)^2).$$

Kadison called a Jordan automorphism a quantum mechanical isomorphism or a C*-isomorphism!

Automorphisms of the space of observables

Theorem

(Kadison) Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. If $\Phi : A \to A$ is a linear map, the following are equivalent.
(i) Φ is a unital order automorphism.
(ii) Φ is an isometry on A. (In fact, then Φ will to an isometry on all of $B(H)$.)
(iii) Φ is a Jordan automorphism of A.
(iv) Φ is a *-isomorphism or a *-anti-isomorphism of $B(H)$.
(v) The map $\rho \mapsto \rho \circ \Phi$ is an affine automorphism of K.

Description of order automorphisms of $B(H)_{sa}$

Corollary

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. If $\Phi : \mathcal{A} \to \mathcal{A}$ is an order automorphism, then there is an invertible C in $B(H)$ such that either $\Phi(X) = CXC^*$ for all X in $\mathcal{A}$, or $\Phi(X) = CX^tC^*$ for all X in $\mathcal{A}$.

Description of order automorphisms of $B(H)_{sa}$

Corollary

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. If $\Phi : \mathcal{A} \to \mathcal{A}$ is an order automorphism, then there is an invertible C in $B(H)$ such that either $\Phi(X) = CXC^*$ for all X in $\mathcal{A}$, or $\Phi(X) = CX^tC^*$ for all X in $\mathcal{A}$.

Proof.

Suppose first that Φ is unital, i.e., $\Phi(I) = I$. Then by Kadison's results above, Φ is a Jordan automorphism, hence $\Phi(X) = UXU^*$ for a unitary U or else $\Phi(X) = UX^tU^*$.

Description of order automorphisms of $B(H)_{sa}$

Corollary

Let $\mathcal{A} = \mathcal{B}(H)_{sa}$. If $\Phi : \mathcal{A} \to \mathcal{A}$ is an order automorphism, then there is an invertible C in $B(H)$ such that either $\Phi(X) = CXC^*$ for all X in $\mathcal{A}$, or $\Phi(X) = CX^tC^*$ for all X in $\mathcal{A}$.

Proof.

Suppose first that Φ is unital, i.e., $\Phi(I) = I$. Then by Kadison's results above, Φ is a Jordan automorphism, hence $\Phi(X) = UXU^*$ for a unitary U or else $\Phi(X) = UX^tU^*$.
If Φ is not unital, then $B := \Phi(I)^{1/2}$ is positive and invertible. Then $X \mapsto B^{-1}\Phi(X)B^{-1}$ is a unital order automorphism, and now $\Phi(X) = (BU)X(BU)^*$ or $\Phi(X) = (BU)X^t(BU)^*$.

□

Description of affine automorphisms of K.

Theorem

Let K be the normal state space of $B(H)$. If $\Psi : K \to K$ is an affine automorphism, then there is a unitary U such that either

$$\Psi(\rho)(X) = \rho(UXU^*) \text{ for all } \rho \in K \text{ and all } X \text{ in } B(H),$$

or such that

$$\Psi(\rho)(X) = \rho(UX^tU^*) \text{ for all } \rho \in K \text{ and all } X \text{ in } B(H).$$

These results imply that the convex structure of the normal state space K (or equivalently the order structure on the space $\mathcal{A} = \mathcal{B}(H)_{sa}$) determine the Jordan product and the norm on $\mathcal{B}(H)$, and one of two possible associative products.

II. Applications to complete positivity of certain maps

Let $\Phi : M_n \to M_m$ be a linear map. Then Φ is *positive* if $a \geq 0$ implies $\Phi(a) \geq 0$.

II. Applications to complete positivity of certain maps

Let $\Phi : M_n \to M_m$ be a linear map. Then Φ is *positive* if $a \geq 0$ implies $\Phi(a) \geq 0$.

Φ is *completely positive* if the map $I_p \otimes \Phi : M_p \otimes M_n \to M_p \otimes M_n$ is positive for all p.

(If we identify $M_p \otimes M_n$ with $M_p(M_n)$, this is equivalent to the entry-wise map $(a_{ij}) \to (\Phi(a_{ij}))$ being positive.)

M_n^* denotes the dual vector space of M_n.

We will be investigating complete positivity of certain maps from M_n to M_n^*, so we need a definition of order on $M_p(M_n^*)$ for $p \geq 1$.

M_n^* denotes the dual vector space of M_n.

We will be investigating complete positivity of certain maps from M_n to M_n^*, so we need a definition of order on $M_p(M_n^*)$ for $p \geq 1$.

Definition

A matrix of functionals $(f_{i,j}) \in M_p(M_n^*)$ is positive if and only if the linear map $\Phi : M_n \to M_p$ given by $\Phi(A) = (f_{i,j}(A))$ is completely positive.

Definition

A linear map Φ from M_n to M_n^* is completely positive if $I \otimes \Phi : M_p \otimes M_n \to M_p \otimes M_n^*$ is positive, i.e. $(a_{ij}) \mapsto (\Phi(a_{ij}))$ is a positive map.

Definition

A linear bijection Φ from M_n to M_n or to M_n^* is a *complete order isomorphism* if both Φ and Φ^{-1} are completely positive.
Φ is called a *completely co-positive order isomorphism* provided that its composition $\Psi \circ t$ with the transpose map t on M_n is a complete order isomorphism.

Examples

If $\rho \in M_n^*$, then there is a unique matrix $D_\rho \in M_n$ such that $\rho(A) = \mathrm{tr}(AD_\rho)$. The matrix D_ρ is called the density matrix for ρ.

Examples

If $\rho \in M_n^*$, then there is a unique matrix $D_\rho \in M_n$ such that $\rho(A) = \mathrm{tr}(AD_\rho)$. The matrix D_ρ is called the density matrix for ρ.

Example

The map that takes a functional on M_n to its density matrix is a completely co-positive order isomorphism.

Examples

If $\rho \in M_n^*$, then there is a unique matrix $D_\rho \in M_n$ such that $\rho(A) = \operatorname{tr}(AD_\rho)$. The matrix D_ρ is called the density matrix for ρ.

Example

The map that takes a functional on M_n to its density matrix is a completely co-positive order isomorphism.

Example

The map that takes $\rho \in M_n^*$ to $D_\rho^* \in M_n$ is a complete order isomorphism but is conjugate linear.

Definition

Given a basis $\mathcal{B}$ of M_n, the *duality map* $\mathcal{D}_{\mathcal{B}} : M_n \to M_n^*$ is the linear map that takes the basis $\mathcal{B}$ to its dual basis.

Definition

Given a basis $\mathcal{B}$ of M_n, the *duality map* $\mathcal{D}_{\mathcal{B}} : M_n \to M_n^*$ is the linear map that takes the basis $\mathcal{B}$ to its dual basis.

Theorem

(Paulsen-Todorov-Tomforde) For the standard basis $\mathcal{E} = \{E_{ij} \mid 1 \leq i, j \leq n\}$, $\mathcal{D}_{\mathcal{E}}$ is a complete order isomorphism.

Definition

Given a basis $\mathcal{B}$ of M_n, the *duality map* $\mathcal{D}_{\mathcal{B}} : M_n \to M_n^*$ is the linear map that takes the basis $\mathcal{B}$ to its dual basis.

Theorem

(Paulsen-Todorov-Tomforde) For the standard basis $\mathcal{E} = \{E_{ij} \mid 1 \leq i,j \leq n\}$, $\mathcal{D}_{\mathcal{E}}$ is a complete order isomorphism.

Main question: for which bases $\mathcal{B}$ is the duality map a complete order isomorphism?

Why should one care?

1. Curiosity: what is special about the standard basis $\mathcal{E}$ of M_n when working with complete positivity? Would other bases commonly used in applications work as well?

Why should one care?

1. Curiosity: what is special about the standard basis $\mathcal{E}$ of M_n when working with complete positivity? Would other bases commonly used in applications work as well?

2. The answer leads to alternate versions of Choi's characterization of completely positive maps

Why should one care?

1. Curiosity: what is special about the standard basis $\mathcal{E}$ of M_n when working with complete positivity? Would other bases commonly used in applications work as well?

2. The answer leads to alternate versions of Choi's characterization of completely positive maps

3. Greater convenience when working with bases of interest in quantum information: e.g., Pauli spin matrices and their tensor products, and the Weyl basis.

Why should one care?

1. Curiosity: what is special about the standard basis $\mathcal{E}$ of M_n when working with complete positivity? Would other bases commonly used in applications work as well?

2. The answer leads to alternate versions of Choi's characterization of completely positive maps

3. Greater convenience when working with bases of interest in quantum information: e.g., Pauli spin matrices and their tensor products, and the Weyl basis.

4. A source of "entanglement witnesses": matrices that provide a test of entanglement.

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units. Define $M_{\mathcal{B}} : M_n \to M_n$ by $M_{\mathcal{B}} = D_{\mathcal{B}}^{-1} D_{\mathcal{E}}$.

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units. Define $M_{\mathcal{B}} : M_n \to M_n$ by $M_{\mathcal{B}} = D_{\mathcal{B}}^{-1} D_{\mathcal{E}}$.

Since $D_{\mathcal{E}} : M_n \to M_n^*$ is a complete order isomorphism, then $D_{\mathcal{B}} : M_n \to M_n^*$ will be a complete order isomorphism (resp. completely co-positive order isomorphism) iff $M_{\mathcal{B}} : M_n \to M_n$ is a complete order isomorphism (resp. completely co-positive order isomorphism.)

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units, with a fixed order. A *change of basis map* is any linear map $C_{\mathcal{B}}$ in $L(M_n)$ taking the set $\mathcal{E}$ to the set $\mathcal{B}$.

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units, with a fixed order. A *change of basis map* is any linear map $C_{\mathcal{B}}$ in $L(M_n)$ taking the set $\mathcal{E}$ to the set $\mathcal{B}$.

Definition

By slight abuse of notation, we write $C_{\mathcal{B}}^T$ for the unique linear map in $L(M_n)$ whose matrix in the standard basis $\mathcal{E}$ is the transpose of the matrix of $C_{\mathcal{B}}$.

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units, with a fixed order. A *change of basis map* is any linear map $C_{\mathcal{B}}$ in $L(M_n)$ taking the set $\mathcal{E}$ to the set $\mathcal{B}$.

Definition

By slight abuse of notation, we write $C_{\mathcal{B}}^T$ for the unique linear map in $L(M_n)$ whose matrix in the standard basis $\mathcal{E}$ is the transpose of the matrix of $C_{\mathcal{B}}$.

Theorem

$M_{\mathcal{B}} = C_{\mathcal{B}} C_{\mathcal{B}}^T$.

Definition

Let $\mathcal{B}$ be a basis of M_n and $\mathcal{E}$ the standard basis of matrix units, with a fixed order. A *change of basis map* is any linear map $C_{\mathcal{B}}$ in $L(M_n)$ taking the set $\mathcal{E}$ to the set $\mathcal{B}$.

Definition

By slight abuse of notation, we write $C_{\mathcal{B}}^T$ for the unique linear map in $L(M_n)$ whose matrix in the standard basis $\mathcal{E}$ is the transpose of the matrix of $C_{\mathcal{B}}$.

Theorem

$M_{\mathcal{B}} = C_{\mathcal{B}} C_{\mathcal{B}}^T$.

It follows that $M_{\mathcal{B}}$ depends on the basis $\mathcal{B}$, but not on the particular choice of change of basis map $C_{\mathcal{B}}$ (i.e., not on the order of the basis).

Main theorem on complete positivity of $\mathcal{D}_B$.

Theorem

Let $\mathcal{B}$ be a basis of M_n. Then $\mathcal{D}_\mathcal{B} : M_n \to M_n^*$ is a complete order isomorphism iff $C_B C_B^T = \mathrm{Ad}_C$ for some $C \in M_n$, and is a completely co-positive order isomorphism iff $C_B C_B^T = \mathrm{Ad}_C \circ t$ for some $C \in M_n$.

Examples: some bases closely related to the standard basis

Theorem

Let $(\lambda_{ij}) \in M_n$, with all λ_{ij} nonzero, and let $\mathcal{B}$ be the basis $\{\lambda_{ij} E_{ij}\}$. Then $\mathcal{D}_{\mathcal{B}}$ is an order isomorphism if and only if the matrix (λ_{ij}^2) is positive semi-definite with rank one. In that case, $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism.

Examples: some bases closely related to the standard basis

Theorem

Let $(\lambda_{ij}) \in M_n$, with all λ_{ij} nonzero, and let $\mathcal{B}$ be the basis $\{\lambda_{ij} E_{ij}\}$. Then $\mathcal{D}_{\mathcal{B}}$ is an order isomorphism if and only if the matrix (λ_{ij}^2) is positive semi-definite with rank one. In that case, $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism.

Example

If $C \in M_n$ is invertible, for the basis $\mathcal{B} = \{CE_{ij}C^*\}$, the duality map $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism. In particular, if $\mathcal{B}$ is a system of matrix units then $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism.

Weyl basis

Definition

Let $e_0, \ldots, e_{n-1}$ be the standard basis of $\mathbb{C}^n$. Let $z = \exp(2\pi i/n)$. Define $U, V \in M_n$ by

$$Ve_j = z^j e_j$$

and

$$Ue_j = e_{j+1}$$

for $j \in \mathbb{Z}_n$. Then $\{\frac{1}{\sqrt{n}} U^a V^b \mid a, b \in \mathbb{Z}_n\}$ is an orthonormal basis for M_n which we call the *Weyl basis* $\mathcal{W}$.

The unitary matrices $\{U^a V^b \mid a, b \in \mathbb{Z}_n\}$ are usually called the *discrete Weyl matrices* or the *generalized Pauli matrices*.

Theorem

For the Weyl basis $\mathcal{W}$, the duality map $\mathcal{D}_{\mathcal{W}} : M_n \to M_n^*$ is a complete order isomorphism if $n = 2$, and is not an order isomorphism for $n > 2$.

Theorem

For the Weyl basis $\mathcal{W}$, the duality map $\mathcal{D}_{\mathcal{W}} : M_n \to M_n^*$ is a complete order isomorphism if $n = 2$, and is not an order isomorphism for $n > 2$.

Corollary

For the basis of $M_2^{\otimes n}$ consisting of tensor products of the 2×2 Weyl basis, the duality map $\mathcal{D}_{\mathcal{W}}$ is a complete order isomorphism

Testing complete positivity using non-standard bases

Definition

If $\Phi : M_m \to M_n$ is a linear map, the Choi matrix of Φ is

$$C_\Phi = \sum_{ij} E_{ij} \otimes \Phi(E_{ij})$$

Theorem

(Choi) If $\Phi : M_m \to M_n$ is a linear map, then Φ is completely positive iff $C_\Phi \geq 0$.

Choi's characterization of complete positivity doesn't necessarily hold for other bases of M_m in place of $\{E_{ij}\}$. The following is a consequence of the preceding results.

Choi's characterization of complete positivity doesn't necessarily hold for other bases of M_m in place of $\{E_{ij}\}$. The following is a consequence of the preceding results.

Corollary

Let $\mathcal{B} = \{B_j : 1 \leq j \leq n^2\}$ be a basis for M_n, and let $\Psi : M_n \to M_p$ be a linear map.

1. If the duality map $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism, then Ψ is completely positive if and only if $\sum_{j=1}^{n^2} \Psi(B_j) \otimes B_j \in (M_p \otimes M_n)^+$.

Choi's characterization of complete positivity doesn't necessarily hold for other bases of M_m in place of $\{E_{ij}\}$. The following is a consequence of the preceding results.

Corollary

Let $\mathcal{B} = \{B_j : 1 \leq j \leq n^2\}$ be a basis for M_n, and let $\Psi : M_n \to M_p$ be a linear map.

1. If the duality map $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism, then Ψ is completely positive if and only if $\sum_{j=1}^{n^2} \Psi(B_j) \otimes B_j \in (M_p \otimes M_n)^+$.
2. If the duality map $\mathcal{D}_{\mathcal{B}}$ is a completely co-positive order isomorphism, then Ψ is completely positive if and only if $\sum_{j=1}^{n^2} \Psi(B_j) \otimes B_j^t \in (M_p \otimes M_n)^+$.

Entanglement witnesses

Definition

A state ρ on $M_n \otimes M_n$ is *entangled* if it is not a convex combination of product states.

It is not easy to tell if a state is entangled. One way is by finding an entanglement witness.

Definition

If $W = W^* \in M_n \otimes M_n$, then W is an *entanglement witness* if W is positive on product states but $\rho(W) < 0$ for some state ρ. (This implies ρ is entangled, and we say W witnesses the entanglement of ρ.)

Corollary

Let $\mathcal{B}$ be a basis of M_n such that the duality map $\mathcal{D}_{\mathcal{B}}$ is a complete order isomorphism. If $\Psi : M_n \to M_n$ is any map that is positive but not completely positive, then $\sum_{B_i \in \mathcal{B}} B_i \otimes \Psi(B_i)$ is an entanglement witness.

A basis-free description of the Choi matrix

Recall the Choi matrix for $\Phi : M_n \to M_n$ is defined by $C_\Phi = \sum_i E_{ij} \otimes \Phi(E_{ij})$. Here the basis $\{E_{ij}\}$ can't be replaced by an arbitrary orthonormal basis. The following result provides an alternate description of the Choi matrix that does have this independence property. Given a matrix $B = (b_{i,j})$ we set $\overline{B} = (\overline{b_{i,j}})$.

A basis-free description of the Choi matrix

Recall the Choi matrix for $\Phi : M_n \to M_n$ is defined by $C_\Phi = \sum_i E_{ij} \otimes \Phi(E_{ij})$. Here the basis $\{E_{ij}\}$ can't be replaced by an arbitrary orthonormal basis. The following result provides an alternate description of the Choi matrix that does have this independence property. Given a matrix $B = (b_{i,j})$ we set $\overline{B} = (\overline{b_{i,j}})$.

Theorem

Let $\{B_l\}_{l=1}^{n^2}$ be an orthonormal basis for M_n, and $\Phi : M_n \to M_p$ linear. Then Choi's matrix is given by

$$C_\Phi = \sum_{l=1}^{n^2} \overline{B_l} \otimes \Phi(B_l) \qquad (1)$$

This expression shows that the Choi matrix is the partial transpose of a matrix defined by Jamiołkowski

$$\mathcal{J}(\Phi) = \sum_{ij} E_{ij}^* \otimes \Phi(E_{ij}). \tag{2}$$

Jamiołkowski defined this correspondence as a tool in studying linear maps from M_n into M_p. Here E_{ij} could be replaced by any orthonormal basis, but positivity of $\mathcal{J}(\Phi)$ is not equivalent to complete positivity of Φ.

Reference

V. Paulsen and F. Shultz., Complete positivity of the map from a basis to its dual basis, Journal of Mathematical Physics 54 (2013) 072201.

UDA and UDP

I'm going to discuss a result from the paper

J. Chen, H. Dawkins, Z. Ji, N. Johnston, D. Kribs, F. Shultz, and B. Zeng, Uniqueness of quantum states compatible with given measurement results, *Physical Review A* **88** (2013) 012109.

and its connection with the results on affine automorphisms above.

One goal of quantum tomography is to make measurements to determine a state.

Definition

A set of observables $\mathcal{A}$ in M_n is *informationally complete* if $\operatorname{tr} A\rho_1 = \operatorname{tr} A\rho_2$ for all $A \in \mathcal{A}$ implies $\rho_1 = \rho_2$.

One goal of quantum tomography is to make measurements to determine a state.

Definition

A set of observables $\mathcal{A}$ in M_n is *informationally complete* if $\operatorname{tr} A\rho_1 = \operatorname{tr} A\rho_2$ for all $A \in \mathcal{A}$ implies $\rho_1 = \rho_2$.

Clearly there are informationally complete sets of $n^2 - 1$observables whose span (with the identity) is all of M_n, hence $n^2 - 1$ observables suffice, and one can show no smaller number of observables suffices.

Suppose one has additional information, for example, that the states to be distinguished are all pure states. Then Heinosaari, Mazzarella, Wolf showed that $4n - 5$ observables suffice.

Suppose one has additional information, for example, that the states to be distinguished are all pure states. Then Heinosaari, Mazzarella, Wolf showed that $4n - 5$ observables suffice.

Now suppose that one has a particular pure state ρ and would like to know how many observables are needed to to distinguish that state ρ among all states.

Suppose one has additional information, for example, that the states to be distinguished are all pure states. Then Heinosaari, Mazzarella, Wolf showed that $4n-5$ observables suffice.

Now suppose that one has a particular pure state ρ and would like to know how many observables are needed to to distinguish that state ρ among all states.

Definition

Let ρ be a pure state on H and $\mathbf{A}$ a finite set of observables. We say $(\rho, \mathbf{A})$ has the UDA property if $\sigma(A) = \rho(A)$ for a state σ and for all $A \in \mathbf{A}$ implies $\sigma = \rho$. If this holds when σ is restricted to being a pure state, we say $(\rho, \mathbf{A})$ has the UDP property. (The acronym "UDA" stands for "uniquely determined for all".)

Suppose one has additional information, for example, that the states to be distinguished are all pure states. Then Heinosaari, Mazzarella, Wolf showed that $4n-5$ observables suffice.

Now suppose that one has a particular pure state ρ and would like to know how many observables are needed to to distinguish that state ρ among all states.

Definition

Let ρ be a pure state on H and $\mathbf{A}$ a finite set of observables. We say $(\rho, \mathbf{A})$ has the UDA property if $\sigma(A) = \rho(A)$ for a state σ and for all $A \in \mathbf{A}$ implies $\sigma = \rho$. If this holds when σ is restricted to being a pure state, we say $(\rho, \mathbf{A})$ has the UDP property. (The acronym "UDA" stands for "uniquely determined for all".)

Chen, Dawkins, Ji, Johnston, Kribs, S., and Zeng construct a set of observables with $|\mathcal{A}| = \mathbf{5n-7}$ possessing the UDA property.

Another UDP/UDA result

Lemma

Let G be a compact group of unitaries on a real or complex finite dimensional Hilbert space H, and let L be the set of fixed points of G. Let μ be Haar measure on G, and define $P : H \to H$ to be the linear map satisfying

$$\langle P\xi, \eta\rangle = \int_G \langle g\xi, \eta\rangle \, d\mu(g) \tag{3}$$

for $\xi, \eta \in H$. Then P is the orthogonal projection onto L, $Pg = gP = P$ for all $g \in G$, and P is in the convex hull of G.

Let K_n be the state space of M_n. Recall that symmetries of K_n are given by conjugation by unitaries or by the transpose map or by composition of these two types of symmetries.

Let K_n be the state space of M_n. Recall that symmetries of K_n are given by conjugation by unitaries or by the transpose map or by composition of these two types of symmetries.

If we view $L(M_n)_{sa}$ as a real Hilbert space (with the usual inner product $\langle X, Y \rangle = \mathrm{tr}(XY)$), then conjugation by unitaries in M_n and the transpose map on M_n both preserve this inner product, so these symmetries are unitaries on the Hilbert space $L(M_n)_{sa}$. Thus we can apply the lemma above.

Let K_n be the state space of M_n. Recall that symmetries of K_n are given by conjugation by unitaries or by the transpose map or by composition of these two types of symmetries.

If we view $L(M_n)_{sa}$ as a real Hilbert space (with the usual inner product $\langle X, Y\rangle = \mathrm{tr}(XY)$), then conjugation by unitaries in M_n and the transpose map on M_n both preserve this inner product, so these symmetries are unitaries on the Hilbert space $L(M_n)_{sa}$. Thus we can apply the lemma above.

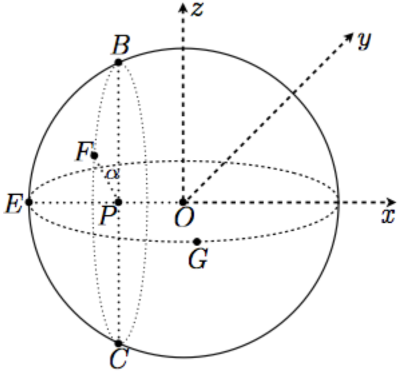
In the following theorem we are identifying states with the associated density matrices: $\rho(A) = \mathrm{tr}(AD)$ and conversely observables with members of the linear span of K_n.

Theorem

Let A be a finite set of observables on H_n with real linear span L. Assume there exists a compact group G of affine automorphisms of K_n whose fixed point set is $L \cap K_n$. Then each pure state which is UDP for measuring A is also UDA.

Theorem

Let A be a finite set of observables on H_n with real linear span L. Assume there exists a compact group G of affine automorphisms of K_n whose fixed point set is $L \cap K_n$. Then each pure state which is UDP for measuring A is also UDA.



Corollary

For $n = 2$, for all pure states and all sets $\mathbf{A}$ of observables, UDP implies UDA.

Corollary

Let $\mathbf{A} = \{A_1, \ldots, A_p\}$ be observables in M_n. If the (complex) linear span of $\mathbf{A}$ is a *-subalgebra $\mathbf{A}$ of M_n, then UDP = UDA for pure states measured by these observables.

Corollary

Let $\mathbf{A} = \{A_1, \ldots, A_p\}$ be observables in M_n. If the (complex) linear span of $\mathbf{A}$ is a *-subalgebra $\mathbf{A}$ of M_n, then UDP $=$ UDA for pure states measured by these observables.

Example

Let $\mathbf{A} = \{E_{11}, \ldots, E_{nn}\}$. Then the complex linear span of $\mathbf{A}$ consists of the diagonal matrices. From the corollary it follows that for each pure state ρ on M_n, UDP for $\mathbf{A}$ implies UDA.